

TOPCIT

ESSENCE

TOPCIT ESSENCE Technical Field 04 Understanding of Security

TOPCIT

ESSENCE Ver.2

Technical Field
04 Understanding of Security



TOPCIT

ESSENCE Ver.2

Technical Field

04 Understanding of Security



TOPCIT ESSENCE is published to provide learning materials for TOPCIT examinees.

The TOPCIT Division desires the TOPCIT examinees who want to acquire the necessary practical competency in the field of ICT to exploit as self-directed learning materials.

For more information about TOPCIT ESSENCE, visit TOPCIT website or send us an e-mail.

As part of the TOPCIT ESSENCE contents feed into authors' personal opinions, it is not the TOPCIT Division's official stance.

Ministry of Science, ICT and Future Planning
Institute for Information and Communications Technology Promotion
Korea Productivity Center

Publisher TOPCIT Division
+82-2-398-7649 www.topcit.or.kr/en helpdesk@topcit.or.kr

Date of Publication 1st Edition 2014. 12. 10
2nd Edition 2016. 2. 26

Copyright © Ministry of Science, ICT and Future Planning
All rights reserved.

No part of this book may be used or reproduced in any manner whatever without written permission.

TOPCIT

ESSENCE Ver.2

Technical Field

04 Understanding of Security

TOPCIT

ESSENCE Ver.2



Technical Field

04 Understanding of Security

Understanding the Basic Concept of Information Security 12

01 Concept of Information Security	13
Outline of Information Security	13

Confidentiality, Integrity, and Authentication for Software Developers 15

01 Outline of Cryptography	16
Concept and History of Cryptography	16
Ancient Cryptography	18
Modern Cryptography	19
Contemporary Cryptography	20
Key Exchange Algorithm	25
Use of Cryptographic Technologies	26
Encryption and Decryption of Java Language	29

02 Hash function	31
Definition and Characteristic of Hash Function	31
Types of Hash Functions	32
Application of Hash Function	34

03 Authentication Technologies	36
Concept of Authentication	36
Major Authentication Methods	37
Digital Signature	41
PKI	43

Understanding the Concept and Types of Network Security and Build Secure Network 48

01 Outline of Network Security	49
Concept of Network Security	49
Communications Protocol Layer and Security	53
Types of Network Attacks and Defense Mechanisms	56

02 Security Protocol and Security Solution	59
IPSec	59
SSL	62
Security Solution	65
Screened Host Gateway	67

03 Security of Wireless LAN	72
Characteristics of Wireless LAN	72
Security Threats and Response	73
Security Standards for Wireless LAN	74

04 Security for Application Layer	76
E-mail Security	76
Ftp Security	77
Http Security	77
Dns Security.	78

Security Readiness for Safer System Management 80

01 Access Control	81
-------------------	----

CONTENTS

Outline of Access Control	81	Policy for Database Access Control	98
Access Control Model	82	Implementation Methods of DB Access Control	98
02 Security for Windows System	83	03 Database Encryption	100
Outline of Security for Windows System	83	Factors to Be Considered in Database Encryption	100
Management of Accounts and Passwords	84	Object for Database Encryption and Relevant Methods	100
Access Control	85	Types of Database Encryption	101
System Security	86	How to Apply Encryption Algorithms for Database	102
Service Security	87	Processes of Database Encryption	105
Checkup of Terminal Services	87	04 Database Encryption Key Management	106
03 Security for UNIX systems	87	Types of Keys Used for Database Encryption	106
Outline of Security for Unix-like Systems	87	How to Manage Encryption Key in Each Stage of Key Lifecycle	106
Management of Accounts and Passwords	88	Understanding Information Security Management System and Risk Management	109
Access Control	88	01 Information Security Management System	110
System Security	89	Outline of Information Security Management System	110
Service Security	89	Risk Management	112
04 Secure OS	92	Standards Related to Information Security Management System	114
Outline of Secure OS	92	Building Disaster Recovery System that Reflects Organizational Circumstances	119
Security Mechanism and Key Functions of Secure OS	92	01 Disaster Recovery System	121
Managing Database Securely	95	Outline of Disaster Recovery	121
01 Outline of Database Security	96		
Introduction to Database Security	96		
Sources of Database Security Threats and Responses	97		
02 Database Access Control	98		

Business Continuity Planning	123	Latest Trend of Information Security Standardization	145
Understanding Personal Information Protection	126		
01 Personal Information Protection	127		
Outline of Personal Information Protection	127		
Certification System for Personal Information Protection	131		
Understanding about the Latest Threats to Information Security	135		
01 Latest Threats in Information Security	136		
APT (Advanced Persistent Threat)	136		
Smishing	137		
Open SSL Vulnerability (HeartBleed)	138		
GNU Bash Shell Vulnerability (Shell Shock)	139		
Spear Phishing	141		
NTP (Network Time Protocol) Vulnerability	141		
02 Latest Information Protection Technologies	142		
Network Separation/Bridge	142		
MDM (Mobile Device Management)	143		
WIPS (Wireless Intrusion Prevention System)	143		
FDS (Fraud Detection System)	143		
02 Latest Standards for Information Security	144		
Legislations and Regulations Related to Information Security	144		

Understanding the Basic Concept of Information Security

▶▶▶ Latest Trends and Key Issues

Widespread adoption of IoT, the ever-increasing sophistication of malware, personally identifiable information within the big data framework, Fraud Detection System (FDS), and personally-customized cloud security services have emerged as the key issues in information security in 2015. While industrial technologies get more sophisticated, information security technologies have yet to be developed to keep up with those advanced industrial technologies. Therefore, cyber crimes, which take advantage of convergence technologies, will likely come in various forms. Against this backdrop, some advanced countries are developing a variety of technologies and products to enhance the competitiveness of information security in the area of convergence technology.

▶▶▶ Study Objectives

- * To be able to explain about the concept of information security
- * To be able to explain what information security is for and why it is important

▶▶▶ Practical Importance High

▶▶▶ Keywords

Information security, Managerial · Technical · Physical information security, Confidentiality, Integrity, Availability, Non-repudiation, Authentication, Access control

+ Practical tips

Mr. Kim is responsible for the development of PHP sources and their deployment, and is also responsible for the maintenance of source programs at Company A. Kim periodically conducts inspections over the web pages and the servers.

In this process, Kim is required to secure the integrity of many sources that Kim manages. Managing performance and capacity of the servers to guarantee their availability, which support smooth operation of application programs, is also one of his responsibilities. He also needs to ensure confidentiality of customers' personal information stored in application programs through technical security measures, such as encryption.

All these activities mentioned above are done by Mr. Kim in a bid to ensure confidentiality, integrity, and availability. In this chapter, we will cover the basic concept and goals of information security in detail.

01 Concept of Information Security

Outline of Information Security

① What is information security?

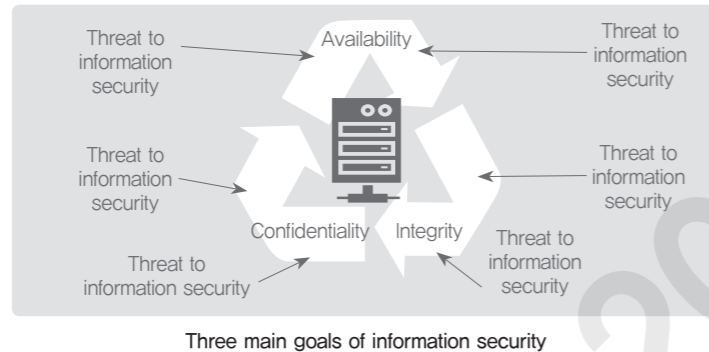
Information security is the practice of managerially, physically, and technically protecting information from unauthorized destruction, modification, or leakage in the course of collecting, processing, storing, and transmitting information.

② Why is information security important?

There are growing needs for securing privacy on the Internet and preventing cyber crimes. In a world which is globally connected with the rise of the Internet, concerns are growing as well that proprietary technologies or information of a county could be leaked to others.

③ What does information security pursue?

Information security is designed to ensure confidentiality, integrity and availability – known as three main goals of information security – in a managerial, physical, and technical way.

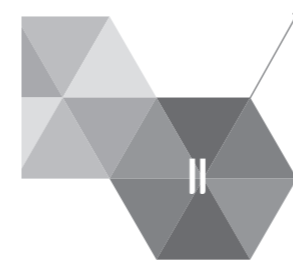


- Confidentiality refers to protecting information from being disclosed to any unauthorized parties when information is stored or transmitted.
- Integrity refers to protecting information from being generated, manipulated, or deleted by any unauthorized parties when information is sent or received.
- Availability refers to ensuring that only the authorized parties are able to gain access to and use the information they want when needed.

Apart from the three main goals mentioned above, non-repudiation, authentication and access control are other goals of information security. In the following chapter, we will take a look at how these goals of information security are achieved by using various information security technologies.

Related E-learning Contents

- **Lecture 1** Basic Concept of Information Security and Related Technologies



Confidentiality, Integrity, and Authentication for Software Developers

▶▶▶ Latest Trends and Key Issues

As the cyberspace is being widened and developed, it has led to many subsequent problems, such as unauthorized access, information leakage, and file manipulation. Worse yet, even patch programs of Windows or vaccine programs are distributed after they are infected with a virus or manipulated. Against this backdrop, information security can provide the means to actively respond against various forms of security threats, ensuring that confidentiality and integrity are firmly in place. Confidentiality means that only authorized parties can read or understand a certain set of data. Integrity refers to protecting data from being modified or fabricated and ensuring that the data remains intact. Therefore, when one works to ensure confidentiality and/or integrity, the nature of data should be taken into consideration.

▶▶▶ Study Objectives

- * To be able to explain about the concept of cryptography that is intended to ensure the confidentiality service, and ancient cryptographies
- * To be able to explain about the secret key encryption algorithm and public key encryption algorithm
- * To be able to explain about the hash function that is used to ensure the integrity service
- * To be able to explain about the digital signature and PKI (Public Key Infrastructure) used to make transactions safe.
- * To be able to explain about key sharing
- * To be able to explain about authentication technologies and authentication methods used for access control.

▶▶▶ Practical Importance High

▶▶▶ Keywords

Cryptographic algorithm, Secret key-based encryption, Public key-based encryption, Hash function, Authentication, Digital signature, PKI, Access control, Cryptographic protocol, DES, AES, RSA, ECC, Hash collision, Public key certificate, Multi factor authentication, Session key

+ Practical tips To manage information securely

Mr. Kim, who works for a web application program development company, is responsible for the development of PHP-based sources, their deployment, and the maintenance of source programs. Periodically, Kim inspects the web pages and web servers in which he manages the sources. However, such periodic maintenance inspections alone cannot make the company free from more diversified and sophisticated security threats.

One of his duties is to share source programs with his business partners in a secure manner, so that the source programs are not exposed to other competitors.

In this environment, Mr. Kim has to prevent the source programs from being exposed to unauthorized third parties in the processes of storing or transmitting the programs. In this chapter, we will take a look at what measures can be taken to guarantee confidentiality and how they are applied to the actual environment.

01 Outline of Cryptography

Concept and History of Cryptography

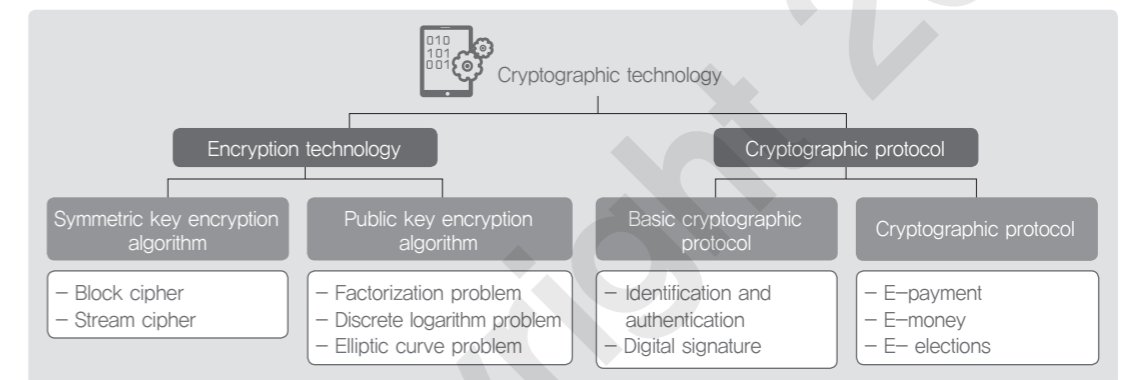
The word cryptography comes from the Greek word Kryptos which means "secret". The definition of encryption is the conversion of a plaintext, which is readable to all, into another form called a ciphertext, which cannot be easily understood by anyone except the authorized parties. The definition of decryption is the process of converting the ciphertext back to the plaintext, so that it can be read and understood. In a nutshell, these two processes constitute the Cryptography. A mathematical formula used for these conversion processes is called a cryptographic algorithm. The cryptographic algorithm uses a key to perform encryption and decryption. Simply put, encryption is an important practice of ensuring confidentiality, one of the three main goals of information security.

The history of cryptography can be divided into three periods – ancient, modern and contemporary. The ancient cryptography means the cryptography used in the period before the First World War broke out. At the time, there were no electronic cryptographic devices. The era of the modern cryptography began in the 1920s when the First World War took place. During the First and Second World Wars, radio communications technologies were significantly developed. Based on these technologies, a variety of mechanical and electronic cryptographic devices were developed and widely used until the 1970s. Since the 1970s, with the wide use of computers, cryptographic technologies have been developed by utilizing computers. This period is so called the era of the contemporary cryptography.

① Classification of cryptographic technologies

As shown in (Figure 1), a cryptographic technology can be divided into encryption technology and cryptographic protocol at a high level. The encryption technology is sub-divided into two types – symmetric key encryption and public key encryption, depending on whether an encryption key and a decryption key are symmetric or asymmetric. When they are symmetric, it is called a symmetric key encryption, while, when asymmetric, it is called a public key encryption.

Cryptographic protocol refers to a protocol which utilizes cryptographic technologies. A protocol is defined as a finite series of steps in which more than two parties join in order to achieve a certain objective. In this sense, the cryptographic protocol should ensure not only the meaning of each message in the protocol, but also a certain objective of the protocol (such as authentication, confidentiality, integrity, non-repudiation, etc.). To achieve such a goal, the cryptographic protocol needs to ensure that participating parties or a third party cannot deny their involvement in the communications.

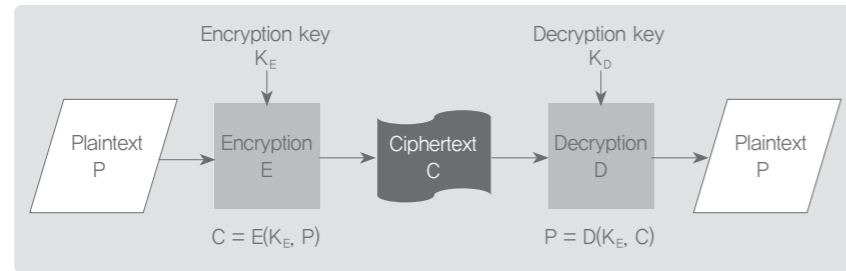


〈Figure 1〉 Classification of cryptographic technologies

② Encryption mechanism

A cryptographic algorithm that uses a cryptographic key is illustrated in (Figure 2). In this figure, P refers to a plaintext, E to an encryption function, and K (KE, KD) to a key value. Like in the public key encryption, an encryption key and a decryption key can be different. In such a case, they are referred to as KE and KD respectively. A ciphertext is usually transferred through insecure communication lines or networks. Hence, converting a plaintext to a ciphertext and transferring the converted text can be the way for securing message confidentiality between a sender and a receiver.

The sender wants to transfer P (plain text), readable to everyone, in a secure way. For this, the sender converts P to C, using KE and E (Encryption algorithm), and sends C to the receiver. One cannot understand the message of C if a decryption key is not available, which is called non-computable. Non-computable means that it takes countless trials, but it is possible to find out a plaintext from a ciphertext without a decryption key. Attackers use various methods to read and understand the content of a plaintext. On the other hand, an authorized receiver can get the plaintext exactly as it was transmitted, using KD and D (Decryption algorithm).



〈Figure 2〉 Cryptographic algorithm mechanism

All required for a series of encryption and decryption processes are called the elements of a cryptosystem. In general, the cryptosystem should meet the following requirements.

- Encryption and decryption should be effectively performed by using an encryption key.
- The cryptosystem should be easy to use.
- Security should be achieved through an encryption key, rather than an encryption algorithm.

③ Cryptographic algorithm

An algorithm refers to the methods or procedures that are used to solve a certain problem. The procedure used to convert a plaintext to a ciphertext is called an encryption algorithm, while the inverse procedure is called a decryption algorithm. Both encryption and decryption algorithms are called a cryptographic algorithm.

Ancient Cryptography

① Scytale cipher

There are records of ancient Greek soldiers using the transposition cipher (a tool that changes the order of the letters) in 400 B.C. It is now called the Scytale cipher, shown in 〈Figure 3〉. In the Scytale, the diameter of the rod is the secret key shared only between the sender and the receiver.

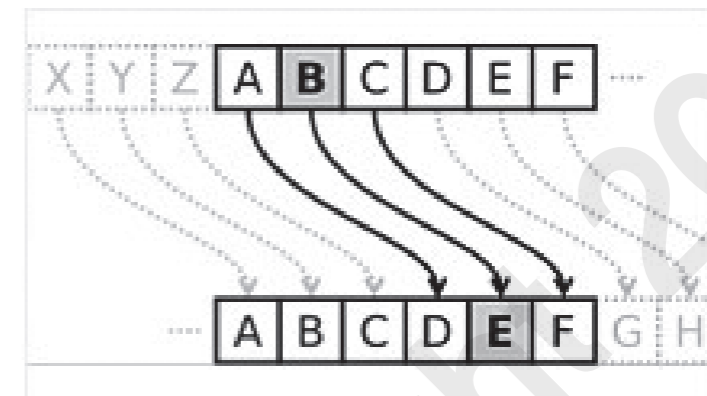


〈Figure 3〉 Scytale cipher

(Source: <https://seed.kisa.or.kr/iwt/ko/index.do>, "KISA "Facilitation of cryptography use")

② Caesar cipher

A Roman Emperor Julius Caesar used the Caesar cipher, which is also called a substitution cipher where letters are represented by other letters, in order to secretly communicate with his family. As shown in 〈Figure 4〉, a ciphertext is created in a way that each letter is replaced by the letter three places down the alphabet. The secret key shared between the sender and the receiver for the encryption is set to 'the number of letters to be relocated'. The decryption procedure is also performed based on this logic.



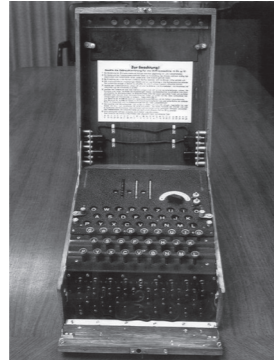
〈Figure 4〉 Caesar cipher

(Source: <https://seed.kisa.or.kr/iwt/ko/index.do>, "KISA Facilitation of cryptography use")

Modern Cryptography

Since the 20th century, many studies about cryptography had been conducted as there were growing needs for code–design and code–breaking during the First and Second World Wars, thanks to the development of communication technologies and research on mechanical calculators. In his paper, Claude Shannon proved that the one–time pad is perfectly secure. He also proposed the Theory of Confusion and Diffusion, the two basic principles used for the design of a cryptosystem. In the design of the cryptosystem, the 'confusion' hides the relationship between the plaintext and the corresponding ciphertext, while the 'diffusion' dissipates the statistical properties of the plaintext over the whole ciphertext in order to hide the plaintext. These two – confusion and diffusion – are important concepts that are still used in the current cryptosystem.

William Frederick Friedman is well known as a cryptographer who broke the German military's cipher, Enigma (shown in 〈Figure 5〉), and the Japanese military's cipher, Purple cipher, during the Second World War. The Enigma works in a way that the letters from a plaintext entered using an enigma machine (consisting of some different electrically–connected keyboards) are substituted by the letters in a ciphertext, based on the prescribed electric connection. Without the enigma machine, the encrypted text cannot be cracked.



(Figure 5) Enigma used by the German military

(Source: <https://seed.kisa.or.kr/iwt/ko/index.do>, "KISA Facilitation of cryptography use")

Contemporary Cryptography

The history of the contemporary cryptography began in the Stanford University and MIT in the late 1970s. In their paper, titled "New Directions in Cryptography", Diffie and Hellman of the Stanford University presented the concept of a public key encryption for the first time in 1976.

In 1978, Rivest, Shamir, and Adleman at MIT invented the RSA public key encryption which works based on the difficulty of prime factorization. It has been the most widely used public key mechanism up to today. The adoption of the public key encryption marked a significant milestone for the development of the contemporary cryptography.

Meanwhile, in 1977, the U.S. National Bureau of Standards (NBS, now NIST) issued a public request for proposals for a cryptographic algorithm to be used for computer data protection. As a result, IBM's DES (Data Encryption Standard) was adopted as a standard cryptographic algorithm.

These standardized cryptographic algorithms are embedded in the operating systems such as Windows, Linux, or Mac. The IPSec protocol (for Internet security) and the SSL/TLS protocol (for encrypting sessions between users) are some of the great examples using multiple cryptographic algorithms for information security in the communications system. Furthermore, the cryptographic technologies start to be used in various fields; mobile communications security between mobile phones, copyright protection, e-mail security, public key certificate, E-commerce, and E-government services.

① Symmetric key cryptosystem

In a Symmetric Key Cryptosystem, the same cryptographic key is used for both encryption and decryption. The symmetric key cryptosystem is powerful in that the length of the key does not have to be long and it runs fast for encryption and decryption. However, the biggest obstacle in successfully deploying the symmetric key cryptosystem is to make sure that keys are exchanged properly when the sender and the receiver are located at a distance. It is also difficult to create and manage different keys in a secure manner when there are many participants who want to join the encrypted communications. This mechanism is also called a secret key cryptosystem since the key should be stored and managed in a secret manner. It is also referred to as a conventional key cryptosystem since it has been used conventionally.

In the symmetric key cryptosystem, an algorithm is a combination of the substitution and the transposition, which

makes it faster to encrypt and decrypt data. Therefore, this cryptosystem is still widely used despite its difficulty in key sharing. As shown in (Table 1), the symmetric key cryptosystem is divided into Block Cipher and Stream Cipher, based on how data in the plaintext is converted.

(Table 1) Block cipher vs. Stream cipher

	Block Cipher	Stream Cipher
Mechanism	The plain text is divided into fixed length blocks and this block is encrypted one by one	The plain text is encrypted bit by bit
Strength	Easy to implement	Low error propagation Well suited for the mobile communications environment
Weakness	High error propagation Initial value required to be set	Slower in running Susceptible to modifications by attackers with malicious intentions

• Block cipher algorithm

In the block cipher algorithm, encryption and decryption are performed, using an algorithm that transforms 'fixed-length blocks of input' into 'fixed-length blocks of output', using a secret key. Feistel Network, DES (Data Encryption Standard), AES (Advanced Encryption Standard), IDEA (International Data Encryption Algorithm), SEED, and ARIA are examples of the block cipher algorithm.

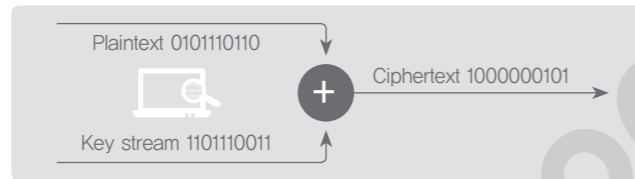
In the following (Table 2), main techniques of cryptanalysis applicable to block ciphers are described.

(Table 2) Block cipher cryptanalysis

Cryptanalysis technique	Details
Differential cryptanalysis	It is a chosen-plaintext attack. The idea of differential cryptanalysis is to compare the difference between bits in two plaintext blocks with the difference between bits in corresponding ciphertext blocks to infer the key used for encryption.
Linear cryptanalysis	It is a known-plaintext attack. The secret key is found out by approximating non-linear structures within the cryptographic algorithm
Exhaustive search attack	It is a technique of putting all of the possible keys in the plaintext and ciphertext pair until one works.
Statistical cryptanalysis	It is a technique of using all available statistical data, including statistics on the number of occurrences of letters/words of the plaintext appearing in the ciphertext.
Mathematical cryptanalysis	It is a technique of using statistical analysis and mathematical properties of the encryption algorithm in an attempt to decrypt data.

- Stream cipher algorithm

A Stream cipher, which was developed and advanced mainly in Europe, is a method of encrypting a text in which the key stream is XORed with a stream of plaintext bits to produce a ciphertext, as shown in (Figure 6). Unlike the block cipher in which encryption and decryption are achieved block by block, the stream cipher performs encryption and decryption bit by bit. RC4 is a stream cipher which is most widely used. A5/1 and A5/2 are other examples of algorithms used.

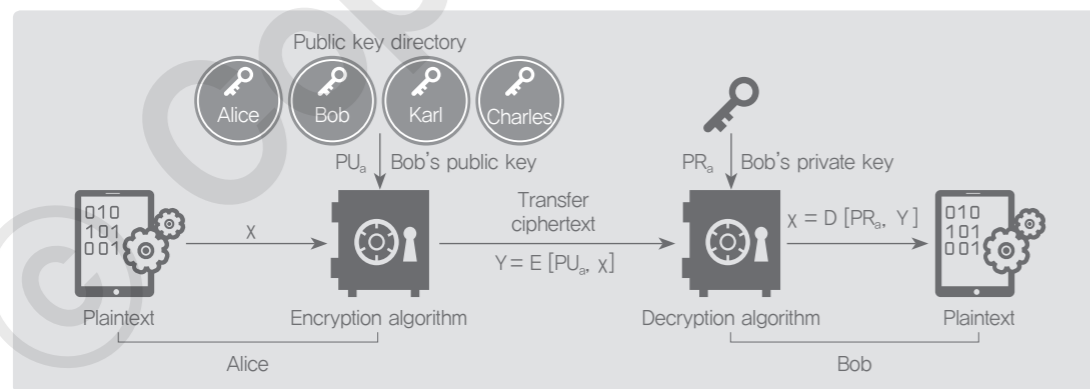


(Figure 6) Example of mechanism of stream cipher algorithm

② Public key cryptosystem

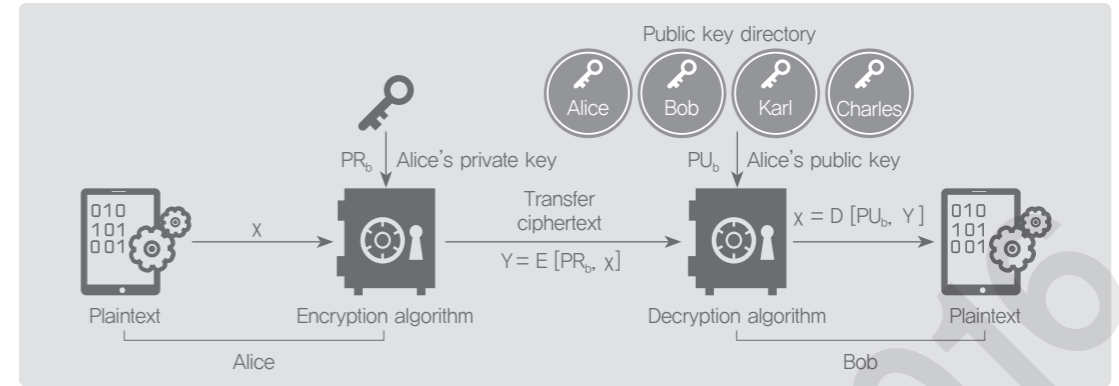
The concept of the public key encryption was first introduced by Diffie and Hellman in 1976, which was followed by the development of a practical public key cryptosystem, so called RSA, in 1978. Since then, the public key cryptosystem has played a significant role in the contemporary cryptography.

As shown in (Figure 7), the public key cryptosystem is a cryptosystem in which the sender and the receiver join in secure communications by using two different keys, as opposed to the mechanism of the secret key cryptosystem. The sender uses the receiver's public key to encrypt data and sends this encrypted data to the receiver over the network. The receiver then uses his/her matching private key (which is paired with the public key) to decrypt the encrypted data and recover the plaintext. (Figure 8) illustrates how the public key cryptosystem is applied in the authentication procedure (digital signature).



(Figure 7) Mechanism of public key cryptosystem

(Source: W. Stallings, Network Security Essentials, Pearson, p.80)



(Figure 8) Use of public key cryptosystem for authentication

(Source: W. Stallings, Network Security Essentials, Pearson, p.80)

The merit of the public key cryptosystem is that there is no need for the exchange of keys between users who wish to communicate with one another in a secure way. The key to be used for sending the message to the user (called a public key) is publicly known. The key used for decrypting the information encrypted with their public key (called a private key) is kept as a secret. Therefore, the information can be encrypted by anyone, whereas the encrypted information can be decrypted by a user who has the corresponding private key. Let's take an example: suppose there are N number of users, each of whom wanting to communicate with the others over the network. On this entire network, the total number of the keys required equals $2N$, because each user needs a pair of 2 keys – a public key and a private key. For each of the users, he/she needs only these two keys to make the data communications possible.

The primary disadvantage of the public key cryptosystem is that it is less efficient than the symmetric key cryptosystem in computation. In public the key cryptosystem, however, a public key is available to anyone while a matching private key is a secret known only to a specific user. Hence, this encryption mechanism can be applied to various authentication functions and the secure exchange of keys. RSA (Rivest, Shamir and Adleman), ElGamal, and ECC (Elliptic Curve Cryptosystem) are the examples of the most widely used public key encryption algorithms.

- RSA

RSA is one of the public key cryptosystems that is used for encryption and authentication. The RSA security mechanism is based on the difficulty of factoring large integers. Since a random number is not employed in the process of encryption, a ciphertext output converted from the same plaintext is always identical. The security of the RSA is based on keeping two prime numbers – p and q – as a secret, so the prime numbers should be carefully chosen.

The following shows how key generation, encryption, and decryption works within the RSA cryptosystem.

1) Key generation

- Choose two distinct prime numbers, p and q , and compute $n=pq$
- Compute $\phi(n) = (p-1)(q-1)$
- Choose an integer e which is coprime to n and computed which satisfies $de=1 \pmod{\phi(n)}$
- (n, e) is published as a public key and (n, d) is kept as a private key

2) Encryption
 – To encrypt m (a message to be encrypted), compute $c = m^e \cdot \text{mod } n$, using (n, e) (the receiver's public key)

3) Decryption
 – To decrypt c (a ciphertext received), compute $m = c^d \cdot \text{mod } n$, using (n, d) (the receiver's private key)

- ElGamal
 ElGamal cryptosystem is the first public key encryption algorithm which is based on the difficulty of finding a solution to the discrete logarithm. It was first introduced by T. ElGamal, a cryptographer of the Stanford University in 1984. Under the ElGamal mechanism, a ciphertext is twice as long as a plaintext. However, the mechanism provides a powerful benefit from the information security perspective: random numbers are used during the encryption process, so a ciphertext converted from the same message is always different.
- ECC
 Elliptic Curves Cryptography, or ECC, is designed based on the difficulty of finding a solution to the discrete logarithm of the elliptic curves. It has emerged as one of the best public key encryption algorithms since it is very secure and fast. For example, ECC needs a 160-bit key to yield the same level of security with a 1,024-bit key of the RSA cryptosystem. ECC is now getting attentions as the next-generation public key cryptosystem, because it is well suited as an encryption algorithm for the devices with limited power source such as mobile communications devices (cell phone).

<Table 3> shows a comparison of the symmetric key cryptosystem with the public key cryptosystem.

<Table 3> Symmetric key cryptosystem vs. Public key cryptosystem

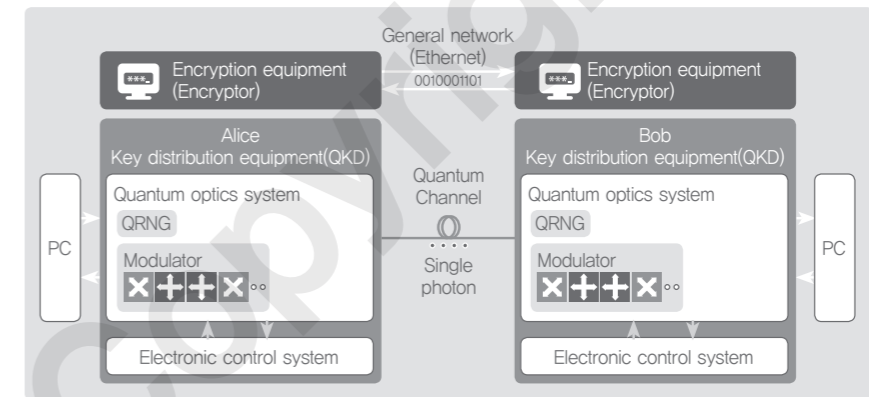
	Symmetric key cryptosystem	Public key cryptosystem
Relationship between keys	Encryption key = Decryption key	Encryption key \neq Decryption key
Encryption key	Not open	Open
Decryption key	Not open	Not open
Algorithm	Open	Open
Number of keys	$n(n-1)/2$	$2n$
Number of keys required to be managed by each	$n-1$	1
Encryption speed	High	Low
Authentication (Digital signature)	Complex	Simple
Strength	<ul style="list-style-type: none"> • Fast encryption/decryption • The key length is short. 	<ul style="list-style-type: none"> • Easy key distribution • The number of keys required to be managed is small. • Widely applicable to various fields, such as authentication

	Symmetric key cryptosystem	Public key cryptosystem
Weakness	<ul style="list-style-type: none"> • The number of keys required to be managed increases as the number of users increases. • High frequency in key changes 	<ul style="list-style-type: none"> • Slow in encryption/decryption • The key length is long. • Low frequency in key changes

③ Quantum Cryptography

Quantum Cryptography, which was proposed by C. H. Benett and G. Brassard in 1984, is a cryptosystem that supports secure communications, based on the natural laws of quantum. It is one of the most ideal ways to generate a one-time pad that is used for encryption. In the quantum cryptography, eavesdropping attempts on quantum signals are detected and it results in signal distortion, so that the eavesdropper cannot get correct information. It is also called the Quantum Key Distribution system. In the quantum cryptography, communications are secured, using the quantum key distribution and cryptographic communications. The quantum key distribution refers to a technique that uses quantum mechanics to enable the sender and the receiver to share a secret key in an absolutely secure way.

As shown in <Figure 9>, the quantum cryptography is divided into Quantum Key Distribution (QKD) and encryptor. The QKD uses the features of quantum to enable the sender and the receiver to securely share a secret key. The encryptor performs the data encryption and decryption, using the shared secret key to enable cryptographic communications. In general, the quantum cryptography represents only the quantum key distribution.



<Figure 9> Mechanism of quantum cryptographic communications

Key Exchange Algorithm

The secret keys should be exchanged securely, and this is a prerequisite for using a symmetric key cryptosystem. In other words, the symmetric key cryptosystem can work only when the secret key is securely shared among the authorized parties, and a key exchange algorithm is employed in this procedure.

Two of the most common key exchange algorithms are: Diffie-Hellman Key Exchange and RSA. In the RSA, a public key should be shared between users. On the other hand, in the Diffie-Hellman Key Exchange, you do not have to know the public key of the counterpart. However, the Diffie-Hellman Key Exchange by itself cannot identify the

legitimacy of the counterpart, so a proper process should be in place for the user authentication.

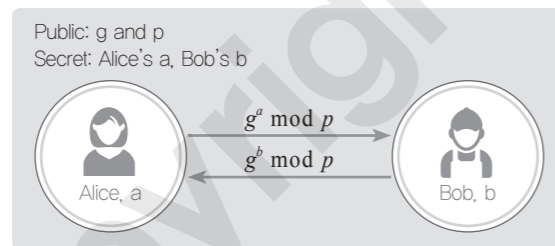
① Diffie–Hellman Key Exchange

⟨Figure 10⟩ briefly illustrates how the Diffie–Hellman Key Exchange works when Alice and Bob join in the communications over a public network. The detailed procedures are laid out, as follows.

- 1) Alice chooses a prime number p and an integer g (from 1 to $p-1$). Then, Alice shares these two with Bob.
- 2) Alice chooses an integer “ a ”. She keeps the integer as a secret from everyone, including Bob.
- 3) Alice computes $A = g^a \bmod p$, which equals to the remainder when g^a is divided by p .
- 4) Bob also chooses an integer “ b ” and computes $B = g^b \bmod p$.
- 5) Alice sends A to Bob and Bob sends B to Alice.
- 6) Alice computes $B^a \bmod p$ and Bob computes $A^b \bmod p$.

In the final step, $B^a = (g^b)^a = g^{ab}$ and $A^b = (g^a)^b = g^{ab}$. Therefore, the secret key $g^{ab} \bmod p$ is shared between Alice and Bob. In other words, the value of $g, p, g^a \bmod p, g^b \bmod p$ can be used as the secret key for the symmetric key encryption.

A and B are not available to anyone, except Alice and Bob, while $g, p, g^a \bmod p, g^b \bmod p$ may be available to all.



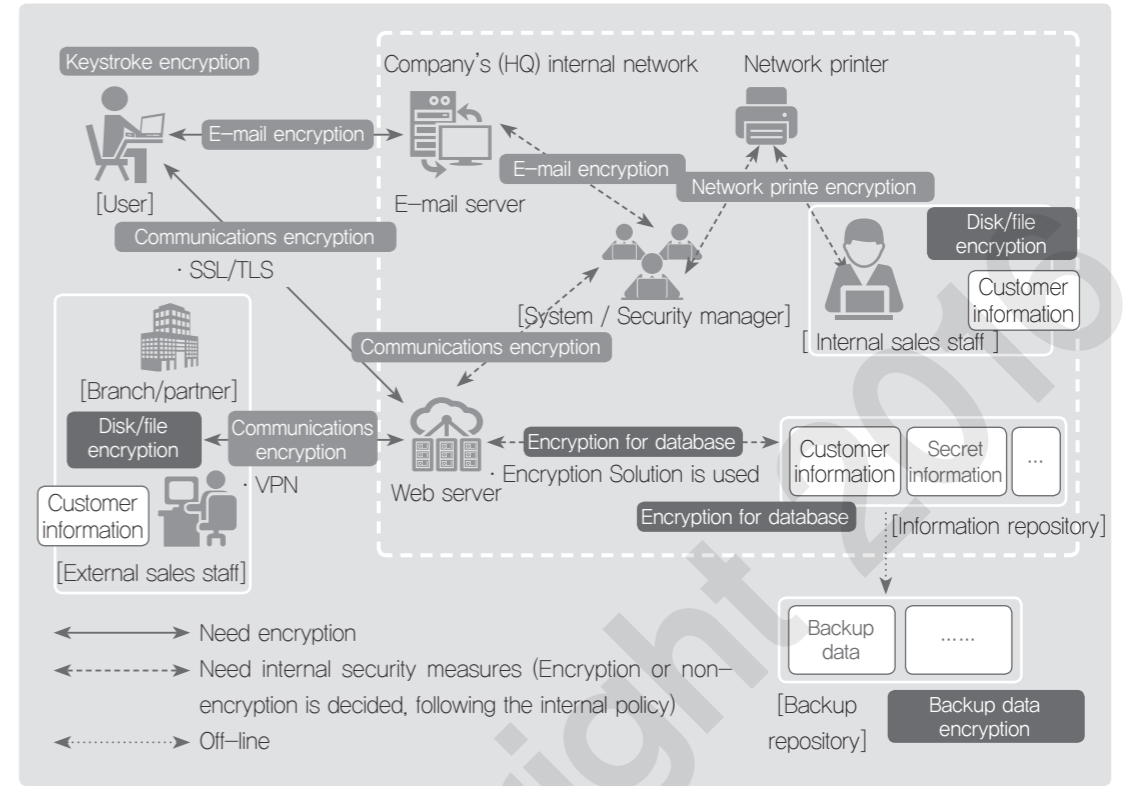
⟨Figure 10⟩ Diffie–Hellman key exchange

② RSA key exchange

With the RSA algorithm, the process of sharing a secret key between Alice and Bob for the symmetric key encryption is very simple. As shown in ⟨Figure 7⟩, Alice and Bob agree on a value for the secret key which they share with one another. The value is encrypted by using Bob's public key and sent to Bob. Bob uses his own private key to decrypt it and get the secret key. This is how they share the secret key.

Use of Cryptographic Technologies

A variety of cryptographic technologies can be used in each phase for storage, management and transmission of information. ⟨Figure 11⟩ shows what cryptographic technologies are applied to each phase of information use within a company that provides network services that enable external users, branches, and partners to have access to the HQ network via email servers and web servers.



⟨Figure 11⟩ Example of cryptographic technologies used in each phase of information use

① Storage & management phases

• Encryption for disks

If computing devices (e.g. PDAs, smart phones and laptops) and storage media (e.g. CDs, DVDs and USB devices) are not located in a secure place, information stored in such devices and media are highly likely to be exposed to or destroyed by unauthorized parties who attempt to use such information with malicious intentions. In particular, the leakage of information which is caused by the theft of laptops or other mobile devices has emerged as the main causes of information exposure of companies. In this regard, it is of significant importance to encrypt parts of or the whole disks of such computing devices and storage media in order to protect information stored in them.

Management of cryptographic keys is a vital part of disk encryption. A careful and thorough management of cryptographic keys is essential, since data cannot be recovered from the encrypted disk if the key is lost without any back-up and copied data. The integrity of keys and places for key storage should be also guaranteed. If not, in other words, if they are manipulated or destroyed, the encrypted data cannot be recovered. Therefore, keys and places for key storage should be secured through encryption or access control.

• Encryption for files

File encryption encrypts an individual file not only to protect information stored in the file, but also to transmit the file securely over the network. In a network environment which does not support secure communications, the

file itself should be encrypted to make sure that the sender can securely transmit the information.

Like in the disk encryption, careful management of encryption keys is all the more important in the file encryption. In particular, if unauthorized parties obtain an encrypted file and a secret key used to decrypt the file during the transmission of the encrypted file, the information stored in that file can be exposed. In this regard, there are rising needs for finding a way of securely sending decryption keys to the receiver.

- Encryption for database

Database encryption is designed to encrypt and store the important information residing in a database, such as customers' personal information or companies' confidential information. The purpose of database encryption is to protect the data stored in a database from being modified or acquired by unauthorized parties.

Data encryption is achieved by the DBMS (Database Management System) and Database Encryption Solution (Hereinafter, called Encryption Solution). The former is designed to manage and control a database, while the latter is specifically designed to provide a solution for database encryption.

- Encryption for backup data

Copies of confidential data which are used for back-up and data retention should be protected. Since a storage medium for backup and data retention can be accessed by unauthorized parties, encryption is essential to protect such confidential data.

Whether to encrypt backup data is determined by the type of storage media for backup or backup solutions. More importantly, a medium for back-up is a space for the copied version of data which is required to be encrypted. To decide whether to encrypt backup media, not only the sensitivity of the data, but also the status of physical and technical security measures employed in the storage place should be considered.

② Transmission phase

- Encryption for keystrokes

Keystrokes encryption is designed to encrypt important personal information (e.g. ID, password, account numbers, card numbers, etc.) that is input (typed-in) through a keyboard, in order to protect the important information from being leaked by keystroke hacking programs. The attacks of keystroke hacking programs can be prevented mainly by a mechanism in which keyboard input data is encrypted and transmitted through a different transmission path, instead of following the existing flow of keyboard data.

Keystroke encryption solution should be able to provide real-time and system-level keyboard input encryption, using secure algorithms and keys.

- Encryption for electronic mail

E-mail encryption means to encrypt e-mail messages sent and received in order to protect the contents of the email from being leaked. An e-mail service is prone to disclosure or manipulation of e-mail messages by unauthorized attackers during the transmission over the network, e-mail relays, or the process in which a user sends/receives an e-mail over the network in mail servers, such as IMAP or POP3.

In the e-mail encryption, a system or security administrator is required to consider requirements from users, such as a company or institute, their business environment, and the potential scenarios to determine whether to encrypt an e-mail and if so, to which extent the encryption should be applied.

- Filtering of an encrypted e-mail is costly, since the contents of the e-mail are filtered through mail servers or firewalls in order to detect a virus or a malicious program embedded in the e-mail.

- Without any encryption functions provided from a mail server or a firewall, an e-mail cannot be filtered, resulting in errors during the transmission of the message.
- Additional upgrade of devices is required to support e-mail encryption/decryption.
- It demands continuous management in key distribution, recovery, and revocation for e-mail encryption.
- Encrypted e-mail contents cannot be read or understood when it is required to investigate the contents in accordance with internal rules of a company/institution or laws.

- Encryption for communications

The client-to-web server and server-to-server communications happening on the public network like the Internet need a protection mechanism for the information exchanged. Cryptographic technologies, such as SSL/TLS or VPN, can be used to protect the communications process.

- Encryption for printers connected to the network

There is increasing number of companies that use a multi functional office devices (printer + copy machine + fax + scanner) connected to the network so that many employees can share the same device. As a result, the printers connected to the network have emerged as a security issue.

When any confidential information is printed through the printers connected to the network, the information leakage on the network is highly likely to take place and even unauthorized internal users can have access to the physical documents that have been printed out. Therefore, it is recommended to use printers that can support network traffic encryption and user authentication feature.

In addition, internal risks can be more detrimental rather than the risks from attackers, because printers connected to the network can have some connection errors, which can make printed documents exposed to the internal users who are not intended to or unauthorized to acquire the information.

Encryption and Decryption of Java Language

Mr. Kim decided to use AES, a kind of symmetric-key algorithm, in Java programs to store and utilize the important information securely. In this chapter, we will study how the Java language encryption and decryption works.

To apply the AES encryption and decryption in the Java language, 'javax.crypto' package is used. The first step is to import the related classes and packages. (Figure 12) is an example of the AES encryption and decryption in the Java language.

```
package CipherTest;

import java.security.*;
import javax.crypto.*;
import javax.crypto.spec.*;

public class CipherAES {

    public static void main(String args[]) {
        try {
            // to generate a symmetric key for encryption and decryption
            KeyGenerator kg = KeyGenerator.getInstance("AES");
```



```

Key key = kg.generateKey( );
// to generate a Cipher object for encryption and decryption

Cipher c = Cipher.getInstance("AES/CBC/PKCS5Padding");

// to initialize the Cipher object for encryption
c.init(Cipher.ENCRYPT_MODE, key);

// data preparation for encryption
byte input[] = "critical data which requires confidentiality".getBytes( );

// encryption processing
byte encrypted[] = c.doFinal(input);
byte iv[] = c.getIV( );

// to initialize Cipher object for decryption
IvParameterSpec dps = new IvParameterSpec(iv);
c.init(Cipher.DECRYPT_MODE, key, dps);

// decryption processing
byte output[] = c.doFinal(encrypted);

// to print out the outcome
System.out.println("plain text : " + new String(input));
System.out.println("encrypted text : " + new String(encrypted));
System.out.println("decrypted outcome : " + new String(output));
} catch (Exception e) {
    e.printStackTrace( );
}
}
}

```

⟨Figure 12⟩ Java AES program source code

The following is the detailed explanation about the key steps of encryption used in ⟨Figure 12⟩.

- Generating a symmetric key: the `getInstance` method of the `KeyGenerator` class is used to generate a symmetric key to be used in the encryption process and the parameter selected is 'AES'. By using the generated `KeyGenerator` object, the `generateKey` method is called in order to generate the key to be used in encryption and decryption.
- Generating an object to carry out encryption: the object `c` (for encryption and decryption) is generated by using the `getInstance` method of `Cipher` class and parameter values. The parameter 'AES/CBC/PKCS5Padding' specifies cryptographic algorithm/block cipher algorithm operation mode/padding.
- Initializing the object to carry out encryption: the `init` method of object `c` is for initializing the object `c` that was generated for data encryption or decryption and the key must be provided in this process. If the selected algorithm is based on the symmetric key, a secret key should be assigned. If the selected algorithm is based on the symmetric key, a secret key should be assigned and if the selected algorithm is based on the public key, a

public key should be assigned for encryption and a private key should be assigned for decryption. This method carries three parameters: the first parameter is about the type of mode and encryption was selected here; the second parameter is about the key to be used in encryption or decryption; and the last parameter is algorithm parameter specification and the `IvParameterSpec` class is usually used.

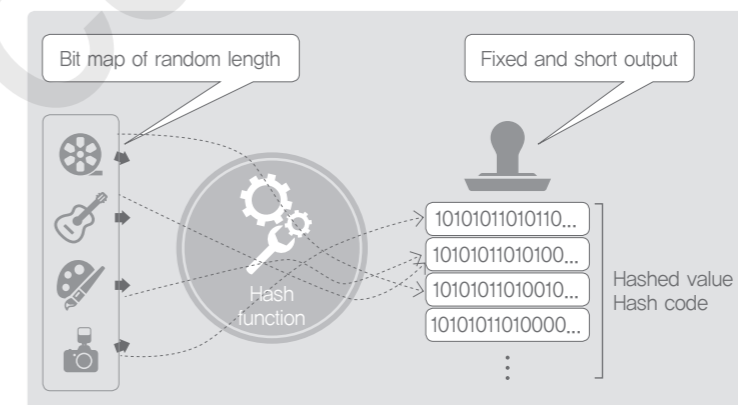
- Carrying out encryption: once the object `c` is initialized, actual target data is put in for encryption processing and the outcome of encryption is stored in the array. In this example, only one parameter (encryption target data) is selected in the `doFinal` method.
- Extracting the initialization vector: the IV (Initialization Vector) which was generated in the CBC (Cipher Block Chaining) encryption process is extracted by using the `getIV` method for the decryption process

Note) 'openssl' library is usually used for the AES in the 'C' language. You can download the most recent version from '<http://www.openssl.org>' site and use it after declaring '#include <openssl/aes.h>'.

02 Hash Function

Definition and Characteristic of Hash Function

A Hash Function or Hash Algorithm, as shown in ⟨Figure 13⟩, is a mathematical function that can be used to map the data of arbitrary size to the data of fixed size. The values returned by a hash function are called hash values or hash codes. In other words, the hash function is designed to summarize a bit string of arbitrary size into a short and fixed one. For example, HAS-160 (Hash Algorithm Standard 160) and SHA-1 will print out the result with 160 bits. Cryptographic algorithms rely on keys, but hash functions do not use keys. That means if the input value is identical, the outcome will be always the same (single outcome). One of the reasons for using such as a function is to ensure data integrity by extracting an evidential value for input messages that cannot be changed, thereby detecting errors in messages or modification to them.



⟨Figure 13⟩ Conceptual diagram of hash functions

The hash function, generally expressed as $h(x)$, is deterministic in its nature. In other words, if the hash value is different, the original data is supposed to be different; and output is always the same for an identical input value. The output values, in their nature, are evenly distributed as much as possible.

As the range of output value is smaller than that of the input value, in some cases, different input values may result in same the output incidentally. This case is called the Hash Collision, which means that the same hash value does not always have the same original input values. Almost all the hash functions developed so far have been proven to have hash collision issues and SHA-3 is the only one that does not have any proven hash collision as of now.

As the algorithm for hash functions is simple (a function h works on calculation of input value x), it consumes relatively less resources such as CPU and memory. In order to achieve functional stability, hash functions should meet the requirements described in (Table 4).

(Table 4) Basic requirement of hash functions

Property	Details
Preimage resistance	• When y is given, it should be hard to identify x that meets $h(x)=y$
Second preimage resistance	• When x and y are given to meet $h(x)=y$, it should be hard to identify x' that meets $h(x')=y$. ($x \neq x'$)
Collision resistance	• It is hard to identify x and x' ($x \neq x'$) that meet $h(x)=h(x')$.

The original text can never be restored just by using the hash value and that is why hash functions are used widely in security related works. In other words, it is not computable to restore the original text only from the hash value.

Hence, hash functions are used to store sensitive information, such as passwords, in a safe manner. However, there is a possibility of detour attack that exploits hash collision.

Types of Hash Functions

① MD5 (Message Digest Algorithm 5)

MD5 is a kind of hash functions which is used to verify integrity of files or programs and produces a 128-bit hash value. The formulation is specified in RFC 1321, IETF, but a series of major defects were found.

MD5 is usually used for passwords; a password hashed using the MD5 and the resulting value is stored. This means that a server operator or a third party cannot know the original password just with the hash value stored in the system. If a user types in an accurate password, the same hash value will come as an outcome all the time, which makes it possible to verify whether the password is valid or not.

② SHA (Secure Hash Algorithm)

SHA was further developed from the MD5 and refers to a set of cryptographic hash functions. The SHA was designed by the NSA for the first time in 1993 and later selected as a national standard of the US. The first formulation of the SHA is called as the SHA-0 to make it differentiated from other functions. The SHA-1, an

upgrade from the SHA-0, was announced after two years. Later, the SHA-2 families were introduced such as SHA-224, SHA-256, SHA-384, and SHA-512. The SHA-3, which is totally different from the SHA-1 and 2, was developed and the SHA-3 was selected in 2012.

SHA-0 and SHA-1 produce 160-bit hash values and the SHA-224/256/384/512 produces 224/256/384/512-bit hash values respectively. In addition, the SHA-256 or higher is recommended for safe hashing. The attacks specific to the SHA-2 were not found yet, but there is likelihood to find possible attacks since the SHA-2 functions use a similar mechanism with the SHA-1.

③ Supplementation for hash function

- Weak points of hash function

The following process is deemed to be secure enough in most of the websites: an account is generated with a password; the password is hashed through a hash function; the hash value is stored and compared against the hash value generated from the password a user typed in during the log-in process. However, there are two vulnerabilities involved in that mechanism.

(1) Recognizability

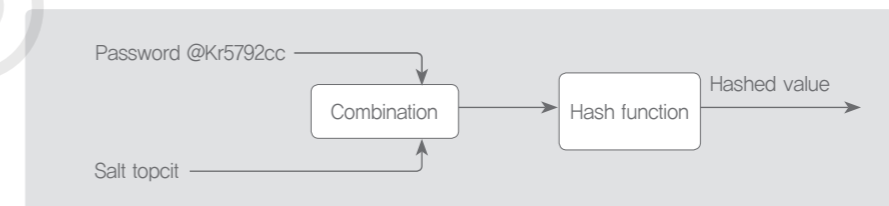
If the same message can generate the same hash value all the time, an attacker can acquire pre-computed hash values as many as possible and then compare those values along with the stolen hash values to find out the original message or a message that can generate the same effect. Such a digest list is called the Rainbow Table and an attack using the aforementioned mechanism is called the Rainbow Attack. To make matters worse, if two or more users have the same password, the hash value of the password for those users will be identical. Hence, many users' passwords may be stolen at once.

(2) Speed

Hash functions, from the beginning, were not intended to store passwords safely, but to search data in a short amount of time. As hash functions are speedy, attackers can compare the hash value from a random string against the hash value of the hacking target in a short period of time. If assumptions and trials are repeated, it does not take a long time to break the password unless the password is long or complicated enough. To make matters worse, most users do not use long or complicated password and even they use the same password in some cases.

- Supplementing hash functions using Salt

A salt is a random data that is used as an additional input to a hashing process. In other words, salting means to add additional bits to the original message and generate a hash value. For example, as shown in (Figure 14), "topcit" can be added to the original password "Kr5792cc" to generate a hash value.



(Figure 14) Salting

Even though an attacker finds out the corresponding hash value for "@Kr5792cc", the attacker will face difficulties to find out the password match for the new hash value generated from salting. In addition, if different salts can be used for each of the users, even the users who have the same password will end up with different hash values. This method will be significantly helpful in resolving recognizability issues.

Hash values of salts and passwords can be stored in the database of a server and the typed-in password can be hashed on the spot to validate the password match. Each of the passwords should have a unique salt when using this method and it is known that the salt length should be longer than 32 bytes to make it hard to predict salt and digest.

Application of Hash Function

① Integrity verification

In the area of server or network security, methods of integrity verification can be divided into: to detect errors in the process of data transmission; or to prevent arbitrary changes, as shown in (Table 5). In the case of integrity verification to detect errors in the process of data transmission, there are Checksum and CRC (Cyclic Redundancy Check) methods. The checksum is a kind of redundancy test to verify integrity, which gets the checksum value by adding all the data and translates the value into a certain bit value to be added on the message.

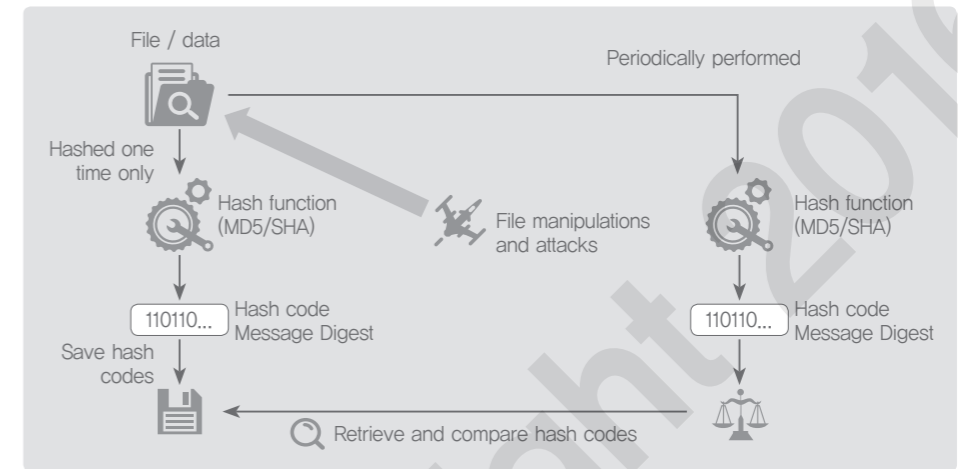
CRC is usually used for detecting errors occurring in the process of data transmission in communications systems such as the Internet. It works based on the polynomial expression that can be useful for error detection and correction. On the transmission side, polynomial calculation is made to get the checksum and adds it onto the header, and then the receiving end calculates checksum again based on the same polynomial expression so that the checksum from two ends can be compared for the verification of integrity.

(Table 5) Integrity verification methods

Cause of modification	Solution
Data transmission error	<ul style="list-style-type: none"> • Checksum • CRC <ul style="list-style-type: none"> ✓ To verify data ✓ Fixed length numeric value is generated
Arbitrary modification	<ul style="list-style-type: none"> • Hash functions <ul style="list-style-type: none"> ✓ MD5 <ul style="list-style-type: none"> - Expansion of CRC - Supplement to MD2~4 - 128-bit hash function - SHA-1 is recommended ✓ SHA-1 <ul style="list-style-type: none"> - MD5 alternative and expansion - Used in security protocols and programs ✓ SHA-2 <ul style="list-style-type: none"> - Refers to SHA265~512 - Existing attack mechanism against SHA1

② File integrity

Mr. Kim can use a hash function in transmitting a file on the Internet or uploading a file onto a homepage. He can get a hashed value and send it along with the file to make sure that the file is not manipulated. As for the critical source files that Mr. Kim managed in the server, he created a list and saved the hash value for each of the files. He can bring the hash value for each file on the list with a certain time interval and compared the value with the original hash value to make sure that the file is not manipulated, as shown in (Figure 15).



(Figure 15) Server file integrity test

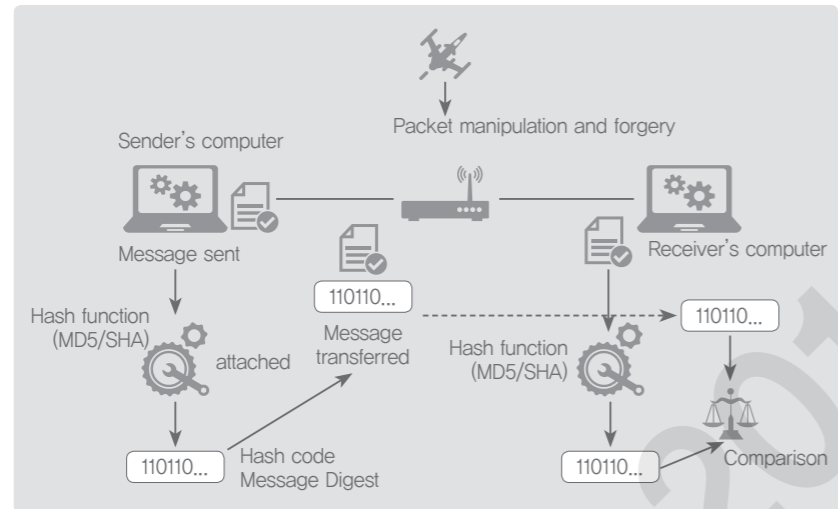
However, such a periodic integrity test cannot find out any security breach that might have occurred in between the two tests, it could have been better if the test were performed more frequently. However, it is not effective because making hash values for many files and comparing them frequently will increase load on the server.

The alternative for the periodic integrity test is to adopt a kernel-level real time detection method. In other words, the integrity test is conducted only once in the beginning and the real time testing is conducted every time a file is run or loaded onto the memory to detect any file manipulation. This effective way can manage the CPU load and even prevents manipulated files from being loaded onto the memory.

③ Integrity in the process of transfer

Message integrity on the network is one of the key security concerns. As shown in (Figure 16), a hacker can hijack the message in the middle and manipulate the message. To make sure that the delivered message is not manipulated, the sender should create a hash value for the message and send it along with the message. The receiver should run the integrity test upon receiving the message and can ignore the message if it turns out to be manipulated.

In the case when the sender ID does not have to be authenticated and only integrity (not manipulated) during the transfer process needs to be verified, a hash function can be used as a MAC: Message Authentication Code. This means the sender's message input is used to calculate a hash value and the hash value is used as a MAC. If the MAC can be sent along with the message, the receiver can be assured that the message was not modified in the middle of the transfer.



(Figure 16) Integrity test for transferred file

④ Password-based encryption

Both hash functions and encryption can be effective in hiding passwords, but there is a certain difference between the two. Encryption algorithms can turn a plain text into an encrypted text and decrypt it later. However, in hash functions, it is not possible to find out the original value just based on the hashed value.

Hash functions can be used in the PBE (Password Based Encryption). In the PBE mechanism, the encryption key is the hashed value from a function that uses "password + salt (output of a random number generator)" as an input. This mechanism can be helpful in preventing password-related attacks.

⑤ Digital signature

Hash functions can also be used as a digital signature. A signatory can work on the hash calculation by using his/her private key in order to guarantee integrity and authentication (of a signatory) at the same time. To sign on all the messages is ineffective in that public key calculation should be repeated in every message block. Hence, a better way to create an effective digital signature is to calculate a hash value for a message and a signature can be put on the hashed value. The signatory signed on the hashed value not on the message, but it is hard to find another message that carries the same hash value. In that sense, this signature can be accepted as the signature for the message.

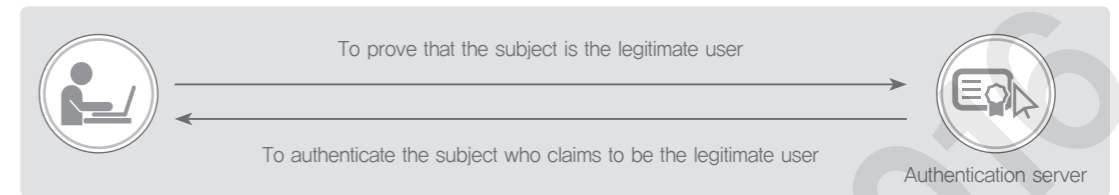
03 Authentication Technologies

Concept of Authentication

Authentication means a way to verify: whether the information between a sender and a receiver was manipulated or

deleted; and the information is exchanged between legitimate senders and receivers. Therefore, authentication can be categorized into message authentication and user authentication.

User authentication means that a user proves that he/she is a legitimate user to the counterpart located on the opposite side of the network, as shown in (Figure 17). That means it should not be possible for a third party to impersonate an authentic user.



(Figure 17) User authentication

Message Authentication means to verify that the contents of the message were not manipulated and left as they were. The integrity of the message and the authenticity of users can be verified at once if you use a digital signature. User authentication is sometimes called an identification, which is used to identify a user and to bestow authority to use a certain service when the user logs-in to the server. A remote user can fully enjoy all the authority given to the user once user authentication is completed, so the server side (service providers who provide important services) should apply a stringent authentication process to remote access users.

User authentication, in which a user verifies its identity to the server, can be achieved based on three factors: knowledge (what you know), possession (what you have), and biometric factors (who you are).

① Knowledge-based authentication

This authentication method works based on "what you know"; PIN (Personal Identification Number), password, account number and the like.

② Possession-based authentication

This authentication method works based on "what you have"; OTP (One Time Password), smart card, card key, and the like.

③ Biometrics-based authentication

This authentication method works based on "what you are", especially a certain body part or a person's physical characteristics, such as iris, fingerprint, voice, face and the like.

Major Authentication Methods

① Password

• Introduction to password

A user can define his/her password and the defined password is compared against the password a user typed in to authenticate a user. This method is most widely used, but is the most vulnerable technology at the same time, as shown in (Figure 18). Therefore, it is necessary to pay keen attention when using the password-based authentication.



(Figure 18) Vulnerability of password-based authentication

- Password policy
 - Creation of a password: a password should be longer than 8 digits with the combination of lower case and upper case letters, numbers, and special characters and it should be easy to remember for users and hard to assume for attackers.
 - Storage of a password: a password should not be stored in plain text or bidirectional encryption algorithm, but it should be stored with a hash function.
 - Usage of a password: an authentication system should set a limit for the invalid password attempts (account lockout)
- Types of attacks targeting passwords and responses
 - Attacks targeting password: Brute Force Attack, Dictionary Attack, Trojan Horse, direct access to password file, and social engineering attack.
 - Responses: to use a password generator, to limit the number of invalid password attempts, to periodically change passwords, to use the IDS (Intrusion Detection System) against Brute Force Attack and Dictionary Attack, to train users for security awareness, and to use OTP and other physical devices.

② OTP-based authentication

- Introduction to OTP

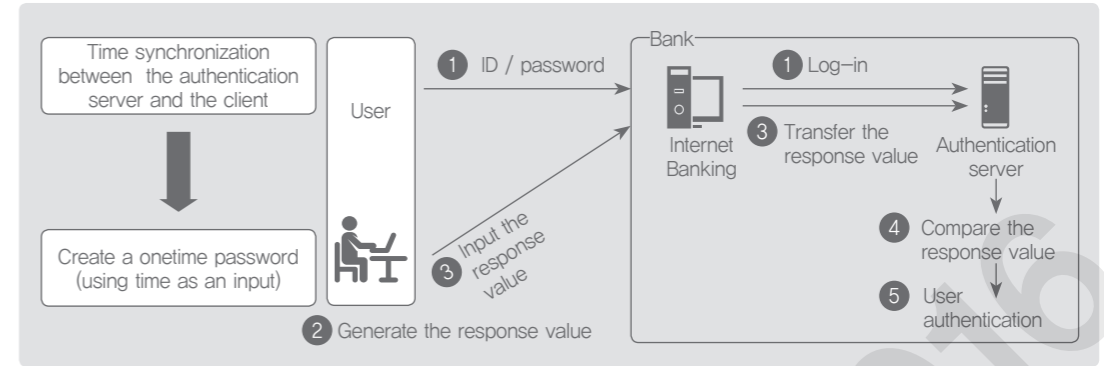
OTP is a user authentication technology used in the authentication system; a device generates a one-time password for every session, so that a user can type in the password.
- Types of OTP

OTP can be categorized into Sync-type and Async-type, as shown in (Table 6).

(Table 6) Types of OTP

	Classification	Details
Sync	Challenge-Response	An authentication server generates a random number and sends the number to the client to generate a one-time password, using the random number as an input
	Time-Synchronous	The time is synchronized between the authentication server and the client, and a one-time password is generated, using the time as an input
Async	Event-Synchronous	The authentication counter is shared with the authentication server. Then, it is used as an input to generate a one-time password.

The mechanism of action for time-synchronous OTP is described in (Figure 19).



(Figure 19) Mechanism of action for time-synchronous OTP

③ Biometric authentication

- Introduction to biometrics

Biometrics-based authentication is the process of extracting measurable biological or behavioral characteristics, by using an automated sensor, for the purpose of uniquely identifying or authenticating an individual.
- Requirement for biometric factors
 - Universality: everyone using a system should possess the trait
 - Uniqueness: the trait should be sufficiently different from individuals in the relevant population such that they can be distinguished from one another
 - Measurable: the trait should be able to be measured and quantified
 - Permanence: the trait should not be changed and should be permanent
 - Accuracy: the trait should be accurate all the time without being impacted by circumstantial changes
 - Acceptability: how well individuals accept the technology such that they are willing to have their trait captured and used
- Types of biometrics-based authentication

There are two types of biometric authentication, as shown in (Table 7): using biological factors or behavioral characteristics.

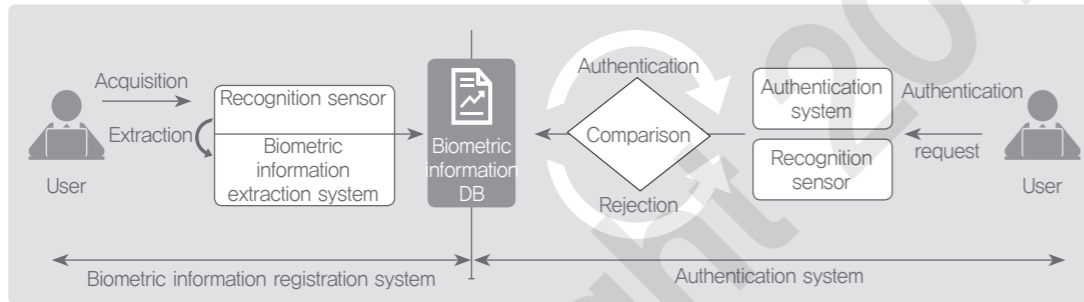
(Table 7) Types of biometric authentication

Classification	Type	Details
Biological factors	Fingerprint	Highest market share: semi-conductor, optical, hybrid
	Iris	Very accurate and runs fast, but requires an expensive authentication system
	Face	Face has a lot of information to be used for authentication and it is the most natural way of authentication
	Vein	Shape of veins is read to be used as a pattern for authentication
	DNA	Most accurate method

Classification	Type	Details
Behavioral factors	Signature	Signature can guarantee a certain pattern: not only a unique style or shape but also hand move patterns.
	Voice	Usually used in physical access control applications

• Process of biometric authentication

The mechanism for biometric authentication can be implemented with a 'biometric information registration system' and 'biometric authentication system', as shown in (Figure 20). The biometric information of users is stored in a database first and the stored information is compared against the biometric information extracted from the user at the moment of user authentication.

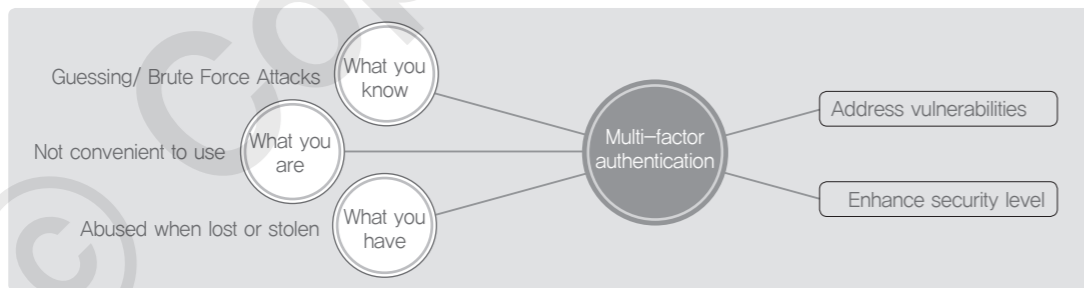


(Figure 20) Process of biometric authentication

④ Multifactor authentication

• Introduction to multifactor authentication

Multifactor authentication literally means to combine two or more authentication factors to surmount the weakness of single factor authentication and to make the authentication process more secure as shown in (Figure 21)



(Figure 21) Concept of multifactor authentication

• Use cases of multifactor authentication

Typical example of multifactor authentication can be found in the Korean banking system. In the case of on-line banking, different security level is assigned to different activities and transactions, wire transfer limit is differentiated based on the given security level, and various other authentication methods are applied. The security level and the factors used in each level are explained in (Table 8).

(Table 8) Cases of multifactor authentication

Security level	Factors used
First level	OTP + Public key certificate
	HSM public key certificate + Security card
	2-channel authentication+ Security card + Public key certificate
Second level	Security card + Security SMS + Public key certificate
Third level	Security card + Public key certificate

To build a stronger multifactor authentication system, knowledge, possession, and physical factors should be combined, just like in the case when an OTP and fingerprint are used together.

Digital Signature

① Definition of digital signature

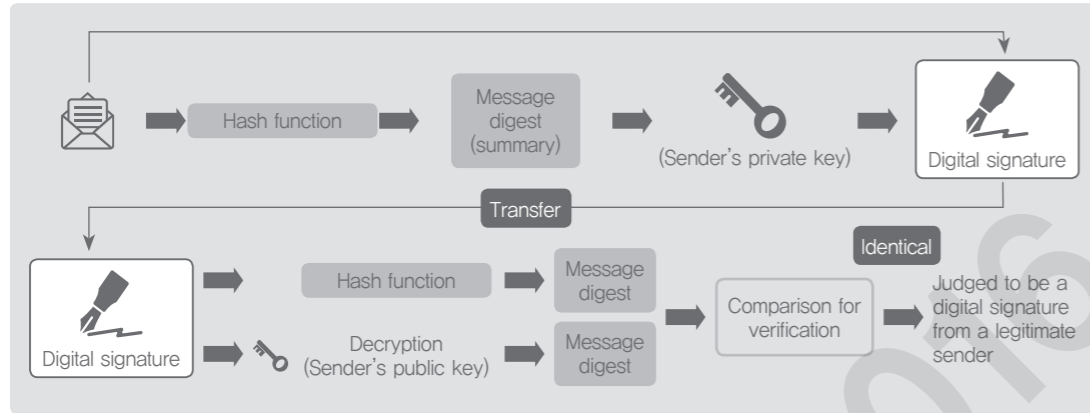
If you use an encryption algorithm, your private and confidential information can be safely exchanged even on the public communications network like the Internet. However, can we really say that e-transactions are fully secured just based on the encryption-based confidentiality? To make an on-line transaction safe, you should be able to verify who your counterpart is and to be able to sign on the documents (a contract or receipt) even though the transaction is not a face-to-face transaction. However, paper-based signatures or certified stamps cannot be used in the on-line environment.

Then, an e-document with a hand-written signature can be accepted legally? The answer is 'No'. Any e-document can be copied and manipulated easily and it is not possible to distinguish the original document from a copied one.

To take care of this kind of issue, digital signature was made available. The mechanism for the digital signature is explained in (Figure 22), which uses authentication functions used in cryptography technologies in order to put a signature on a digital document. Thanks to the authentication function that can be provided by Public Key Encryption, it is possible to authenticate the identity of a signatory and to perform authentication for the digital document at the same time, making the process carries validity as a digital signature.

The basic assumption of the public key encryption mechanism is that the user (owner) of a private key (secret key), which corresponds to a public key, should securely store the key all the time. Within such an ideal situation, if a digital signature was made based on the private key, it should be accepted as a valid signature, because only the key owner is supposed to do it.

By using the public key encryption mechanism, a sender encrypts the message digest (hashed value of the message) with the private key to create a digital signature, and sends the digital signature along with the original message. A receiver decrypts the digital signature with the public key of the sender, and calculates the message digest by using the received message on his/her own, and compares the two values (one from decryption, the other from received message). In this way, it is possible to authenticate the sender and verify non-repudiation and integrity.



(Figure 22) Conceptual diagram of digital signature

② Requirements for secure digital signature algorithm

- Anti-counterfeiting: no one should be able to forge the signature (only one valid signatory)
- User authentication: it should be possible to identify who the signatory is just based on the digital signature
- Non-repudiation: a signatory should not be able to deny the fact he/she signed
- Manipulation prevention: the content of the documents should not be changed once it is signed.
- Non-reuse: one signature to one document cannot be reused as a signature for another document.

③ How digital signature works

There are six steps in (Table 9) to describe how digital signature works.

(Table 9) Six steps of digital signature processing

Sequence	Details
Step 1	The sender applies a hash algorithm to the message in order to generate a fixed length string called a message digest.
Step 2	The sender encrypts the generated message digest with his/her private key in order to create a digital signature.
Step 3	The sender sends out the message and digital signature to the receiver.
Step 4	The receiver decrypts the received digital signature with the sender's public key in order to extract the message digest that has been generated by the sender.
Step 5	The receiver applies the hash algorithm, the same one as the sender used, to the received message to generate a new message digest.
Step 6	The receiver compares the message digest delivered from the sender and the message digest he/she generated. If the two values match, it is assumed that the digital signature is valid.

PKI

① Definition of PKI

PKI (Public Key Infrastructure) is a basic foundation for public key management which is regarded as a core factor in encryption and authentication. The PKI is necessary for secure transactions and works as a foundation to securely distribute keys and certificates for encryption and decryption, which are used to provide information security services. The PKI can be defined as a network built among the parties who build and provide policies, instruments, and tools that can make use of certificates and encrypted communications easier in many security-sensitive application areas such security of information systems and e-commerce.

② Components involved in PKI

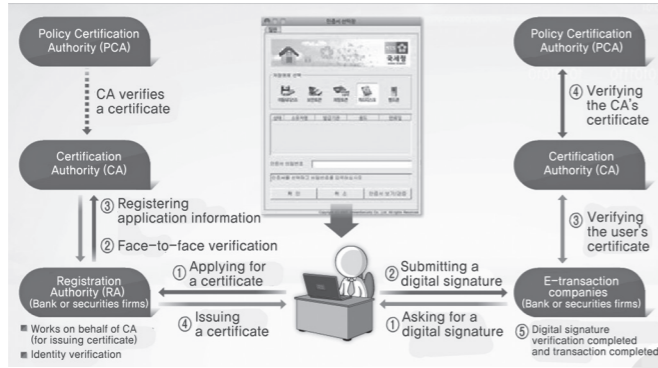
PKI is composed of Policy Approving Authority (PAA), Policy Certification Authority (PCA), Certification Authority (CA), Registration Authority (RA), and Public key certificate (Certificate), as shown in (Table 10)

(Table 10) Components of PKI

Components	Details
Policy Approving Authority (PAA)	In charge of creating policy and procedure for the entire PKI (MSIP: Ministry of Science, ICT and Future Planning)
Policy Certification Authority (PCA)	In charge of detailed planning based on the policies approved from PAA (KISA)
Certification Authority (CA)	In charge of issuing public key certificates and managing the list of discarded certificates (KICA, Koscom, KFTC, Korea Electronic Certification Authority, KTNET)
Registration Authority (RA)	Works on behalf of CAs-receiving applications for public key certificates (Banks, Securities firm)
Certificate owner	Owner of public key certificate: got the certificate issued, signs on an e-document, carries out the encryption.
User	User who verifies the certification path and the digital signature by using the public key of CAs
Public key certificate and CRL repository	To use a certificate that is in compliance with the X.509 v3 standard A digital file that can verify the relationship between the digital signature verification key and its owner CRL repository to manage the list of discarded certificates

③ Operation of PKI

A user goes to a branch of an RA and completes the application process and identification verification to apply for a certificate. The RA sends out the request from a user to a CA. The CA issues the certificate that is signed with the CA's private key and deploys that to the directory server and delivers the certificate to the user via the RA. The user can store the certificate in the hard drive of a PC or in a portable drive and use the certificate in on-line financial or e-commerce transactions. At this moment, financial institutions verify the certificate via the CA. The overall workflow among PKI parties is described in (Figure 23). In the figure, CRL (Certificate Revocation List) means the list of discarded certificates.



〈Figure 23〉 Workflow of PKI parties

④ Digital signature and encryption within PKI

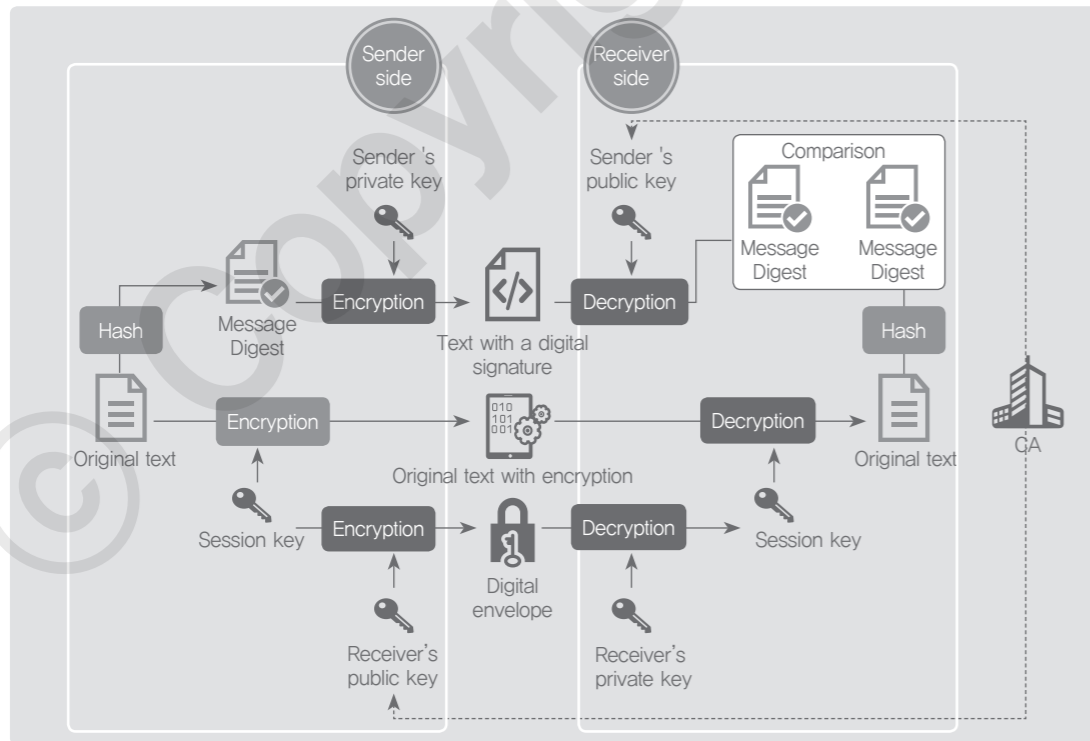
As for the PKI environment where the sender and the receiver operate a cryptographic system based on public key certificates: 〈Figure 24〉 shows the process of how the certificate can be used for user authentication and message confidentiality; and 〈Table 11〉 describes the steps of actions on the sender and the receiver sides. A Session Key, mentioned in 〈Figure 24〉, refers to a one-time-use secret key which was generated by the receiver in order to use the symmetric key mechanism for the message. To ensure the secure delivery of the session key, the key should be encrypted with the receiver's public key. The encrypted session key is also called a digital envelope.

〈Table 11〉 Steps of actions from the sender and receiver sides

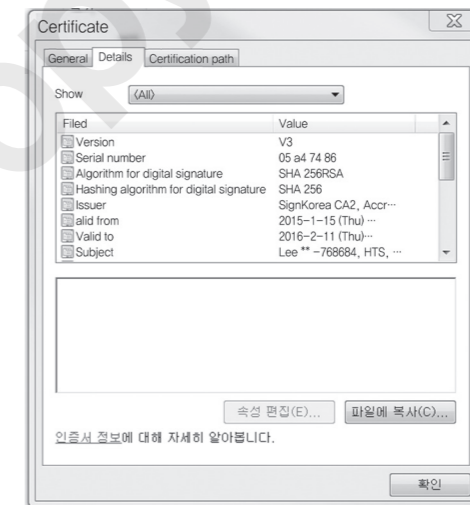
Classification	Sequence	Details
Sender	Step 1	To apply a hash algorithm to the original message in order to generate a message digest
	Step 2	To apply the public key algorithm to the generated message digest in order to make encryption with the sender's private key. (To generate digital signature)
	Step 3	To apply a symmetric-key algorithm to the original message to encrypt the message with a session key.
	Step 4	The session key used in the encryption is encrypted with the receiver's public key. (Digital envelope)
Receiver	Step 1	The digital signature is decrypted with the sender's public key in order to generate a message digest.
	Step 2	The encrypted session key is decrypted with the receiver's private key to extract the session key.
	Step 3	The extracted session key is used to decrypt the encrypted original message.
	Step 4	A hash algorithm is applied to the decrypted original message in order to generate a message digest.
	Step 5	To compare the two message digests

⑤ Public key certificate

A public key certificate is issued by CAs in compliance with the X.509 standard. There are a few types of such public key certificates: NPKI certificate which is used by general citizens in financial transactions and e-commerce; and GPKI certificate which is used by government agencies for administrative works. 〈Figure 25〉 shows an example of NPKI certificate.



〈Figure 24〉 Process of digital signature and encryption within PKI



〈Figure 25〉 Example of public key certificate

The cryptographic system using the public key certificate started to be upgraded in 2011: the length of the RSA digital signature key was changed from 1,024 bits to 2,048 bits; and the SHA-1 (a hash function with a 160-bit output) was replaced by the SHA-256 (a hash function with a 256-bit output). The core elements of NPKI certificate are explained in (Table 12).

(Table 12) Key elements of public key certificate

Elements	Details
Version	Versions for the structure of the certificate
Serial Number	Unique integer value, which is a serial number within a single CA
Algorithm Identifier	Signature algorithm OID (Object Identifier), used to generate the certificate
Issuer	DN (Distinguish Name) of the issuing CA
Period of Validity	Period of validity which tells the time of generation and the time of expiration (up to second level)
Subject	DN of a certificate owner
Public-key Information	A subject's public key and the identifier of the algorithm where the key will be used
Signature	Signature signed with the CA's private key

- Use cases of digital signatures, using public key certificate
Public key certificate-based digital signatures are used widely in many areas. In accordance with the article 3 of the Digital Signature Act, digital signatures carry legal validity. The use cases are listed in (Table 13).

(Table 13) Use cases of public key certificate

Area	Use case
Finance	Internet banking, on-line stock trading, credit card payment, insurance, giro-based payments,
B2B E-commerce	On-line bidding, on-line contract, sales & tax invoice
Government related administrative works	E-government complaint, registration of real estate/corporation, national & local tax, customs service for import/export, public bidding, electronic applications
E-commerce (B2B or B2C)	On-line contract, sales & tax invoice, on-line certificate
Real estate	On-line application for apartment purchase
Healthcare	E-prescription, administrative works for e-healthcare
Trade	Customs, logistics, on-line letter of credit, global certification, country of origin

Example Question

Question type

Descriptive question

Question

During the document exchanges on the Internet, digital signatures can be generated based on the public key mechanism in order to prevent the denial of the fact that the sender actually sent the document. Explain the digital signature generation process in two steps.

Intent of the question

To underline the importance of digital signatures in e-commerce and to evaluate if the learner has knowledge to utilize digital signatures

Answer and explanation

- 1) Apply a hash function to the document to be sent and generate a message digest (MD).
- 2) Use the sender's private key to encrypt the message digest in order to generate a digital signature

The sender encrypts the message digest (hashed value of the document to be sent) with the private key that only the sender knows in order to generate a digital signature. The digital signature is sent along with the document. On the receiver side, the receiver decrypts the digital signature with the public key of the sender. The receiver can compare the hash values from the same hash function: one from the decryption and the other from the received message. This verification method can be used in preventing the denial of the fact that the sender actually sent the document.

Related E-learning Contents

- **Lecture 1** Basic Concept of Information Security and Related Technologies

Understanding the Concept and Types of Network Security and Build Secure network

▶▶▶ Latest Trends and Key Issues

The Internet has witnessed its rapid growth backed by the development of wired/wireless communications technologies. The Internet now has significant implications in all aspects of our lives, such as politics, economy, and society, resulting in the paradigm shift and changes in everything surrounding us. Now it has evolved into a new form called IoT (Internet of Things). However, there are several constraints in bringing such changes in the remote healthcare, e-commerce, or any other real-life areas. Among them, the most significant and urgent constraint may come from security-related issues. Against this backdrop, core security technologies have been developed and in use in a bid to protect internal information assets from a variety of network security threats, such as Firewall, Virtual Private Network (VPN), and Intrusion Detection System (IDS).

▶▶▶ Study Objectives

- * To be able to identify the concept and types of attacks taking place over the network and explain about the defense mechanisms against them
- * To be able to explain about network security technologies and major solutions
- * To be able to explain about the wireless LAN security standard (IEEE 802.11i) and relevant technologies
- * To be able to explain how the SSL (Secure Socket Layer) works and where the SSL can be used
- * To be able to explain about the security mechanism and details for each of the application layer protocols and utilize the same in practice

▶▶▶ Practical Importance High

▶▶▶ Keywords

Firewall, Virtual Private Network (VPN), SSL, Traffic attack, Denial of Service (DoS), Intrusion Detection System (IDS), IPSec, Transport mode, Tunnel mode, Sniffing, Spoofing, Key management, Security Association (SA), NAT, DMZ, Wireless LAN, IEEE 802.11i, 4-way handshake, OWASP Top 10, Anonymous FTP

+ Practical tips To build a secure network, using a firewall and the DMZ

Company A is a small and medium-sized enterprise in which the network is connected to about 90 units of computers. The company has now 126 IP addresses (211.82.50.0/25, public IP), one router ((211.82.50.126/25), one switch, one DB server, and one web server. Mr. Kim is assigned with the task of building internal, external, and DMZ networks by adopting firewalls under the goal of enhancing the security level of the company. We will look at how to build up the secure networks under the following conditions.

- Internal PCs (90 units) and the DB server are assigned with the private IP address (192.168.1.0/24).
- The web server continues to use its existing address (211.82.50.1/25) and is placed on the DMZ network.
- Each of two subnet addresses, the result of the subnetting of the existing IP bandwidth (211.83.50.0/25), is assigned to the external network and the DMZ network respectively.
- Only one router, one firewall, and two switches are used.

01 Outline of Network Security

Concept of Network Security

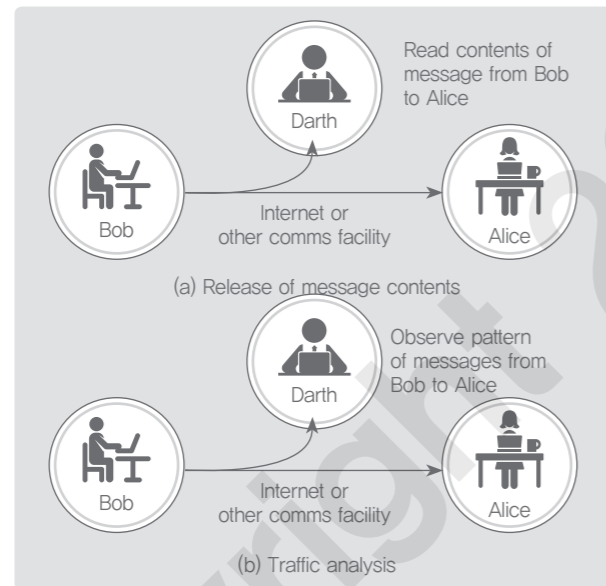
① Types of security attacks

Security attacks, under the X. 800, can be categorized into two types: passive attacks and active attacks. A passive attack is an attack characterized by the attacker attempting to learn about the system information or make malicious use of the information from the system, but not affecting system resources. Meanwhile, an active attack attempts to alter system resources or affect their operation.

- Passive attacks
Passive attacks mean the eavesdropping on or monitoring of data transmission, aiming to steal the data being

transmitted. As shown in (Figure 33), there are two types of passive attacks: 'release of message contents' and 'traffic attack'. A traffic attack is an attack that observes the frequency and length of the message being exchanged, even if the message is encrypted for the sake of confidentiality. Based on the observation, it predicts the nature of the communications.

Passive attacks are very difficult to detect because they do not involve any alteration of the data. Thus, prevention is more important than detection when dealing with passive attacks.



(Figure 33) Passive attacks

(Source: W. Stallings, Cryptography and Network Security – Principles and Practice, Prentice Hall, p.17)

• Active attacks

As shown in (Figure 34), active attacks involve some modifications of the data stream or the creation of a false stream. The active attack can be subdivided into four categories: Masquerade, Replay, Modification of messages, and Denial of service (DOS).

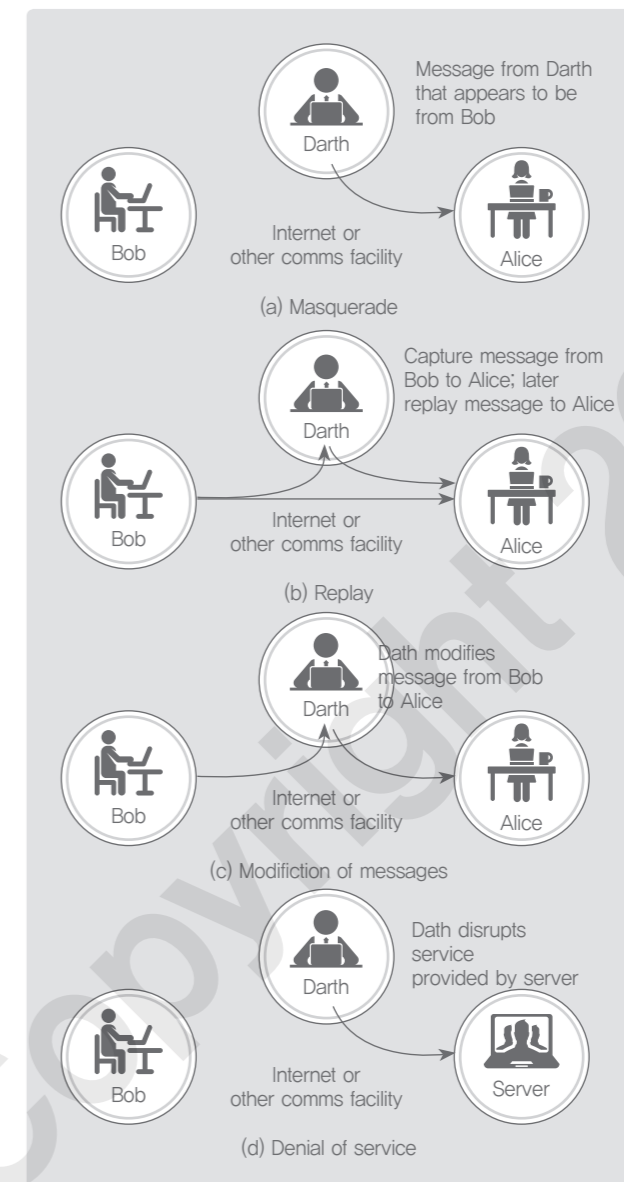
Masquerade takes place when one entity pretends to be a different entity. A masquerade attack usually includes one of the other forms of active attacks.

Replay involves the passive capture of a data unit and its subsequent retransmission to produce an unauthorized effect.

Modification of messages simply means that some portion of a legitimate message is illegitimately altered, or that messages are delayed or reordered, to produce an unauthorized effect.

Denial of service prevents or inhibits the normal use or management of communications facilities (e.g. specific computers or networks). It is typically called the DoS attack. This attack generally has a specific target.

Characteristics of active attacks and passive attacks are opposite to each other. Active attacks are difficult to fully prevent, because it is practically impossible to physically protect all communications facilities and communications lines all the time. A defense mechanism against this attack is to detect attacks and to recover from any disruptions or delays caused by the attacks.



(Figure 34) Active attacks

(Source: W. Stallings, Cryptography and Network Security – Principles and Practice, Prentice Hall, p.18, 19)

② Network security model

A computer network is composed of communications entities (computers) and communications systems (a group of transmission/receiving devices and communications lines). The computer network exists where an originating computer and a receiving computer are linked together to share data, regardless of their locations and distance between the two.

(Figure 35) shows a simple model of network security, describing the components of communications. A message is transferred from a source to a destination across the network, such as the Internet. During this process, both

of the sides must cooperate in the exchange of the message. A logical information channel is established by defining a route through the Internet from a source to a destination and agreeing on the communications protocol to be used for the communications between them. The logical information channel refers to the path between the originating computer and the receiving computer and the channel, which consists of several communications devices, is assigned for the data transmission.

When it is necessary or desirable to protect the transferred data from an opponent who may present a threat to confidentiality, authenticity, and the like, a set of security measures come into play. There are two common components in all the security-related techniques.

- A security-related transformation on the data to be sent; the encryption of the message (which scrambles the message so that it is unreadable by the opponent), and the addition of the code (hash code) based on the content of the message (which can be used to verify the identity of the sender).
- Some secret information should be shared only between the two communications entities and unknown to opponents; an encryption key which is used in conjunction with the transformation to scramble the message before the transmission and unscramble the message after the reception

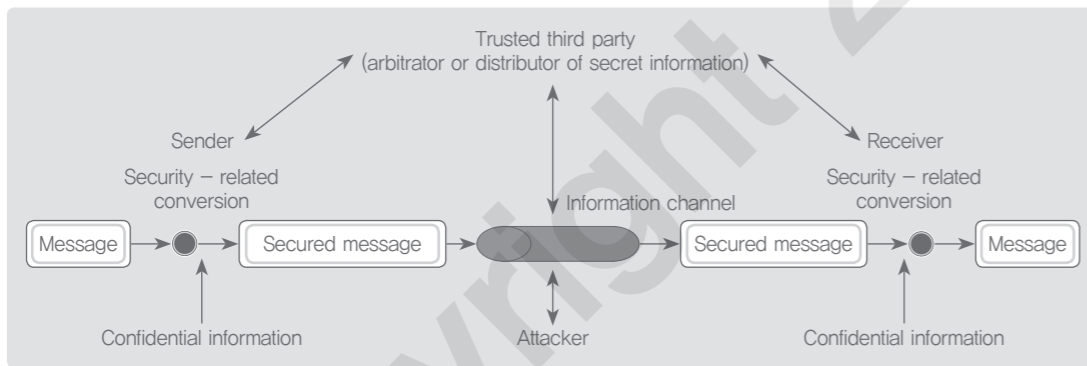


Figure 35) Network security model

(Source: W. Stallings, Cryptography and Network Security – Principles and Practice, Prentice Hall, p.25)

A trusted third party may be needed to achieve secure transmission. For example, a third party may be responsible for distributing the secret information, such as secret keys, to the two parties while keeping it away from any opponents. A third party may be needed to arbitrate disputes between the two parties.

The general network security models which are explained above have four basic tasks in designing a security service:

- To design an algorithm for performing the security-related transformation; an opponent should not be able to defeat the purpose of transformation.
- To generate the secret information to be used for the algorithm
- To develop the method to distribute and share the secret information
- To specify a security algorithm to achieve a certain security service and to assign a protocol enabling the two parties to use the secret information

3 Network access security model

An attacker attempts to break into the information system and then damage the system, destroy or steal personal information stored in the system. A range of malicious software, such as viruses or worms, can harmfully affect the

information system through the network.

As shown in (Figure 36), the security mechanism to cope with the unwanted accesses falls into two broad categories. The first category might be termed as a gate keeper’s function. It includes the password-based login procedures that are designed to deny access to all but authorized users. Once access is granted, either by a user or software, the second line of defense consists of a variety of internal security controls. Internal security control is achieved mainly by the Intruder Detection System (IDS) that monitors the activities of the information system and detects the presence of unwanted intruders.

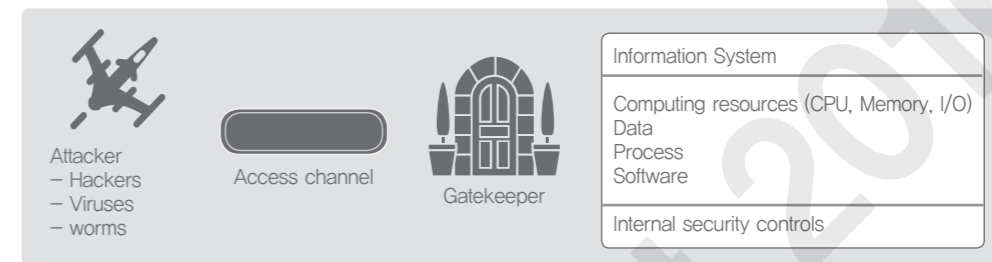


Figure 36) Network access security model

(Source: W. Stallings, Cryptography and Network Security – Principles and Practice, Prentice Hall, p.26)

Communications Protocol Layer and Security

1 OSI 7-layer reference model and TCP/IP protocol layer suite

Figure 37 shows the OSI (Open System Interconnection) 7-layer reference model (described in ISO/IEC 7498-1:1994(E)) that illustrates the architecture of the interconnection between open systems.

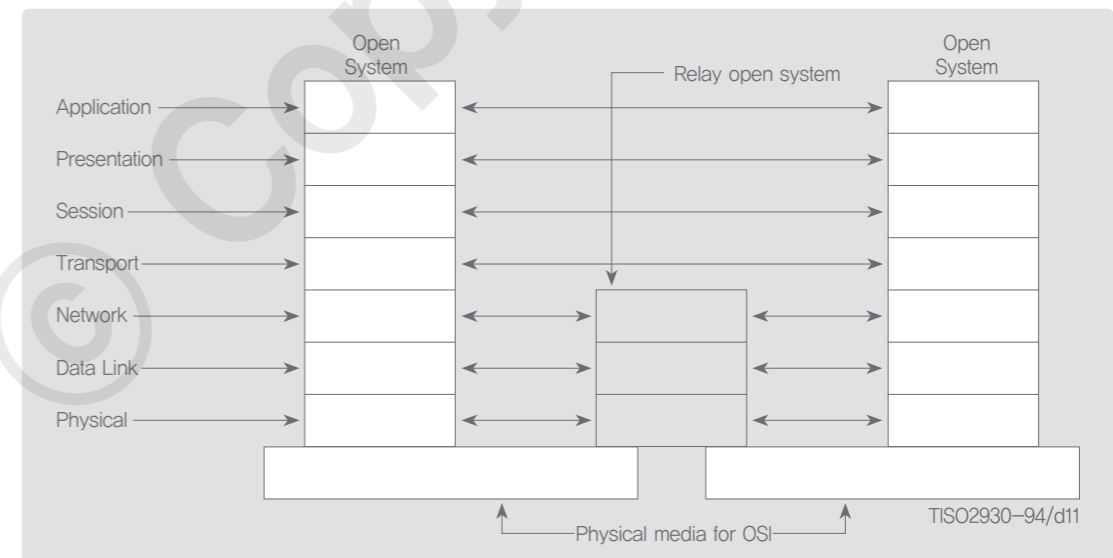


Figure 37) OSI 7-layer reference model

〈Table 18〉 shows the protocols for each layer of the OSI 7-layer reference model and the functions of each protocol.

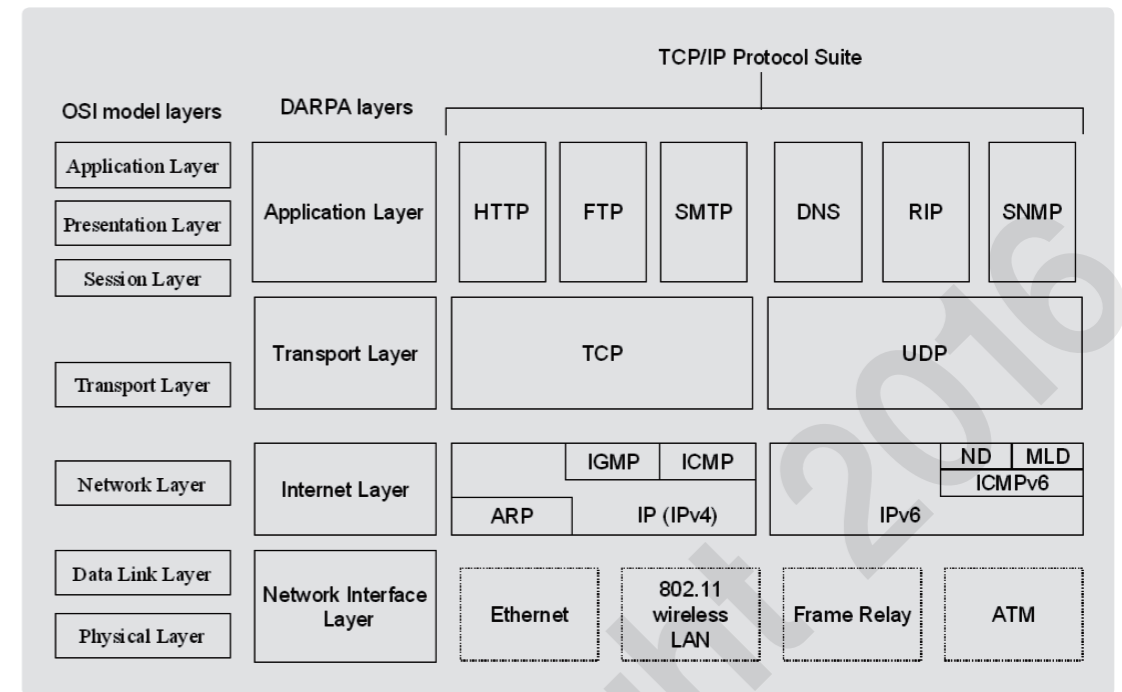
〈Table 18〉 Protocols and their functions for each layer of OSI 7-layer reference model

Layer	Protocol	Function
Application layer	HTTP, SMTP, SNMP, FTP, Telnet, SSH, DNS, etc.	Providing services, such as user interface, e-mail, database management, etc.
Presentation layer	JPEG, MPEG, XDR, etc.	Providing data conversion functions that are performed by using a common format
Session layer	TLS, RPC, NetBIOS, etc.	The layer that manages communications sessions: establishing, managing, and synchronizing sessions between communication devices
Transport layer	TCP, UDP, SCTP, etc.	Providing reliable message transmission between end-to-end (source and destination) processes and error control
Network layer	IP, IPX, ICMP, X.25, ARP, OSPF, etc.	Supporting packet transmission between (heterogeneous) networks from source to destination host.
Data link layer	Ethernet, Token Ring, wireless LAN, etc.	Providing functions which transport frames from one device to another without errors.
Physical layer	Radio wave, coaxial cable, UTP, optical fiber, etc.	Physical layer transforms bits in a computer system into electromagnetic signals for a particular transmission medium.

TCP/IP protocol suite, which is used in the Internet, is based on the ARPANET reference model which came out earlier than the OSI 7-layer reference model. As shown in 〈Figure 38〉, the TCP/IP protocol suite consists of three layers.

- Application layer: provides the application services (including web (HTTP), DNS, Telnet, FTP, e-mail (SMTP / POP3 / IMAP4)) which are operated based on the services provided from the transport layer, a lower level layer than the application layer. This layer logically covers not only the application layer but also the presentation layer and the session layer of the OSI reference model.
- Transport layer: also called the ‘host-to-host transport layer’ and is responsible for data exchanges among abstract ports, such as TCP, UDP, and SCTP protocols which are managed by application programs. This layer is equivalent to the transport layer of the OSI reference model.
- Internet layer: also known as the network layer and is responsible for addressing and routing. This layer is equivalent to the network layer of the OSI reference model.

As shown in 〈Figure 38〉, the Network Interface Layer, or the Network Access Layer, is an independent concept from the TCP/IP protocol suite. This layer is arbitrarily chosen from the network user environment. It is responsible for the actual transmission of TCP/IP packets through physical media, such as IEEE 802.3 Ethernet or IEEE 802.11 WiFi. When compared to the OSI model, this layer is equivalent to the data link layer that takes care of the MAC function and the physical layer that defines electrical signals.

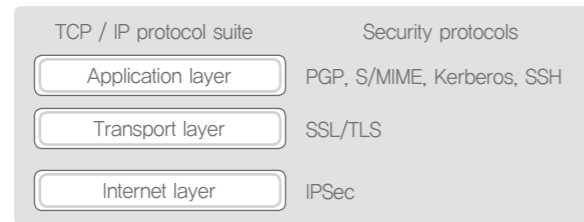


〈Figure 38〉 TCP/IP protocol layers

② Security functions for each layer

The TCP/IP suite was designed to freely exchange data and thus, the security aspect was not factored into the design of the TCP/IP suite. Now that TCP/IP is widely used as the main protocol for the Internet and its application has been expanded to a variety of fields, such as e-commerce, developers have engineered some solutions designed to add protocols that provide security functions to this inherently insecure infrastructure. 〈Figure 39〉 shows the security protocols for each layer of the OSI 7-layer reference model.

- Security protocol for application layer
There are a variety of the application-layer security protocols: PGP and S/MIME for securing email messages; Kerberos for the authentication; and SSH (secure Shell) for supporting the secure remote access.
- Security protocol for transport layer
SSL (Secure Socket Layer) and TLS (Transport Layer Security) are the protocols which logically work over the transport layer. They are responsible for providing the secure transport layer services to the application layer. The TLS is the IETF (Internet Engineering Task Force) standard for the SSL and responsible for providing secure communications and data integrity between two end points.
- Security protocol for Internet layer
IPSec (IP Security) is a protocol that logically works over the internet layer and responsible for providing security services to the internet layer, such as authentication and encryption. This protocol is used for implementing the VPN services.



〈Figure 39〉 Security protocols for each layer

Types of Network Attacks and Defense Mechanisms

① DoS attacks

Denial of Service (DoS) attack is to disrupt the normal operation of a particular server by flooding the server with various forms of requests. It is an attack that undermines availability, which is one of the security services. There are widely used and known DoS attacks, such as Land attack, Ping of Death attack, Syn Flooding attack, and Boink attack.

• Land attacks

Land attack is performed by an attacker who makes the source and destination IP addresses identical with the attacker's IP address, and sends a spoofed packet to the attack target. When the target host tries to reply, it enters a loop, repeatedly sending and receiving the packet, which eventually harms the IP protocol stack and causes the server to crash down.

To protect the host from this attack, it is recommended to block all packets where the source and destination IP addresses are the same, using routers or packet filtering tools.

• Ping of Death attacks

Ping of Death attack is a type of network attacks in which an attacker sends an ICMP packet using a ping command. The ICMP packet, which is deliberately made larger than the normal one, is transferred to the target in the form of many fragmented packets over the network. The target system is required to handle all these fragmented packets, which far exceeds the workload of a normal ping command, and eventually the target cannot perform normally.

The defense mechanism to counter this attack is to employ tools, such as firewalls, that can block the ICMP protocol from sending the Ping command.

• Syn flooding attacks

Syn flooding attack is an attack that exploits the vulnerability of the TCP 3-way handshaking procedure in which the connections can be half-opened. Under this attack, the victim system is unable to respond to the connection requests coming from outside, and eventually unable to work normally. Not only Windows systems, but also all systems that provide TCP-based services on the Internet (e.g. Web server, FTP server, mail server, etc.) can be harmfully affected by this attack.

The defense mechanism to counter this attack includes shortening the time spent by the target system to wait for the acknowledgement of a SYN request or installing the Intrusion Prevention System.

• Boink attacks

Boink attack, a modified version of the Bonk attack, is a type of DoS attacks. Let's suppose that the size of a packet is 100 bytes. Some packets are normally delivered with right sequence numbers; for example, the sequence number (the number of bytes) of the packet sent first is 1 and the next is 101, followed by 201. However, the sequence number of Packet No. 20 is 2002, followed by 101 for Packet No. 21, and 2002 for Packet No. 22. Likewise, this attack sends abnormal packet sequence numbers, causing the target system to be overwhelmed with packet retransmission and reassembly.

The defense mechanism against this attack is similar to that of the Ping of Death attack or Syn Flooding attack.

DDoS (Distributed DoS) attack is an advanced version of the DoS attack, in which malicious traffic comes from multiple sources.

② Sniffing attacks

Sniffing is a passive attack and its concept is identical to that of eavesdropping or overhearing. Every device on the Internet (in other words, every device connected to the LAN) is identified by two addresses – IP address (Layer 3 address) and MAC (Medium Access Control) address (Layer 2 address, which is built into the Network Interface Card). Every MAC address on the Internet has different values, making each system identifiable from each other. All hosts connected to the same LAN share the same communications line. Therefore, a computer is able to see all communications traffic of another computer connected to the same LAN.

To overcome a flaw stemming from such a feature, the Network Interface Card (generally called the LAN card) has a filtering function in which the frame matched with different MAC address is filtered out. This filtering function ensures that only the traffic from the same MAC address can be accepted.

However, on a special occasion, this setting can be changed, so that the LAN card is able to read and receive all the traffic. It is called the Promiscuous mode. The sniffing is an attack that puts the LAN card into the promiscuous mode, allowing an attacker to eavesdrop on all the traffic on a particular LAN.

In case of the switch-based LANs, traffic is transmitted only to a particular intended recipient. In such a case, even if the LAN card is in the promiscuous mode, the attacker is unable to receive the traffic that is not specifically destined for the attacker. Yet, there are numerous sniffing attacks available even in switch-based systems, such as Switch Jamming, ARP Redirect, ICMP Redirect, and MAC spoofing.

All sniffers attempt to eavesdrop on the network by putting its LAN card into the promiscuous mode. Therefore, the system where the sniffer is running can be detected by periodically checking whether a particular host is set to the promiscuous mode. There are several methods that are used to detect the sniffer present on the network, such as Ping method, ARP method, DNS method, and Decoy method.

③ Spoofing attacks

Spoofing is a term that means deception. All that are related to communications, such as IP addresses, host names, port numbers, and MAC addresses can be a victim of spoofing. The spoofing attack occurs when an attacker falsifies its own identifiable information, so as to attack the target system. This attack is employed for other forms of attacks, such as packet sniffing, DoS attack, and session hijacking.

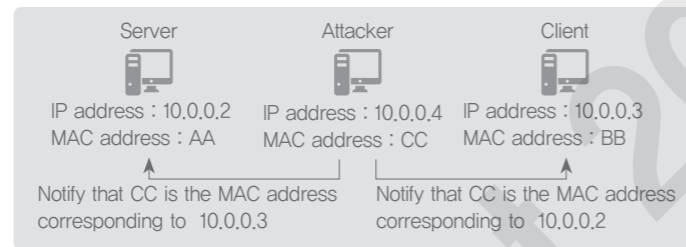
• ARP spoofing

ARP protocol is a protocol that maps an IP address to a MAC address. ARP spoofing is an attack that uses a spoofed MAC address.

As shown in (Figure 40), an attacker sends a client a CC, a spoofed MAC address, which is matched to a server's IP address 10.0.0.2. The attacker sends the server a CC, a spoofed MAC address, which is matched to the client's IP address 10.0.0.3.

The attacker sends its own MAC address to the server and the client. Therefore, both believe that they are directly communicating with each other at the MAC address of the attacker and start to send packets to the attacker.

The attacker reads packets from the server and the client. After then, the attacker sends back the packet, which was received from the server, to the real destination, the client. In the same way, the packet from the client is sent back to the original destination, the server. In such a way, the attacker is able to illegitimately gain all the traffic of the communications between the server and the client.



(Figure 40) ARP spoofing

There is no fundamental defense mechanism against the ARP spoofing, since it stems from the innate flaws of the TCP/IP protocol suite. Yet, it is possible to prevent the MAC address from being spoofed by using an ARP command so as to configure the ARP table settings and to stop the ARP table alteration. However, this command is inconvenient in that it needs to be run whenever the system is rebooted.

- IP spoofing

IP spoofing is a practice of hacking in which an attacker impersonates an IP address of a target host. In other words, it earns the authority that enables the attacker to, for example, log in by stealing the IP address used by other users.

When the trust relationships exist between system A and system B in the network environment, System A is allowed to be connected to System B only with its account. (No authentication is required when connecting from System A to System B on the network) This service is called a trust authentication. In the trust authentication service, trust services are provided based on the authentication by the network address, not with passwords. In other words, IP addresses of trusted clients are stored in the server. If a request for a log-in comes from the client that contains the IP address stored in the list, the log-in is allowed without asking for an ID or a password.

Not to allow the trust authentication, except under special circumstances, is the only way to defense against the IP spoofing.

- DNS spoofing

If the DNS server of a particular domain is under the control of an attacker, the final IP address is directed not to the system that was originally requested, but to the system designated by the attacker. In other words, the attacker sniffs the traffic generated between the DNS and the upper-level DNS site when the user makes a request for address translation to the DNS. It enables the attacker to present the IP address that is directed to a fake website as a final response.

The defense mechanism against the DNS spoofing is to register the IP address information of the important destination servers in the hosts files of the user, so that the user can acquire the IP address without relying on the DNS server. However, it is practically impossible to register the IP addresses of all the servers and manage them properly.

02 Security Protocol and Security Solution

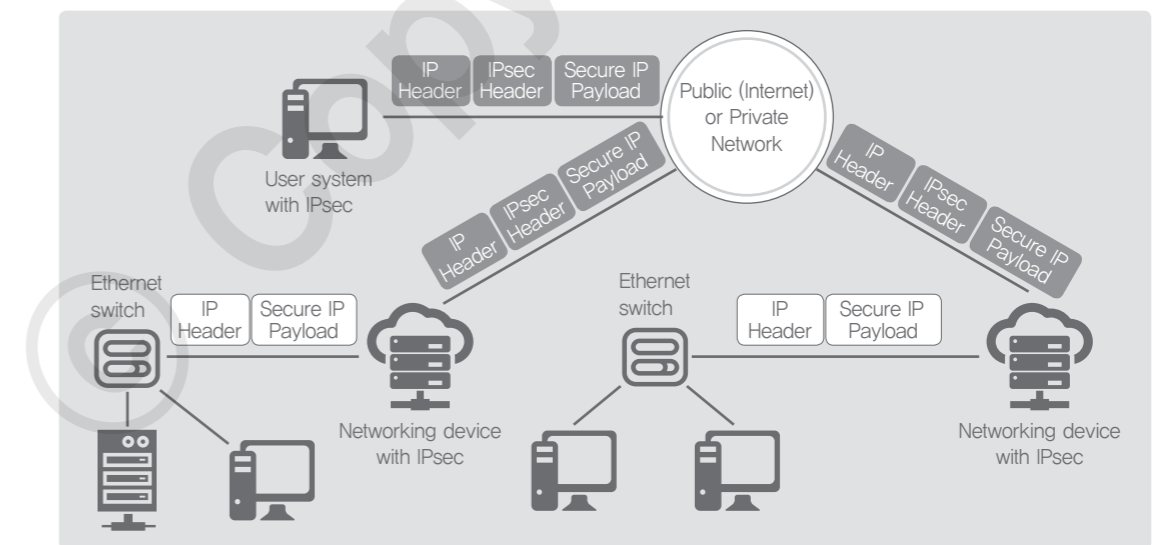
IPSec

① Concept

Internet Protocol Version 4 (IPv4) doesn't provide any authentication services, and it is susceptible to many forms of attacks, such as eavesdropping or packet modification. Against this backdrop, the IPSec (Internet Protocol Security) was developed to enhance security aspects in the Internet Protocol. The IPSec is used to make IP communications secure by encrypting and authenticating each IP packet, so that it can virtually protect all application programs. Security services provided by the IPSec include authentication, confidentiality, and key management. The IPSec is optional in the IPv4, but the IPSec comes as a default for the IPv6.

② Architecture and mechanism

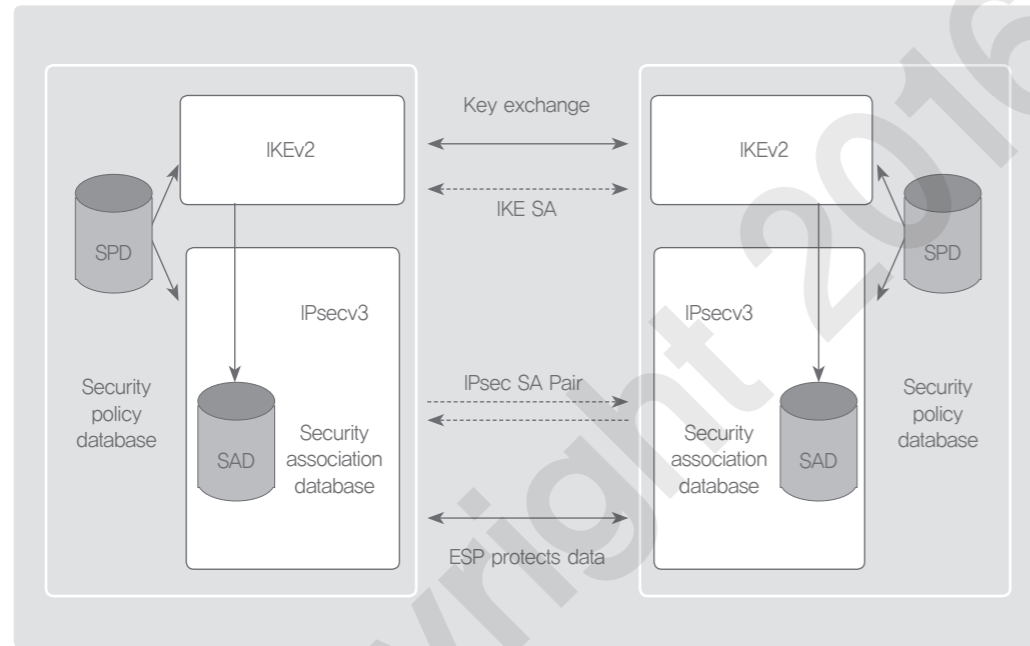
As shown in (Figure 41), when an organization maintains LANs at dispersed locations, the IP traffic can be transferred within the LAN boundary, but the IPSec protocol is used for the outbound traffic to make sure the communications safe. The IPSec protocol is operated in the networking devices, such as a router or firewall. The fact that the IPSec is in operation in the devices is clearly visible to the computers on the LAN.



(Figure 41) Scenario of IPSec use

(Source: W. Stallings, Network Security Essentials, Pearson, p.272)

⟨Figure 42⟩ presents the architecture of the IPSec. It consists of the followings: Internet Key Exchange (IKE) that is used for the SA (Security Association) negotiation; Security Association Database (SAD) that is where SAs are stored; Security Policy Database (SPD) which is a database of security policies that define how to associate the IP traffic with a particular SA; Authentication Header (AH) that is a protocol which provides actual authentication services; and Encapsulating Security Payload (ESP) that provides authentication and encryption services.



⟨Figure 42⟩ IPSec architecture

(Source: W. Stallings, Network Security Essentials, Pearson, p.276)

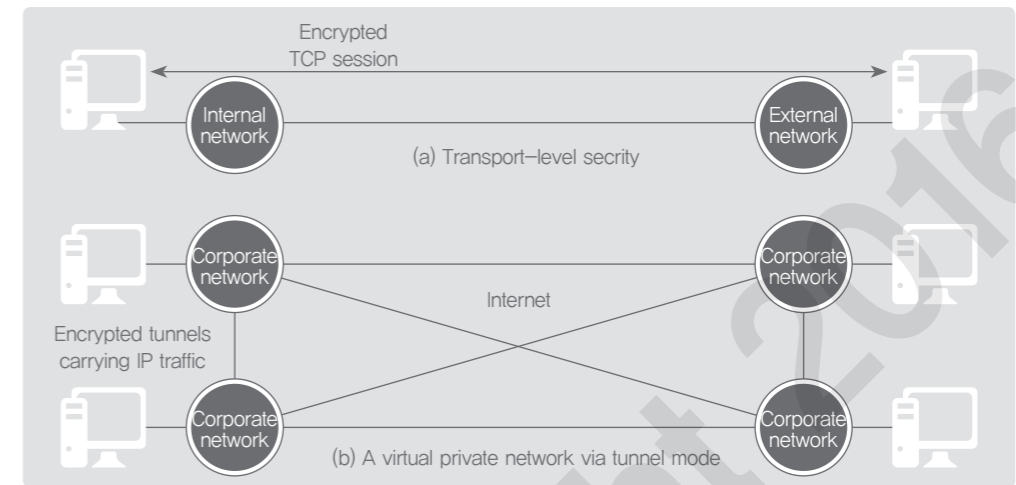
• Transport and tunnel modes

Both of the AH and ESP support the transport and tunnel mode. As shown in ⟨Figure 43⟩, in the transport mode, the IP datagram payload is encrypted without any alteration in the IP header, while in the tunnel mode, the entire IP datagram is encrypted and sent as the payload of a new IP packet. In the tunnel mode, a router generally acts as a proxy for the IPSec.

The transport mode provides protection primarily for the upper-layer protocols. That is, the transport mode protection extends to the payload of an IP datagram. For example, it is used to protect a TCP fragmentation or an ICMP packet. The IPSec in the transport mode operates directly above the IP layer. The ESP, in the transport mode, encrypts the IP payload but not the IP header and the authentication is optional. The AH, in the transport mode, authenticates the IP payload and selected portions of the IP header.

The tunnel mode provides protection to the entire IP datagram. To achieve this, a new outer IP datagram with a new outer IP header is created. During the transmission of this datagram, no routers along the way are able to examine inner IP headers. This is how an IP datagram can be transmitted to an external network through a conceptual tunnel.

The ESP, in the tunnel mode, encrypts and optionally authenticates the entire inner IP datagram, including the inner IP header. The AH, in the tunnel mode, authenticates the entire inner IP datagram and selected portions of the outer IP header.



⟨Figure 43⟩ Encryption in transport and tunnel modes

(Source: W. Stallings, Network Security Essentials, Pearson, p.285)

• Security Association (SA)

To achieve secure communications between the two network entities over the IPSec, the authentication or cryptographic algorithm and an encryption key are needed. Before a secure communication is established, the information regarding a cryptographic algorithm and an encryption key should be exchanged and stored. The Security Association (SA) is a set of such security information. To identify a particular SA among many SAs existing in one system, the Security Parameter Index (SPI), which is an arbitrary value to identify a particular SA, and the destination IP address are required. Since a security association is normally one-way, a two-way communication between the two network entities requires two SAs.

⟨Table 19⟩ illustrates the processes of communications between System A and System B, when SAs are stored. This scenario assumes that the communications is initiated by System A.

⟨Table 19⟩ Communication steps in an IPSec environment

Step	Description
Step 1	To initiate a secure communication with System B, System A looks up its SAD to discover System B's SA.
Step 2	System A gets an encryption key and algorithms from the information stored in System B's SA. By using such security parameters, System A encrypts an IP datagram and inserts the SPI into the IPSec header before sending the encrypted IP datagram to System B.
Step 3	After receiving the encrypted IP datagram from System A, System B looks up System A's SA in its SAD, using the SPI inserted in the IPSec header and the source address A.
Step 4	System B retrieves the encryption key and the algorithms from the security information stored in System A's SA. Using such security parameters, System B decrypts the received packet to get the original IP datagram.

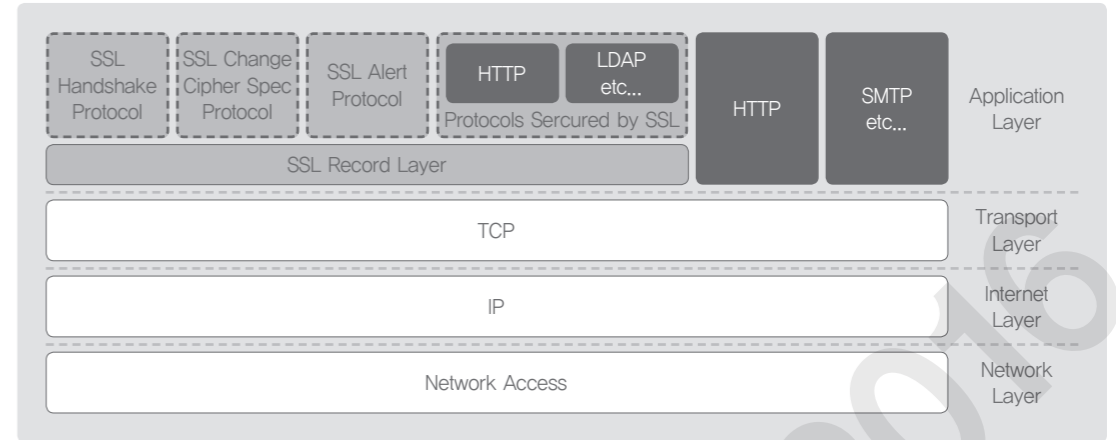
- IKE
The key management portion of the IPsec involves the determination and distribution of secret keys. A typical requirement is four keys for the communications between two applications: transmitting and receiving pairs both for integrity and confidentiality. IKE is used to securely perform the mutual authentication between two applications through the exchange of messages. After this mutual authentication, the IKE generates and stores SAs used for the IPsec communications. The IKE is a protocol that defines procedures for the SA establishment, negotiation, modification, and removal, and specifies the format of packets.

- ③ Use case
IPsec can be used for VPN implementation. In addition, IPsec can provide security services for the application layer services, such as remote access and e-commerce security.

SSL

- ① Concept
SSL is a protocol that was developed by Hickman from Netscape in 1994. After the Version 3.0, the protocol was standardized by the Internet Engineering Task Force (IETF) and was renamed as TLS (Transport Layer Security), and almost all of the web browsers support TLS. SSL is operated between the application layer and the transport layer of the TCP/IP protocol suite, and is designed to use TCP in order to provide reliable and secure end-to-end services. The SSL can be used for a variety of application layer protocols, but most frequently used for HTTP, and it is called HTTPS in this case. Connection and Session are the two main pillars of SSL.
 - SSL connection: An SSL connection means a way of data transfer to provide a service. The connection, in its nature, is 'Peer-to-Peer' and temporary. Each the connection is associated with one session.
 - SSL session: A SSL session means an association between a client and a server. To initiate a session, the handshake protocol (which will be explained later) needs to be used. A session specifies cryptographic parameters shared among multiple connections, especially to avoid the process of parameter negotiation that, otherwise, might have been required in each connection.

- ② Architecture and mechanism
 - SSL protocol suite
SSL protocol suite is composed of four protocols, as shown in (Figure 44): Handshake, Change Cipher Spec, Record, and Alert.



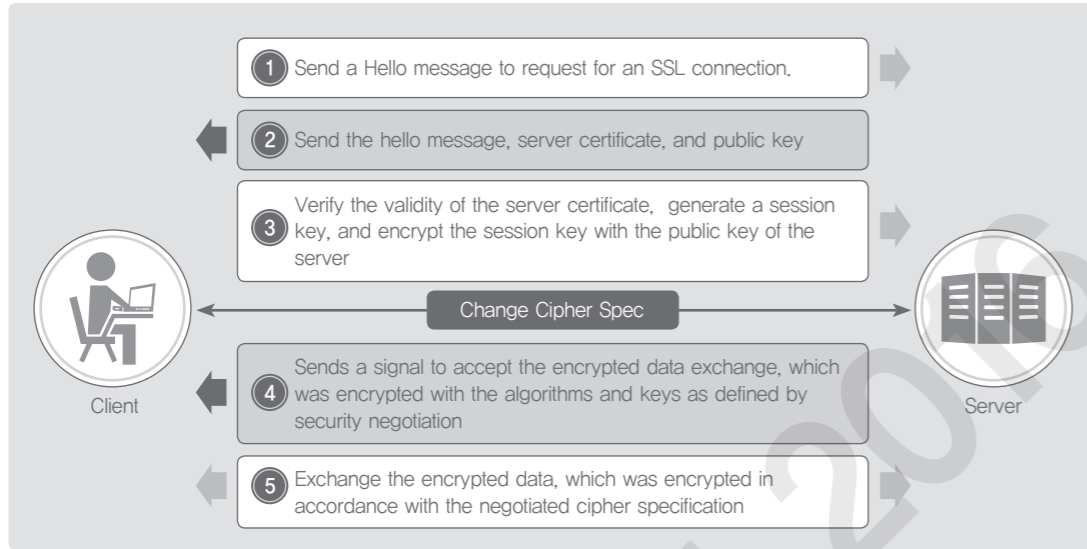
<Figure 44> SSL protocol suite

- Types of SSL protocols
The functions for each of the four SSL protocols are shown in (Table 20).

<Table 20> SSL protocols and their functions

Type	Details
Handshake Protocol	<ul style="list-style-type: none"> • Mutual authentication between the server and the client • Negotiation for the cryptography algorithm, MAC algorithm, and cryptographic keys • Performed before all the application data transfer
Record Protocol	<ul style="list-style-type: none"> • To provide confidentiality and integrity services for the SSL connection • Message encryption by using the predefined secret key algorithm • Encryption is performed with the shared symmetric key
Change Cipher Spec Protocol	<ul style="list-style-type: none"> • To notify the counterpart that the authentication and encryption mechanism specified in the cipher spec will be applied • The message consists of a single byte of value 1.
Alert Protocol	<ul style="list-style-type: none"> • Used to inform the other end, of any irregularity or failure in the SSL process • The message consists of 2 byte messages: the first byte is for the alert level- Warning(1), Fatal(2)

- SSL protocol mechanism
How the SSL protocol works is described in (Figure 46) step by step, and the details for each of the steps are described in (Table 21).



<Figure 45> How SSL protocol works

<Table 21> Detailed explanation for SSL operation steps

Sequence	Details
Step 1	The client sends a Hello message to the server to request for an SSL connection.
Step 2	The server sends the Server Hello message, the server certificate, and public key to the client. If the client certificate is needed, the request for the certificate is also sent.
Step 3	The client verifies the validity of the server certificate, generates a session to be used for encryption, and encrypts the session with the public key of the server. If the cipher spec and the server ask for the client certificate, send the client certificate as well.
Step 4	To send a signal for the exchange of encrypted data, which uses the algorithms and keys as defined in the negotiated cipher specification.
Step 5	To exchange the data encrypted in accordance with the negotiated cipher specification.

③ Use case



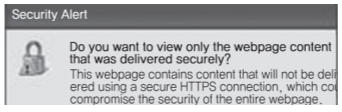

- Installing SSL certificate on servers

SSL certificate should be installed in a web-server in order to enable the communications with the SSL. The first step is to generate a private key from the production web-server; the second step is to fill out the CSR (Certificate Signing Request) and to get an SSL certificate from certification authorities; the third step is to install the certificate onto the web-server and change the configuration. If an SSL Accelerator is in use, the certificate should be installed on the accelerator.

- How to verify your SSL certificate installation

You can verify whether the SSL is working for the web server, in the following methods described below.

<Table 22> How to verify successful installation

Methods	Details
	A yellow lock icon at the bottom of the web-browser
	https:// in the URL
	A pop-up warning message when moving to another page
	Security accreditation seal

- How to deal with SSL-induced workload

Various computing jobs that occur during the SSL handshake procedure can cause a lot of workload to CPUs. Therefore, an SSL accelerator was developed to address this kind of CPU overload issue. The accelerator can come in the form of a PCI card, so that it can be installed on a server. Sometimes, a dedicated device for the SSL acceleration can be employed. However, a web accelerator or a L4 switch can provide the SSL accelerating functions these days, making users only need to buy a license for the SSL accelerator. Once the SSL is applied to the environment, the URL needs to be changed into https:// (including the ones in the source code of applications). In order to reduce the workload caused by the SSL and to enhance the response speed from applications, the SSL web browser cache or web accelerator can be used for caching static contents, such as images, Javascript, CSS (Cascading Style Sheets).

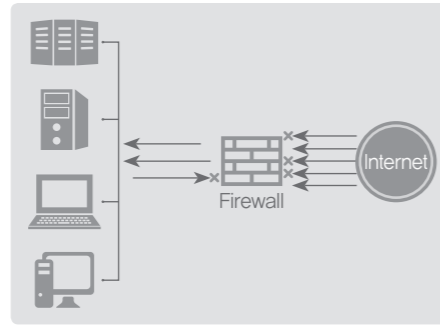
Security Solution

① Firewall

- Introduction to firewall

In the physical world, we use firewalls to stop a fire from spreading further. As such, there is a protective device that can be used to protect a private network from the outside world. A firewall, as shown in <Figure 46>, is a kind of wall located between a public network and a private network under the purpose of protecting the private network from the outer world.

In general, there are two types of firewalls: 1) Packet Filtering Gateway which makes a decision whether to allow a packet to come in or not based on a series of rules; and 2) Proxy Server which authenticates hosts and allows their packets to be delivered into a private network. However, there are some cases that use the two mechanisms at the same time to ensure a higher level of security.



〈Figure 46〉 Role of firewall

- Core technologies pertaining to firewall

The purpose of a firewall is to prevent attacks coming from outside and to keep the network or servers secure. The core technologies used in a firewall are described below.

(1) NAT (Network Address Translation)

NAT is a kind of networking service that allows many systems within a private network to gain access to the Internet with a small number of valid IP addresses. The NAT, actually, is not designed as a security service, but can provide a certain level of security. Within the NAT environment, an internal network and an external network are naturally separated and a direct access from an external network to an internal network is not possible, allowing a certain level of network security.

(2) Packet-Filtering

Packet-filtering literally means to selectively control the traffic flow in accordance with a certain set of rules. The two main rules are passing and blocking. To perform the packet filtering in a proper way, a set of passing rules should be defined in accordance with specific use cases and desired goals. The packet filtering function can also be implemented by a router or an independent host system.

(3) Perimeter Network

Perimeter network refers to a kind of buffer zone located between an external network and an internal network that needs to be protected. It is also called the DMZ. As the DMZ stands for a demilitarized zone, a networking DMZ is intended to segregate an external network from an internal network and to enhance the stability of the internal systems.

(4) Proxy

A proxy is a kind of networking programs, which is an intermediary of a certain service between a server and a client. The client can call for a certain service to a proxy server, and the proxy server provides a connection to an external network following the request from the client.

(5) Bastion Host

Bastion host is located outside of the network that needs to be protected, providing the access authority management of the protected network. It works as a proxy for a web-service or a file transfer service and is responsible for authentication or logging.

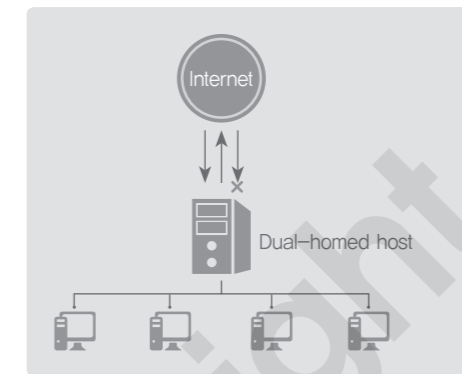
- Types of firewalls

A firewall can be implemented by using the multiple technologies, which were explained above, in accordance with what purpose you have chosen for the firewall. The explanation below provides a high-level explanation about firewall architectures.

(1) Dual-homed hosts

As shown in 〈Figure 47〉, the dual-homed hosts refers to a firewall that uses two network interfaces between an external network and an internal network. However, the architecture uses firewalls where the routing function is disabled.

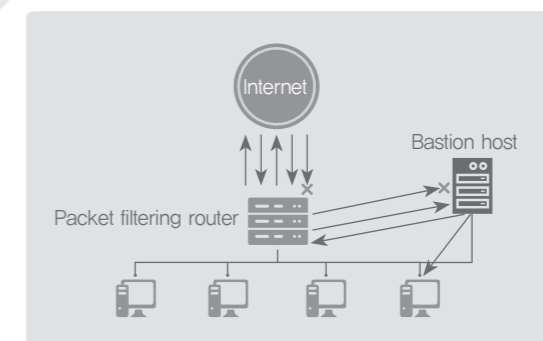
In this firewall architecture, an internal network and an external network are recognized as totally different ones with the dual-homed host located in-between. If an internal network wants to have communications with an external network, the communications must go through the dual-homed host, which means that there is only one actual commutation route between the two networks. However, a dual-homed host should be built with high-performance systems because all the network packets need to be inspected and filtered-out. Because of these reasons, the dual-homed host architecture is suitable for a firewall in a small network.



〈Figure 47〉 Firewall architecture with dual-homed host

Screened Host Gateway

In the screened host gateway architecture, as shown in 〈Figure 48〉, a port of a packet filtering or screening router is connected to an external network and the other ports are connected to an internal network. Also, there is a bastion host connected to the internal network. Overall, the architecture works based on a packet filtering router and a bastion host.

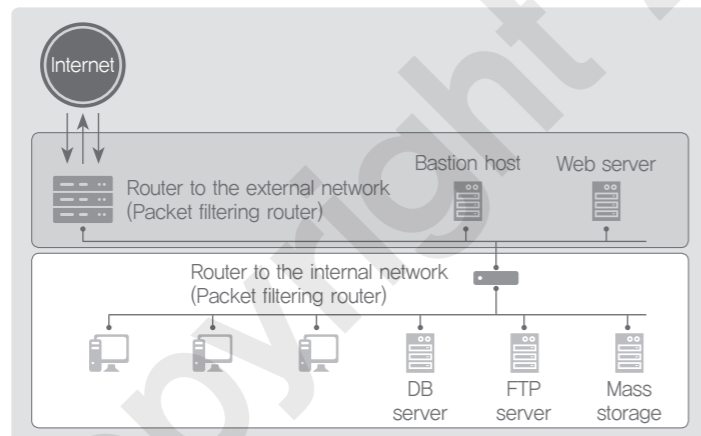


〈Figure 48〉 Firewall architecture with screened host gateway

The role of the packet filtering router is to inspect whether to allow packets, generated from the internal and external networks, to flow in and out. The packets coming from the external network can be delivered only via the bastion host. The bastion host is responsible for the authentication of the internal and external network systems, user authentication, and service authentication. In other words, any user or any service that was authenticated by the bastion host can send packets to the internal network. In this way, a certain level of security is achieved. However, this architecture has a weakness: it is easy to have access to all the hosts and servers connected to the internal network if anyone passes the packet filtering router and the bastion host.

(3) Screened subnet

Screened subnet architecture was designed to overcome the weakness of the screened host gateway architecture and to allow more convenient access for some servers. The screened subnet architecture puts one or more perimeter networks between an internal network and an external network (the Internet), as shown in (Figure 49), so that the internal and the external networks can be fully separated. The simplest implementation of the architecture can be completed with two screening routers (packet filtering routers) and one bastion host.



(Figure 49) Firewall architecture with screened subnet

One screening router is located between the external network and the perimeter network, and the other screening router is located between the internal network and the perimeter network. Meanwhile, the bastion host is located on the perimeter network. In this way, the bastion host is fully segregated from the internal network and an attacker can have access to the internal network only after going through two routers and one bastion host. Hence, it is usually the case: to locate public servers such as web servers, which need frequent access to the external network, on the perimeter network; and to place DB servers and FTP servers, which contain critical information, on the internal network. In this architecture, even though an attacker was successful in attacking the hosts connected to the perimeter network, the attacker should try another attack targeting the firewalls located on the internal network (internal packet filtering routers). Therefore, it can be said that the servers connected to the internal network can enjoy a higher level of security.

• Evaluation criteria for firewalls

The generally used evaluation criteria for firewalls are: identification, access control, integrity, confidentiality, audit records & traceability, and security management. The security management, here, means a series of activities

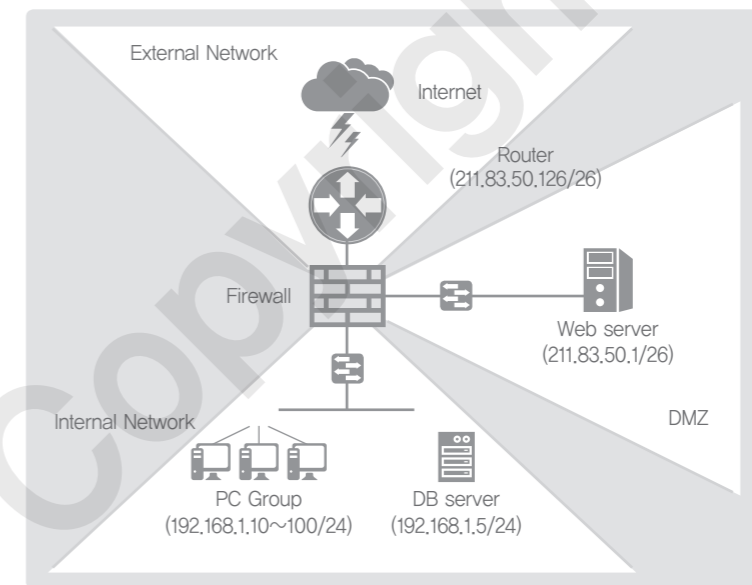
carried out by a firewall administrator to manage security-related data and to ensure that security functions work properly.

② To build a secure network using firewalls

• DMZ

DMZ refers to a shared network area located between an internal network (a private network of a company) and an external network (the Internet). It is possible to have access to the DMZ from the internal/external network, while the computers within the DMZ cannot be connected to the internal network but can be connected only to the external network. Therefore, the computers within the DMZ can provide a certain services to the external network, but cannot gain access to the internal network, for the sake of protecting the internal network. Mail servers, web servers, DNS servers, or servers that need access to the external network are usually located within the DMZ. The connections from the external network to the DMZ are usually controlled by the PAT (Port Address Translation).

In order to build a secure network, company A's network has three main network areas with a firewall at the center, as shown in (Figure 50); internal network, external network, and DMZ. A web-server, which should allow access from outside of the company, is located within the DMZ. However, the DB server, which is used only within the company, is located on the internal network.



(Figure 50) Company A's secured network architecture

• Subnetting and CIDR

CIDR (Classless Inter-Domain Routing) is an IP addressing scheme which does not classify IP addresses into Class A, B, C, and allows a freer way of allocating a network identifier for more flexible IP address management. As the CIDR allows a flexible scheme of IP addressing, it is possible to minimize any waste of IP addresses and build a network more effectively.

It is expressed, for example, as 220.66.32.0/21. The number 21 that comes after '/' means that the first 21 bits of

the IP address (210.66.32.0) correspond to the network address and the remaining 11 bits (32-21=11) correspond to the host address.

In the example of company A's network shown in (Figure 50), the external network and the DMZ network separated the public IP range (211.83.50.0/25) into two. Hence, the address of the web server on the DMZ is changed to 211.83.50.1/26. In addition, the address of the router on the external network is changed to 211.83.50.126/26. The internal network uses the private IP range, so the PCs and DB servers can use any IP address in the range of 192.168.1.1~254 with the exception of 192.168.1.0 and 192.168.1.255.

The DMZ network was separated as a network that can use up to 128 public IP addresses, but the web server should use the existing IP address, so the IP address is changed to 211.83.50.1/26. It is possible to use any IP address within the DMZ network except for 211.83.50.0 (network address), 211.83.50.63 (broadcast address), and 211.83.50.1 (web server address).

③ VPN

Virtual Private Network (VPN) is a network technology that creates a secure network connection over a public network (such as, the Internet) as like in a private network without building a physical private network between two communication points located at a long distance. As like in the connections over a private network, the VPN provides security-related services, such as access control, authentication and confidentiality.

The most widely used technologies for the VPN are the IPSec and SSL. There are multiple ways of implementation, as shown in (Table 23)

(Table 23) VPN implementation methods

Method	Pros	Cons
Implemented on a dedicated system	High speed processing Easy VPN expansion	High cost
Implemented in a router	Relatively less cost	Limitation in router control; limitation in preventing the leakage of confidential information
Implemented on a firewall	Low cost Easy to control	Increased bottleneck in the firewall

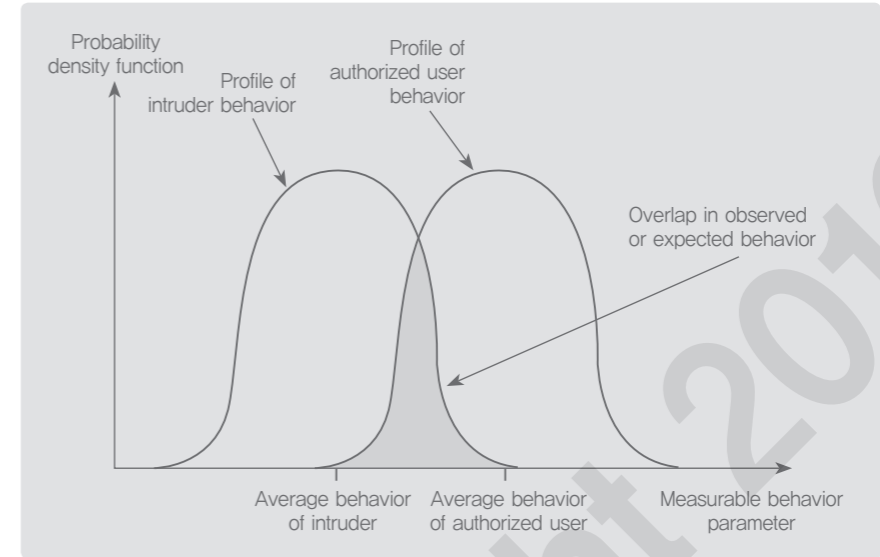
④ Intrusion Detection System

IDS (Intrusion Detection System) is designed: to detect unauthorized activities and abnormal behaviors in the target systems (network detection area); to assess and identify the detected abnormal activities; and to block those abnormal activities in real time. The security system's profile curves of normal and abnormal behaviors are shown in (Figure 51).

As shown in (Figure 51), the average behavior of an intruder and the average behavior of an authorized user have some overlapping areas, which makes it difficult to clearly sort out intruders.

When implementing a security system, the IDS and firewalls are usually built first. The purpose of the IDS implementation is to detect and block abnormal activities, including hacking, on a real time basis and to build a

defense line against the attacks that exploit the packets which were already approved by firewalls.



(Figure 51) Behavioral profile of intruders and authorized users

(Source: W. Stallings, Cryptography and Network Security – Principles and Practice, Prentice Hall, p.20-9)

(Table 24) shows the core features of the IDS and (Table 25) describes the types of the IDS.

(Table 24) Core features of IDS

Feature	Details
Information analysis and real-time monitoring	All the packets within the network (monitoring target of IDS) are monitored and analyzed on a real time basis.
Attack pattern recognition and detection	Recognition and detection of patterns for known attacks occurring within the monitoring zone.
Notification about the attacks detected	Various notification functions: regarding the attacks detected, following the security policy defined in the IDS
Real-time response to intrusion	Blocking the detected attacks, using connection removal or link, following the security policy already defined in the IDS
Post-management based on the logs	Post-management activities: review of the detected attacks, building a database, making a report

(Table 25) Types of IDS

Criteria	Details
Data source	Intrusion detection based on a single host
	Intrusion detection based on multiple hosts

Detection method	Intrusion detection based on abnormal behaviors
	Intrusion detection based on misuse behaviors

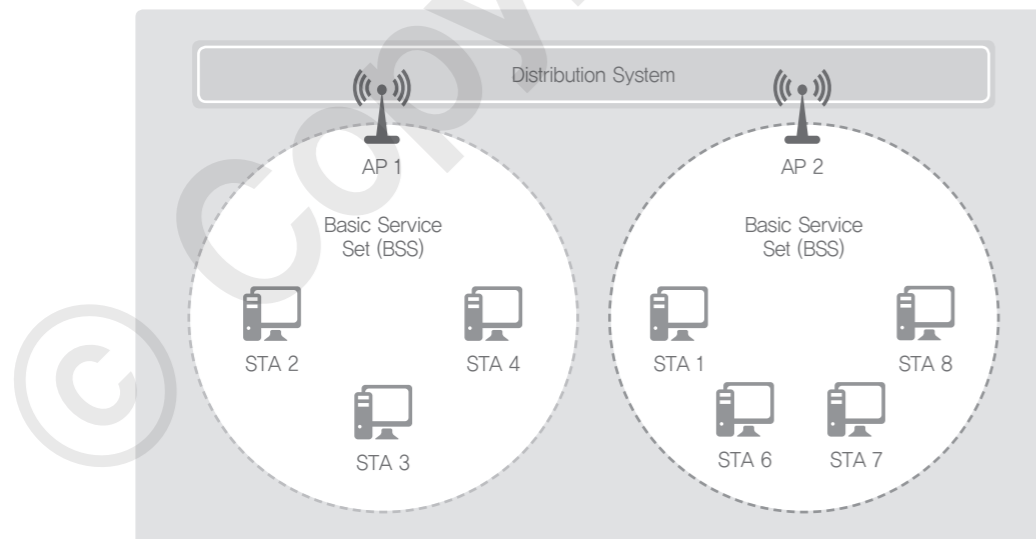
03 Security of Wireless LAN

Characteristics of Wireless LAN

All the data sent/received over the wireless LAN are broadcast to the public via radio waves. Hence, the data over the wireless LAN can be exposed to all the wireless LAN users located in the place where the data can be transferred.

Thanks to its wide range of benefits and convenient features, there has been a rapid increase in the wireless LAN usage. However, the wireless LAN relies on radio waves for its communications, which means the wireless LAN requires more security considerations since it is weaker in security, by nature, compared to the wired LAN. Especially, in the case of the public wireless LAN, which is open to the public for general use, it is absolutely necessary to take some security measures because there is more likelihood of security breaches.

〈Figure 52〉 shows a typical wireless LAN service structure defined by the IEEE 802.11. In the figure, the BSS (Basic Service Set) means a group which is composed of STAs that are operated with the same MAC protocol and compete for the access to the same wireless medium. Meanwhile, the extended service set means an environment where multiple basic service sets are connected to the distribution system for mutual communications.

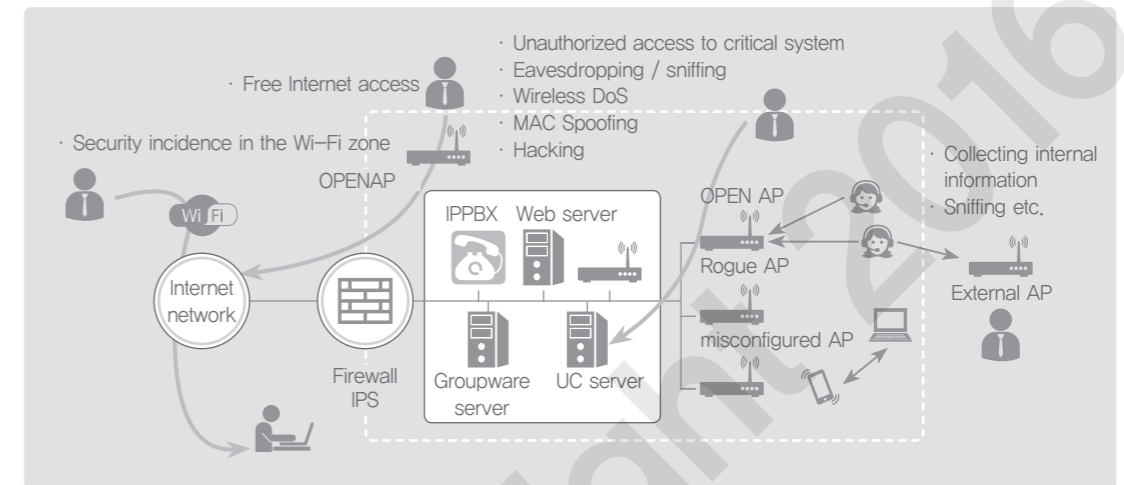


〈Figure 52〉 Extended service set of IEEE 802.11

(Source: W. Stallings, Network Security Essentials, Pearson, p.180)

Security threats and response

A physical access control over the communication medium is not possible in the wireless LAN environment because the communications rely on radio waves. That means that anyone can use wireless LAN services and even pose a wide range of security threats through the acquisition or disturbance/jamming. 〈Figure 53〉 shows various potential security threats over the wireless LAN.



〈Figure 53〉 Security threats over wireless LAN

① Technical security threats

The technical security threats in the wireless LAN environment are: 1) user information leakage and jamming by using radio wave acquisition, unauthorized access, and man-in-the-middle attacks; 2) denial of service by using the transmission of a large amount of packets; and 3) various other types of attacks utilizing vulnerabilities, such as the WEP (Wired Equivalent Privacy), in an attempt to make an unauthorized access to or to intrude into the internal network.

Those technical security threats can be stopped in most of the cases just with the AP (Access Point) level security settings such as the WPA2 (Wi-Fi Protected Access2). However, the corporate network and the like, which handle critical information, should employ an advanced wireless security system such as the WIPS (Wireless Intrusion Prevention System).

② Managerial security threat

Even with a strong set of security measures over the wireless LAN, detouring attacks are possible if a well-organized security management is not in place. The typical examples of managerial security threats are: inadequate management of wireless LAN devices and terminals, lower level of security awareness that may invite intrusions, and improper management of radio waves that can allow external users to gain access to internal APs or internal users to gain access to external APs.

To mitigate managerial security risks, it is necessary: to come up with a set of managerial measures for access devices and terminals (including APs); to periodically conduct awareness programs and trainings for users; and to

inspect unauthorized access from internal and external sources.

③ Physical security threats

The networking devices supporting a wired LAN environment are physically located and managed in a place where general users cannot have access. However, wireless APs are exposed to the public area for many reasons, for example, for better radio wave transmission. In such a public environment, APs can be damaged or stolen and exposed to other risks such as power disconnection or LAN disconnection, causing a service failure. In case when a wireless terminal is stolen and the access information and security configuration within the terminal are exposed to an attacker, it can allow a free access even to an unauthorized user.

To mitigate these kinds of risks, it is necessary not to expose wireless APs to the public and to periodically change the configuration. In addition, it is necessary to come up with a set of measures for terminal management and against terminal losses.

Security Standards for Wireless LAN

① IEEE 802.11i service

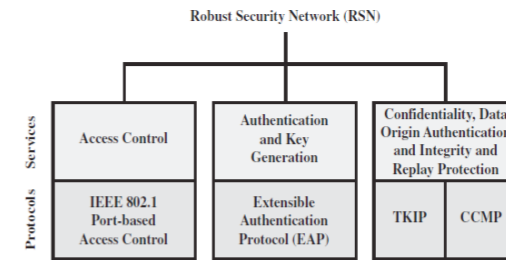
WEP was developed in order to enhance the security level of the IEEE 802.11 wireless LAN protocol, but it was not secure enough and exposed to multiple attacks, including the exhaustive search attacks. Hence, the 802.11i Working Group has developed various functions to address the security issues.

IEEE 802.11i standard specifies user authentication, key exchange, and the enhanced cryptography algorithm for wireless section under the purpose of the wireless user protection. In addition, the IEEE 802.11i made the following features mandatory, meeting its standardization goals: the authentication services described in the IEEE 802.1X, the 4-way handshake key exchange, and the CCMP (Counter Mode With CBC-MAC Protocol) cryptographic algorithm.

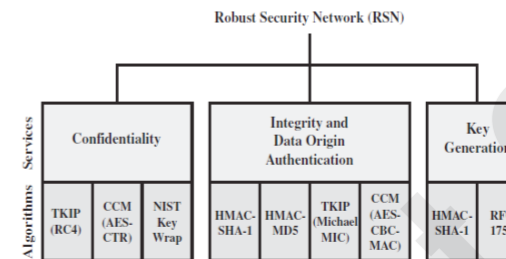
② Components of IEEE 802.11i

IEEE 802.11i security specification defines the following services, and the security and cryptographic protocol suites used for those services are listed in (Figure 54)

- Authentication: provides mutual authentication between a user and an Authentication Server and generates a temporary key to be used between a client and an AP over the wireless link
- Access control: enforces the use of the authentication function, routes the messages properly, and facilitates key exchange, and is able to work along with various authentication protocols
- Privacy with message integrity: encrypted along with a message integrity code to ensure that the MAC-layer data was not altered.



(a) Services and protocols



(b) Cryptographic algorithms

CBC-MAC = Cipher Block Chaining Message Authentication Code (MAC)
 CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
 CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
 TKIP = Temporal Key Integrity Protocol

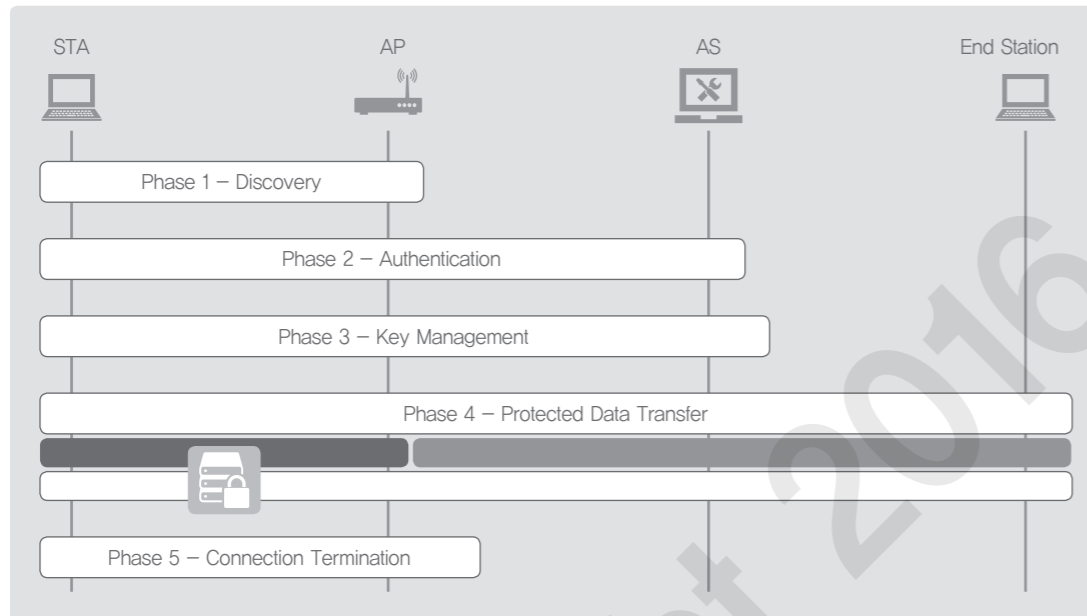
(Figure 54) IEEE 802.11i components

(Source: W. Stallings, Network Security Essentials, Pearson, p.184)

③ IEEE 802.11i operation

IEEE 802.11i operation can vary if the wireless LAN configuration and terminals are different, but in general, it can be explained with the five phases shown in (Figure 55).

- (1) Discovery: An AP broadcasts its IEEE 802.11i security policy. The STA uses this to identify an AP for a WLAN with which it wishes to communicate. The STA associates with this identified AP.
- (2) Authentication: This phase enables mutual authentication between the STA and the AS. The AP does not participate in the authentication transaction other than forwarding traffic between the STA and AS.
- (3) The AS utilizes the RADIUS (Remote Authentication Dial-In User Services) key distribution protocol to transfer the PMK (Pairwise Master Key) to the AP of the STA. After that, the AP and the STA utilize the 802.11x protocol to exchange the message in order to generate and share the cryptographic key.
- (4) Protected data transfer: Frames are securely exchanged between the STA and the end station through the AP. A secure data transfer occurs only between the STA and the AP; the security is not granted end-to-end.
- (5) Connection termination: The AP and STA exchange frames. During this phase, the secure connection is torn down and the connection is restored to the original state.



(Figure 55) IEEE 802.11i phases of operation

(Source: W. Stallings, Network Security Essentials, Pearson, p.185)

04 Security for Application Layer

The following summarizes the security vulnerabilities and the defense measures of widely used protocols of the application layer.

E-mail Security

① E-mail security vulnerability

- Leakage of the content of e-mail: an e-mail is written in plain text and weak to sniffing
- E-mail forgery and manipulation: content of an e-mail can be forged or manipulated
- E-mail spoofing: an attacker can impersonate an authorized user (sender), after a successful spoofing of an e-mail
- Malicious code and spam mails: spam mails sent using the relay function, malicious code distribution, and potential network overload

② Defense measures

- Blocking spam mails: to use a mail client program for spam mail filtering or to configure the mail server as 'spam relay not allowed'. An e-mail policy should be in place: either 'Opt-out' (avoid receiving unsolicited mails after

receiving a mail) or 'Opt-in' (giving permission in advance to senders).

- Blocking malicious codes: to use the 'Class-Map' or 'Policy-Map' in routers, or to use the Virus Wall—a kind of application firewalls
- PGP (Pretty Good Privacy): to be used in the e-mail encryption and decryption and to provide the sender identity verification; an integrity service that provides a digital signature feature
- S/MIME (Secure MIME): to provide security services of authentication, message integrity, non-repudiation, and encryption to securely protect the MIME (which is used for the binary file transfer via e-mails).

FTP Security

① FTP security vulnerability

- Brute force attacks: there is a vulnerability against brute force attacks or guessing attacks targeting the password of FTP users.
- FTP protocol weakness: Exploit Code, which takes advantage of vulnerabilities of the FTP programs and versions, can be used to acquire the ROOT authority.
- Anonymous FTP vulnerability: as all the users have access rights, it is possible to inject a malicious code, if and once the rights to 'Write' are allowed.
- Sniffing: network sniffing can be used to acquire user accounts and passwords.
- FTP bounce attack: it is possible to scan a network port of other hosts indirectly through an anonymous FTP server

② Defense measures

- FTP service should not be encouraged to use unless it is really necessary, and use the Secure FTP only, if it is really necessary.
- Anonymous FTP should not be used, but if it is needed, the rights to 'write' should not be allowed.
- It is recommended to use the up-to-date FTP version (free from vulnerability), considering the recommendation from solution providers
- The '/etc/ftpusers' command is used to describe the users who will not use the ftpd connection. Register the accounts, such as 'Root, Nobody, News, Daemon, Uucp, Bin, Sys, Adm' to the file.

HTTP Security

To provide a web service, a range of protocols, such as FTP, Telnet, HTTP, SNMP, and POP, are used at the same time. Among them, HTTP can be regarded as a main protocol in providing a web service. Those protocols are usually covered under the theme of web security. The Open Web Application Security Project (OWASP), an open community, selects 10 security vulnerabilities pertaining to the web applications and introduces measures to address them every two years.

① HTTP security vulnerability

- GET request type: highly vulnerable as data are presented in the address input area
- Main vulnerabilities in the HTTP request: SQL injection vulnerability, XSS vulnerability, file upload vulnerability,

URL/Parameter manipulation, Cookie/Session manipulation, access control vulnerability, and brute force attacks.

- Main vulnerabilities in the HTTP response: vulnerability in environment configuration (directory listing), vulnerability in core information gathering (Google attacks), file download vulnerability, and unnecessary files.

② Defense measures

- To use a web–firewall
- To apply secure coding to web applications
- To strengthen the security configuration for web servers

DNS Security.

① DNS security vulnerability

- Server list exposure: the list of all the servers can be exposed because of inadequate security readiness in DNS servers
- Version exposure: the version of the servers can be exposed because of inadequate security readiness in DNS servers
- DNS pharming attacks: a forged IP address is placed in the DNS server to redirect the traffic to a bogus site.
- DDoS attacks: operators usually run only two or so DNS server machines, making them vulnerable to the DDoS attacks.

② Defense measures

- To configure the DNS server not to transfer the server list
- To correct the security configuration regarding the version exposure
- To secure availability by using multiple or high–performance DNS servers
- To adopt the DNSSEC (DNS Security Extensions), an update to address the DNS vulnerabilities

Example Question

Question

Descriptive question

Question

Company A would like to have more web–based transactions with its general customers. At the same time, Company A would like to have more stringent access control to its core information resources, such as the database located on the corporate network. Describe two solutions that are usually used to meet these requirements.

Intent of the question

To evaluate the level of understanding and skill set about security solutions that can be used to enhance the network security level of a company.

Answer and explanation

1) Firewall

2) Intrusion detection system

To evaluate the level of understanding and skill set about security solutions that can be used to enhance the network security level of a company.

- 1) A firewall is located between a private network and a public network under the purpose of preventing attacks or intrusions against the company's internal network resources and keeping the internal network and various other servers secure.
- 2) IDS is installed within the corporate network in order to detect unauthorized and abnormal behaviors, to assess those detected abnormal behaviors, and to block intrusions on a real time basis.

Related E–learning Contents

- [Lecture 2 Network Security](#)

IV

Security Readiness for Safer System Management

▶▶▶ Latest Trends and Key Issues

As hacking technologies have recently gotten more sophisticated and intelligent, we have started to find ourselves in difficulties in tackling cyber attacks with the existing security techniques, such as a firewall and an intrusion detection system. In particular, there is nothing that can fully forestall illegitimate attempts to take away a system administrator's control or inappropriate accesses to information resources/assets by an internal user. Against this backdrop, there are growing interests in the Secure OS which is an operating system that has evolved from the existing OS by employing the Security Kernel that is responsible for performing security functions, such as controlling access to the system, providing security features, and protecting the system from various hackings.

▶▶▶ Study Objectives

- * To be able to explain about access control policies and security models
- * To be able to configure security settings in the Windows system
- * To be able to configure security settings in the UNIX and LINUX systems

▶▶▶ Practical Importance Medium

▶▶▶ Keywords

Access control, Identification, Authentication, Authorization, Mandatory Access Control (MAC), Security Level, Security label, Discretionary Access Control (DAC), Role Based Access Control (RBAC), Brute force attack, Password crack, UMASK, Daemon, Anonymous FTP, Secure FTP, Secure OS, Security kernel, Reference monitor

+ Practical tips

On March 20, 2013, Korean major broadcasters and financial institutions experienced a series of cyber attacks, ending up with their systems being paralyzed. Starting at 2 p.m. on that day, three broadcasters and four financial institutions had fell into the chaos as their internal computing systems had been paralyzed at the same time. Chances are high that the paralyzed systems were caused by the cyber terrorists, given the fact that the companies in the similar business experienced this attack simultaneously. Based on this assumption, the police started investigation. According to the Korea Communications Commission, it was found out that malicious codes were distributed through the Patch Management Server (PMS). It announced that the extent of the damage is immeasurably serious. Financial institution A, one of the victims, analyzed that this cyber terror happened because of the following three reasons.

- 1) Security of administrator PCs was poorly managed and the server was widely open, not only to an administrator's IP address.
- 2) Poor security patch and weak authentication in the update server
- 3) No control over the use of default passwords and unnecessary commands

In this chapter, we will learn how to configure security settings, considering the nature of each system in order to effectively tackle cyber attacks such as the attack that caused damage to the Company A. In addition to that, we will take a look at how to securely manage those systems.

01 Access Control

Outline of Access Control

① Concept of access control

Access control is a technique that regulates interactions between a user and a system. It defines exactly who can interact with the system and what the user may do during that interaction. There are three key components of access control: identification, authentication and authorization.

② Identification

The process by which a subject identifies itself to the system, using its unique label, and the system identifies the

subject e.g.) ID, employee card, biometrics

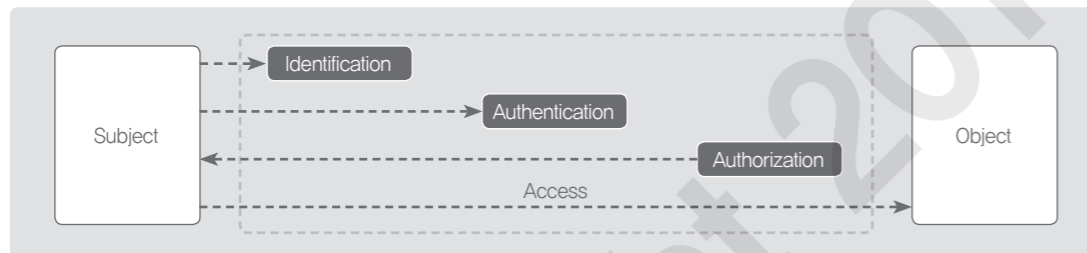
③ Authentication

The process by which a subject verifies its identity to the system and the system authenticates the subject e.g.) password (what you know), certificate (what you have), OTP (what you have), biometrics (what you are)

④ Authorization

The process by which the system determines what a subject can do and what objects he/she can access. e.g.) Mandatory access control, discretionary access control, role-based access control

⑤ Steps for access control: a subject goes through three steps – identification, authentication, and authorization – through the access control system and is finally authorized to gain access to an object.



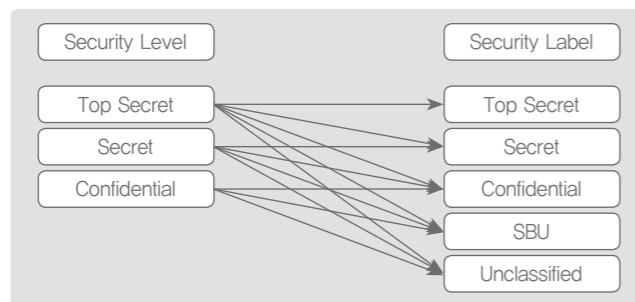
<Figure 56> Steps to access control

Access Control Model

Access control model is a set of policies that govern the access control system in which only an authorized user can have access to the information resources. There are widely used access control models, such as Mandatory Access Control, Discretionary Access Control, and Role Based Access Control.

① Mandatory Access Control (MAC)

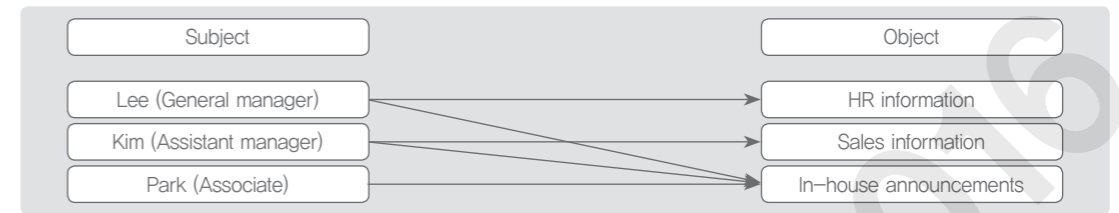
Mandatory Access Control is a model in which a security level is assigned to a subject, while a security label is assigned to an object. Based on the prescribed rules, the MAC model determines whether the subject can gain access to the object. It is mainly suited for military purposes; provides strong security guarantees in the system, but is inefficient in management.



<Figure 57> Mandatory access control

② Discretionary Access Control (DAC)

Discretionary Access Control is a model that determines whether to grant an access to an object, based on the identity of a subject or a group which the subject belongs to. The access to an object is defined by the object owner. It is generally employed for the access control in the UNIX or LINUX systems.



<Figure 58> Discretionary access control

③ Role Based Access Control (RBAC)

Role Based Access Control is a model in which roles are assigned to a subject by an administrator; the relationship between each object and each role is mapped first and the role is assigned to a certain subject. This model is well suited for frequently-changing organizations or systems. While it is efficient in management, its security is hardly guaranteed.



<Figure 59> Role base access control

02 Security for Windows System

Outline of Security for Windows System

Windows system is one of the widely-used operating systems for PCs. Its security needs to be well managed in various areas, such as the management of accounts and passwords, access control, system security, service security, monitoring, and other security management activities.

〈Table 26〉 Windows system security

Classification	Details
Management of accounts and passwords	<ul style="list-style-type: none"> Account-related checkup (unnecessary accounts, accounts with the administrator's privilege) Password-related checkup (insecure password, encryption, automatic account lockout for invalid password attempts, maximum password age, etc.)
Access control	<ul style="list-style-type: none"> Checkup of the access control setting (shared folder, remote registry access, automatic screen lock, etc.)
System security	<ul style="list-style-type: none"> Checkup of the permission setting (permission for system directory, permission for Windows accounts, system utilization, etc.)
Service security	<ul style="list-style-type: none"> Disable services (unnecessary services, terminal service, anonymous FTP, SNMP setting, etc.)
Monitoring	<ul style="list-style-type: none"> System audit policy, logging configuration, etc.
Others	<ul style="list-style-type: none"> Security setting, content of scheduling, vaccines use Y/N, checkup of the latest patches

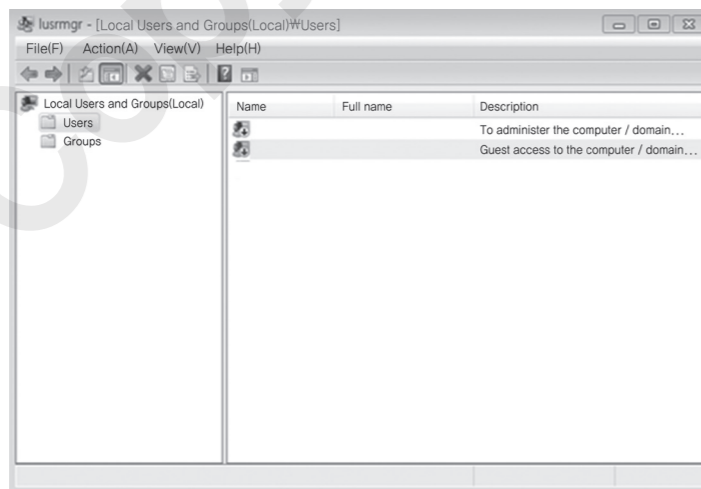
Management of Accounts and Passwords

① Deletion of guest and unnecessary accounts

The use of guest accounts should be refrained. When an access needs to be granted to many unspecified individuals, a general user account should be created and used, instead of a guest account. The guest and unnecessary accounts should be deleted in the lusrmgr (Local Users and Groups).

- How to delete unnecessary accounts

On the [Start] menu, in the [Search programs and files] box, type in lusrmgr.msc. Open the [Local Users and Groups] and delete guest accounts and unnecessary accounts.



〈Figure 60〉 Deletion of unnecessary accounts

② Account lockout setting

To enhance the system security, the account lockout in the security policy setting needs to be configured to limit the number of invalid logon attempts. It is helpful to check-up and configure the account lockout policy to prevent the Brute Force attacks or password cracking.

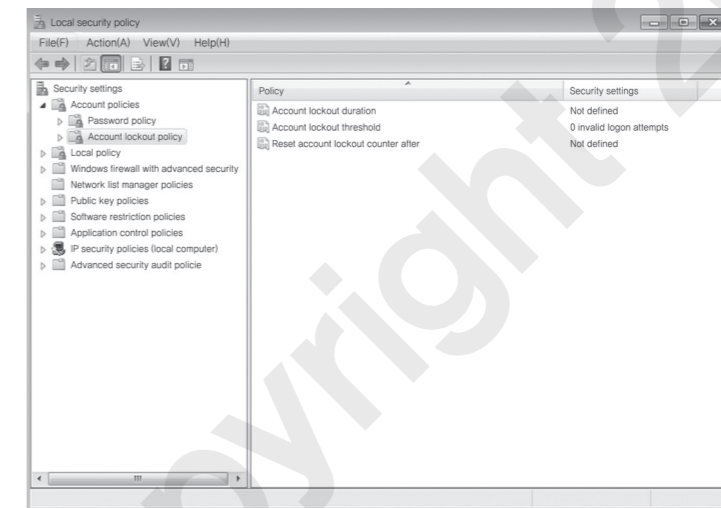
The most ideal configuration in the account lockout policy is 60 minutes in the [Account lockout duration], 5 times in the [Account lockout threshold], and 60 minutes in the [Reset account lockout counter after].

- How to configure the account lockout setting

On the [Start] menu, in the [Search programs and files] box, type in Secpol.msc.

Click the [Account policies] menu and then, click its submenu the [Account lockout policy].

Set the value for the [Account lockout duration], [Account lockout threshold], and [Reset account lockout counter after].



〈Figure 61〉 Account lockout setting

Access Control

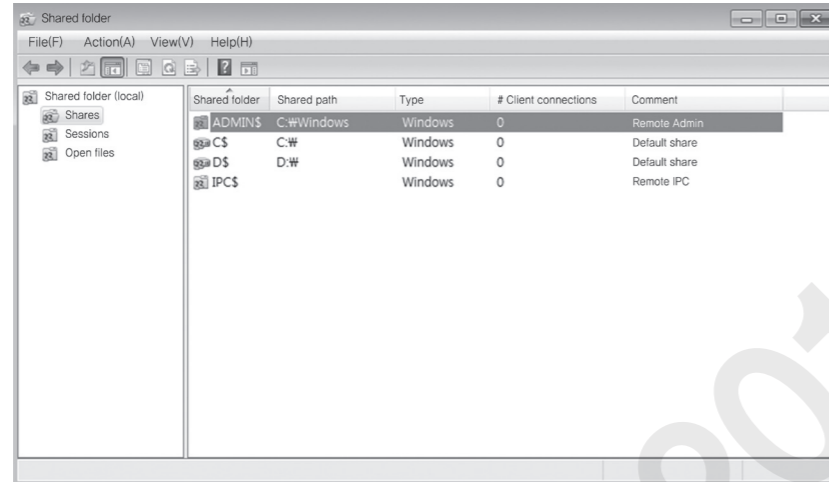
① Checking-up and disabling of unnecessary shared folders

Unnecessary shared folders can lead to the spread of malicious codes or viruses. Therefore, unnecessary shared folders should be disabled. In case when it is inevitable to use the shared folder, the access rights should be allowed only to the authorized users. Shared folders need to be monitored by using the Fsmgmt and unnecessary shared folders should be disabled.

- How to disable unnecessary shared folders

On the [Start] menu, in the [Search programs and files] box, type in Fsmgmt.msc.

Look into whether there are any unnecessary shared folders and disable them if there is any.



〈Figure 62〉 Disabling of unnecessary shared folders

System Security

① Disabling of administrator's automatic logon

Autologon function is susceptible to an attack, as it can be misused by an attacker to learn a login account and password from the Windows registry, using some hacking tools. Therefore, the Autologon function needs to be disabled and the value of AutoAdminLogon in the Windows registry should be set to 0.

- How to disable administrator automatic logon

On the [Start] menu, in the [Search programs and files] box, type in Regedit.

Then, set the value of the AutoAdminLogon (in the HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon) to 0.

If the DefaultPassword entry is present, delete it.

② Checkup of startup programs

Startup program folder is a place where there is a list of programs that automatically start at the boot-up. However, in many cases, a malicious code adds its copies in this folder, so that it enables the malicious code to start every time a computer starts up. Therefore, unauthorized or unnecessary programs should be deleted from the startup program list.

- How to delete startup programs

- On the [Start] menu, in the [Search programs and files] box, type in 'Msconfig'
- When the system configuration utility dialogue box is open, click the [Startup] tab.
- From the Startup tab, uncheck (unmark) the box next to unauthorized programs or unnecessary programs. Click the [OK] button.
- The message asking for restarting the system will pop up. Click the [Restart] button.

Service Security

① 2.5.1 Disabling of unnecessary startup services

There are some unnecessary startup services installed and executed by default. They make the system susceptible to security attacks or waste system resources. Therefore, the unnecessary startup services need to be disabled. It is desirable to disable the services that are installed by default, if they are not for specific purposes. A system administrator is required to clearly understand the purpose of the systems, and then remove the services that turned out to be unnecessary.

- How to disable unnecessary startup services

- On the [Start] menu, in the [Search programs and files] box, type in 'Services.msc'
- To disable the unnecessary services in the registry, change the "Startup type" of the service to "Disabled".

Checkup of Terminal Services

Terminal service is a tool used for the management of remotely located servers. However, it can be misused for hacking when the password is insecure or access control is not properly managed. Therefore, terminal services should be carefully checked up and ones that turned out to be unnecessary should be disabled. In case when terminal services are inevitably required, the encryption level should be set to "Medium" or higher.

03 Security for UNIX systems

Outline of Security for Unix-like Systems

The Unix family of operating systems that are widely used for the server includes Unix and Linux. Its security needs to be well managed in various areas, such as the management of accounts and passwords, access control, system security, service security, monitoring, and other security management activities.

〈Table 27〉 Security for Unix-like systems

Classification	Detail
Management of accounts and passwords	Account-related checkup (unnecessary account, account with Root's right)
	Password-related checkup (insecure password, encryption, automatic account lockout for invalid password attempts, maximum password age, etc.)
Access control	Checkup of the access control setting (access of authorized PC/user, encryption for remote access, session termination time, etc.)

Classification	Detail
System security	Checkup of the permission setting (user environment setting, main directory and files, booting script, etc.)
Service security	Disable services (unnecessary services, NFS setting, Anonymous FTP, SNMP setting, etc.)
Monitoring	Logging configuration, checkup of CPU/file system utilization
Others	Access warning message, content of scheduling, checkup of the latest patches

Management of Accounts and Passwords

① Deletion of unnecessary accounts

In many cases, default passwords are given and used for the default accounts generated when the OS or package is installed. However, default passwords are vulnerable to the password guessing attacks. Therefore, accounts, which are unused for sure or suspicious, need to be deleted. As for the system accounts that generally do not need a login, any login attempts should not be accepted.

• How to delete unnecessary accounts

- In SUN/HP-UX, # userdel [lp | uucp | nuucp | account to be deleted]
- In AIX, # rmuser [lp | uucp | nuucp | account to be deleted]

② Checkup of accounts that use insecure passwords

Setting an insecure password for an account, which is easy to guess, may grant an unauthorized user a permission to access the system. The password should contain a minimum of eight characters which are neither identical nor similar to the account, including alphabets, numbers, and special characters.

• How to check up the accounts that use insecure passwords

- In the case of SUN, add "TIMEOUT=300" (which means the user session is expired when it is idle for more than 300 seconds) in the "/etc/default/login" file.
- For HP-UX, AIX and Linux, add "TMOUT=300, export TMOUT" in the /etc/profile file or .profile file.

Access Control

① Access granted only for authorized systems

Inetd daemon is responsible for starting the daemons of internet services, which are internal programs registered in the /etc/inetd.conf file, when a request comes from an external network. When the access control setting in the inetd.conf(xinetd.d) file is inappropriate, an unauthorized user can register a malicious program in this file and execute it with the Root's rights. Therefore, the lists of authorized and unauthorized users should be added into the /etc/hosts.allow file and /etc/hosts.deny file respectively.

② Session idle timeout setting

If there is no timeout set for idle sessions, it can undermine not only the confidentiality but also the availability. Therefore, the connection to the server should be cut off when the user session is idle longer than the prescribed session idle timeout.

• How to set the session idle timeout

- In the case of SUN, add "TIMEOUT=300" (which means the user session is expired when it is idle for more than 300 seconds) in the "/etc/default/login" file.
- For HP-UX, AIX and Linux, add "TMOUT=300, export TMOUT" in the /etc/profile file or .profile file.
- HP-UX, AIX, Linux에서는 /etc/profile 또는 .profile 파일에 "TMOUT=300, export TMOUT" 을 추가한다.

System Security

① Setting of permission for user environment configuration file

The /etc/profile file is a login script that is used to set environment variables for all users who log in. When the access control setting over the /etc/profile file is inappropriately set, unauthorized users can illegitimately get access to the file and alter the user environment, using various techniques. Therefore, the access control for the /etc/profile file should be limited only to the Root (Bin) user and the write permission of other users should be restricted.

• How to delete other users' permission over the /etc/profile file

- # ls -al /etc/profile
- # chown root /etc/profile
- # chmod o-w /etc/profile

② UMASK setting

To find out what is the Umask setting of the current user, run the command "Umask" from the command prompt. The value should be set to "027" or "022". If the value is 027, a newly created file gets an "rw-r-----" permission. If the value is 022, a newly created file gets an "rw-r--r--" permission. To avoid unnecessary accesses, the UMASK should be set to 022.

• How to setup UMASK

- In the SUN system, delete the # (comment) of UMASK option in the /etc/default/login file and make sure that the Umask is set to 022. In other UNIX operating systems, add "Umask 022" in the .profile.

Service Security

① Disabling of unnecessary services

Letting unnecessary service ports open makes the system vulnerable to security attacks. Therefore, unused services should be deleted. The following table shows the list of daemon services and service ports that need to be checked out for potential disabling.

〈Table 28〉 List of daemon services and service ports to be checked up

Classification	Details
Echo (7)	Simple retransmission of the received messages
Ehargen (19)	A service of returning a string of fixed length
Finger (79)	Print out user information
Nntp (119)	NNTP(Network News Transfer Protocol) A standard service that can create discussion groups on the Internet
Netbios_Dgm (138)	NetBIOS Datagram service; used to broadcast to hosts, groups, or all.
Ldap (389)	A service used for directory service access
Ntalk (518)	A service that enables chatting among different systems.
Ldaps (636)	LDAP over SSL
Nfsd (2049) –NFS	If not in use, NFS server daemon service
Discard (9)	A service that discards the data received from a certain user
Time (37)	TCP version of the RFC 868 time server that is used by Rdate daemon
Sftp (115)	FTP over SSH
Ntp (123)	Ntp (Network Time Protocol) responsible for synchronizing times of a client and a server
Netbios_Ssn (139)	NetBIOS Session service; used to transmit/receive actual data, using network sharing and the like
Printer (515)	Used for spooling of a remote printer
Uucp (540)	Used to copy files between different Unix systems and to send commands that will be executed on a different system
Ingreslock (1524)	A service used to lock Ingre database
Dtspcd (6112)	A daemon service used to control sub processes of the common desktop environment
Daytime (13)	A daemon that prints out the current time and date in ASCII characters in response to the client's question
Tftp (69)	A protocol for file transfer
Uucp-path (117)	Uucp path service
Netbios_ns (137)	NetBIOS name service; used to identify resources on the network
Bftp (152)	Binary File Transfer Protocol
Talk (517)	Used to enable a user to remotely access a system; and to initiate a talk session with another user logged into a different system
Pcserver(600)	ECD Integrated PC board svr, used for RPC-related attacks

② Restriction on anonymous FTP and use of secure FTP

Anonymous FTP can result in malicious users stealing information about the system. It is especially susceptible to various attacks when it allows the anonymous user to write into the directory. Therefore, the use of the anonymous FTP should be limited only to authorized users and the use of the Secure FTP is recommended instead of insecure FTPs.

The use of the anonymous FTP or general FTP (in this case, an account needs to be created) is prone to security breaches, because the user authentication information is in plain text, without encryption, and the FTP protocol itself is insecure by nature. In other words, in the FTP environment, it is possible for a malicious user to get a control over accounts through the brute force attacks or sniffing attacks that exploit the FTP's vulnerability of log-in authentication. Therefore, when you write an FTP program for file transfer, the SFTP server should be installed instead of the FTP server and the FTP client program also needs to be written by using the SFTP.

• How to apply SFTP, using Java

– SFTP open source library can be employed to write the SFTP client program, using Java. To do so, the Commons-Net library needs to be downloaded from the Apache open source project site (<http://commons.apache.org/proper/commons-net/>). After installing the library, the SFTP client program can be written as follows.

```
//library import
import org.apache.commons.vfs2.FileObject;
import org.apache.commons.vfs2.FileSystemOptions;
import org.apache.commons.vfs2.Selectors;
import org.apache.commons.vfs2.impl.StandardFileSystemManager;
import org.apache.commons.vfs2.provider.sftp.SftpFileSystemConfigBuilder;
//FTP connection and file download
StandardFileSystemManager manager = new StandardFileSystemManager();
String sftpUri = "sftp://" + userId + ":" + password + "@ " + serverAddress + "/" +
remoteDirectory + fileToFTP;

FileObject localFile = manager.resolveFile(file.getAbsolutePath());
FileObject remoteFile = manager.resolveFile(sftpUri, opts);
remoteFile.copyFrom(localFile, Selectors.SELECT_SELF);
```

• How to apply SFTP, using "C"

SFTP open source library can be employed to write the SFTP client program, using C. To do so, the Libssh2 library needs to be downloaded from the libssh2 site (<http://www.libssh2.org/>). After installing this library, the SFTP client program can be written as follows.

```
//library include
#include "libssh2_config.h"
#include <libssh2.h>
```

```
#include <libssh2_sftp.h>
//FTP connection and file download
session = libssh2_session_init();
libssh2_userauth_password(session, username, password);
libssh2_sftp_open(sftp_session, sftppath, LIBSSH2_FXF_READ, 0);
libssh2_sftp_read(sftp_handle, mem, sizeof(mem));
```

04 Secure OS

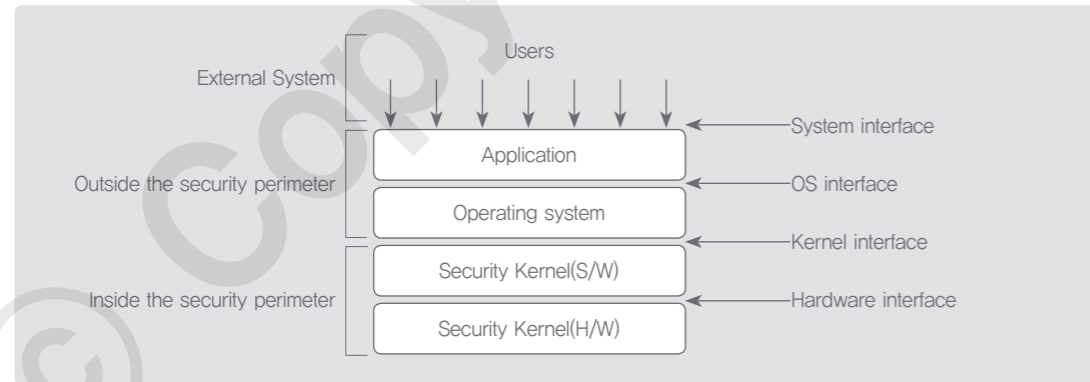
Outline of Secure OS

① Concept of Secure OS

Secure OS is an operating system that has evolved from the existing OS by employing the Security Kernel, which can provide security functions. It is aimed to protect computing systems from various hacking attempts that exploit security flaws in a computer's operating system. In the Secure OS, decisions on the access control over file systems, devices, and processes are made at the kernel-level.

② Architecture of Secure OS

Components within the security perimeter in the Secure OS are the security kernel H/W and security kernel S/W. Like the existing OS, the Secure OS has application programs running on the operating system, outside the security perimeter.

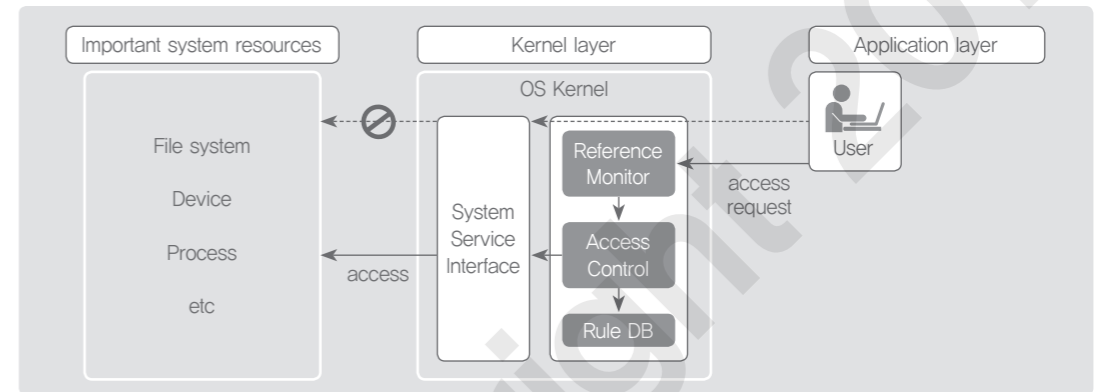


<Figure 63> Architecture of Secure OS

Security Mechanism and Key Functions Of Secure OS

① Security mechanism of Secure OS

- Access request to important system resources
A user sends a request for the access to important system resources to the Reference Monitor, a core component of the Secure OS, using application programs.
- Access Control
The Reference Monitor makes a decision on the access request sent by the user, based on the predefined rules, called the Rule DB, and sends the access request to the System Service Interface.
- Access to important resources
The System Service Interface grants the access to important system resources in accordance with access control rules.
The access request, which is not sent via the Reference Monitor, is not accepted by the System Service Interface.



<Figure 64> Security mechanism of Secure OS

② Key functions of Secure OS

<Table 29> Key functions of Secure OS

Functions	Details
User authentication	Digital signature authentication based on the kernel functions of the OS
Access control policy	Mandatory Access Control (MAC) and Role Based Access Control (RBAC) that conduct a comparison of security levels between an object and a subject
Intrusion protection	Automatic detection of and defense against the DOS and DDOS attacks Automatic detection and blocking of unidentified buffer overflow attacks
Host firewall	Host-based firewall security policies, using the packet filtering
Security audit	Audit logging at the kernel level

Example Question

Question type

Short-answer question

Question

Company A plans to introduce an access control policy. After reading the Company A's characteristics and requirements, answer the following questions.

- (1) What is the access control model best suited for Company A?
- (2) Explain the reason for the answer to the question (1).

Characteristics: The organizational structure and the system of Company A are frequently changing.
Requirement: It seeks efficiency in management, even if it undermines security a little bit.

Intent of the question

To check whether a learner understands the access control models and how to apply the models to the actual environment

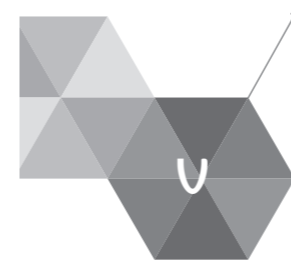
Answer and explanation

- (1) RBAC, Role Based Access Control
- (2) For Company A which experiences frequent changes in its organization and system, the Role Based Access Control is the most suitable model because the model provides efficiency in management, even though it undermines security a bit.

Role Based Access Control is a model in which roles are assigned to a subject by an administrator; the relationship between each object and each role is mapped first and the role is assigned to a certain subject. This model is well suited for frequently-changing organizations or systems. While it provides efficiency in management, its security is hardly guaranteed.

Related E-learning Contents

- Lecture 5 System Security
- [Advanced] Lecture 1 Utilize Cryptographic Algorithm
Lecture 2 Apply Secure Coding Techniques



Managing Database Securely

▶▶▶ Latest Trends and Key Issues

The Personal Information Protection Act was modified and approved in the National Assembly of South Korea as of Feb 28 of 2014, which mandates encryption when storing the social security number of Korean citizens (Korean PIN, hereinafter). The intention of the legislation is to minimize the potential damage from personal information leakages and, to that end, to mandate parties handling personal information to encrypt the Korean PIN. The presidential decree regarding the law specifies the objects of encryption and the timing for the enforcement, considering the volume of the personal information and the potential impact in case of a breach. However, encrypting the Korean PIN can cause a lot of costs and can negatively impact on the systems; system errors and performance slowdown. Because of these concerns, it has been delayed to put the law into practice. These kinds of social and administrative changes brought about increasing interest and attention in the database encryption.

▶▶▶ Study Objectives

- * To be able to explain about the database security requirements
- * To be able to explain about the factors to be controlled for the database security
- * To be able to select the objects for the database encryption and to apply the encryption technology to the targets

▶▶▶ Practical Importance High

▶▶▶ Keywords

Virtual table (Views), Database access control, Agent-based access control, Gateway-based access control, Sniffing access control, API approach, Plug-in approach, TDE approach, Master key, Key lifecycle, HSM(Hard Security Module), Random number generator

+ Practical tips

A lot of information, from personal information to corporate confidential information, is stored within a database. Hence, the database is an important asset to be protected for an organization, and a core target for an attacker. It is necessary, therefore, to understand a range of security threats posed to the database, to come up with the database access control and encryption policy, and to devise diverse protection measures.

Company A asked for a consulting service company to devise the measures for the access control and encryption, with the following requirements.

- 1) Flexible approach in the database access in order to catch up with the flexible organizational changes and frequent changes in its functions and roles
- 2) Encryption for personally identifiable information within the timeline and in compliance with the methods stipulated in the revised Personal Information Protection Act
- 3) Impact analysis: the encryption for personally identifiable information should not cause any system errors or performance slowdown

We will take a look at what kind of database access control can be desirable, what measures should be used for the encryption of personally identifiable information, and what other considerations there can be.

01 Outline of Database Security

Introduction to Database Security

① Three principles of database security

Database security means the managerial, physical, and technical protection against leakage, manipulation, or destruction of information in order to assure confidentiality, integrity, and availability of information within a database

The level of DB performance mattered most in the past, but a secure management of the DB and data protection are deemed more important these days, showing the fact that the value of data has started to carry more significance, thanks to the development of IT services. A lot of information, from personal information to corporate confidential information, is stored within a database; it is an important asset to be protected for an organization, and a core target for an attacker.

〈Table 30〉 Three principles of database security

Three principles	Details	Implementation
Confidentiality	<ul style="list-style-type: none"> • To prevent the information stored in the database from being leaked out • To allow only the authorized users to have access to the database and to see the information 	DB authority management DB encryption
Integrity	<ul style="list-style-type: none"> • To allow only the authorized users to modify the information stored in the database 	DB authority management
Availability	<ul style="list-style-type: none"> • To ensure continuous and non-stoppable database services 	DB redundancy

② Necessity for database security

- Database security for sustainable management

There have been a series of attacks to and personal information leakage from H-capital, S-portal, N-game, and K-telecom, showing the great importance of database security. It can be said that database security is a prerequisite for sustainable business because a database breach can cause a huge amount of financial losses, bring down the trust of customers, and eventually threaten the very existence of a company.

- Database security for regulatory compliance

There has been a growing importance on database security as showcased by the mandates from relevant laws and regulations, such as the Personal Information Protection Act, the Act on Promotion of Information and Communication Network Utilization and information Protection, etc., and the Electronic Financial Transactions Act. Hence, it is of significant importance to fully comply with those laws and regulations.

Sources of Database Security Threats and Responses

① Database security threats

Database security threats come in various forms, but the general threats to the database security that may occur in an organization can be categorized into four areas as follows.

〈Table 31〉 Database security threats

Threats	Details
Web security threats	An unauthorized attacker from the outside can acquire information in an unauthorized way by using the SQL injection attacks or file upload & web shell.
Weak security in identification and authentication	To acquire an authorized user's identity by repeated trials of authentication and by using social engineering techniques
Data leakage	To acquire information illegally: stealing unencrypted data or decrypting the stolen encrypted data
Misuse of cryptographic module	To use a cryptographic module (whose security level is not proven), or to decipher a ciphertext with an inadequate cryptographic mode

② Response to database security threats

Access control, virtual table (view), and encryption can be used in order to avert the threats against the database.

〈Table 32〉 Responses to database security threats

Classification	Details	Examples
Access Control	Only authorized users can gain access to the DB Unauthorized users blocked from the DB access	Account management MAC, DAC, RBAC
Virtual table (Views)	To limit the access areas by using virtual tables: access only granted to the area where he/she got the permission	CREATE VIEW
Encryption	Important data to be stored with one-directional or bi-directional encryption algorithm	SEED, AES SHA-256

02 Database Access Control

Policy for Database Access Control

① Policy for discretionary access control (DAC)

DAC is a method used to determine whether to grant an access to an object, based on the identity of a subject or a group the subject belongs to. The access to an object is defined by the object owner.

For example) The owner of a table can grant the authority to others or revoke the authority from others.

② Mandatory access control (MAC)

MAC is to constrain the ability of a subject to have access to an object which has confidential information, based on the authority the subject has for the object.

For example) Only the DB administrator can have access to the System Catalog.

③ Role-based access control (RBAC)

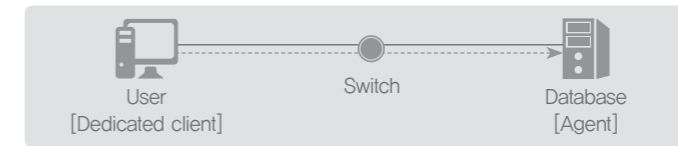
A central administrator controls the relationship between a subject and an object, and grants the access authority based on the roles predefined within the organization.

For example) The role of a DBA is first defined, and a certain employee will get the DBA role and relevant authority.

Implementation Methods of DB Access Control

① Agent-based approach

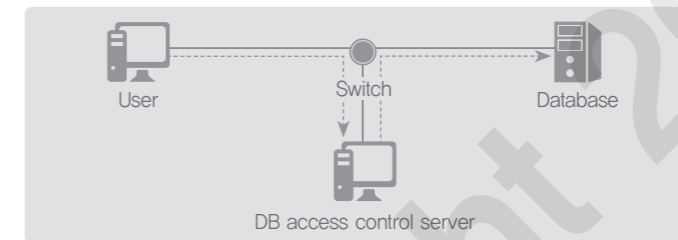
Agent-based approach is a method to install an agent on the DB server to deliver the access control service and logging functions, which means a dedicated client should be used to get access to the DB. A strong access control is in place, but it causes a lot of traffic on the DB server and eventually triggers a performance slowdown.



〈Figure 65〉 Databases access control: agent-based

② Gateway-based approach

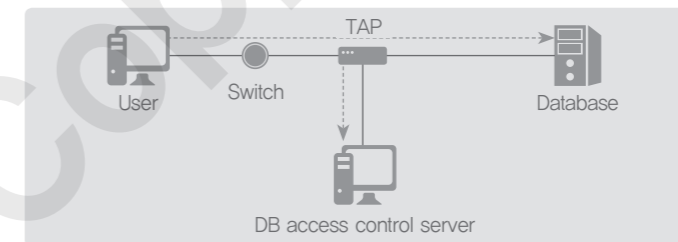
In the gateway-based approach, all the DB server connection requests are directed to the DB access control server (proxy server), which provides the most powerful access control. The DB access control servers can be built with redundancy, not causing any business impacts in case of a system failure.



〈Figure 66〉 Database access control: gateway-based

③ Network switch-based approach

As for the packets over the network, the packet analysis and logging are conducted by using devices such as TAP. There is no need for an agent between a DB server and a client. It is easy to implement without causing the load on the network, but it is difficult to fundamentally prevent potential damages to the data integrity because of unauthorized manipulations.



〈Figure 67〉 Database access control: network switch-based

④ Hybrid method

The hybrid method is generally used in implementing a system for the DB access control in order to overcome the weakness of individual methods explained above. The typical combination can be: agent+gateway, gateway+network switching, agent+gateway+network switching.

03 Database Encryption

Factors to be Considered in Database Encryption

When applying an encryption mechanism on a database, several factors should be considered: which data column should be encrypted, which encryption algorithm will be used, what kind of performance impacts it will bring about, and how the encryption key should be managed.

<Table 33> Factors to be considered in database encryption

Factors	Details
Object and methods of encryption	Select the data defined in the local laws and regulations and other critical data as a top priority for encryption
Encryption algorithm	Algorithms that are recommended by local and international research institutes should be used: one directional algorithm for passwords (SHA-256 or higher), and bidirectional algorithm for other information (SEED, ARIA, AES, and the like).
Search and performance	Need to consider the performance, such as index maintenance, and need to consider the partial encryption as an option.
Encryption key management	A safe key management is required throughout the lifecycle of encryption & decryption keys and master keys. (From creation to disposal)

Object for Database Encryption and Relevant Methods

Data defined in the local laws and regulations and other critical data should be selected as a top priority for encryption. Depending on the type of laws and regulations, the mandatory objects for encryption can vary: password, bio information, Korean PIN, passport number, driver license number, foreigner registration number, credit card number, account number, and transaction logs. A set of encryption methods should be selectively used and a relevant algorithm should be selected for the DB encryption and decryption, considering the nature of the information.

<Table 34> Object for database encryption and relevant methods

Classification	Target	Encryption method
Common	Password	To be stored with one directional encryption algorithm
Personal Information Protection Act	Passport number	To be stored with a secure bi-directional encryption algorithm
	Driver license number	
	Foreigner registration number	
	Korean PIN	
	Bio information	

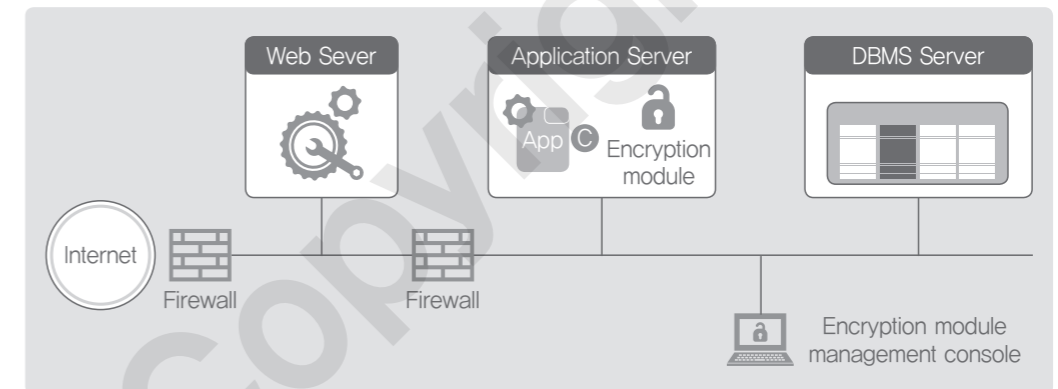
Act on Promotion of Information and Communication Network Utilization and information Protection, etc.	Korean PIN	To be stored with a secure bi-directional encryption algorithm
	Account number	
	Bio information	To be stored with one directional encryption
Electronic Banking Regulation of the Financial Supervisory Service	Transaction log	To be stored with encryption

Types of Database Encryption

There are generally used database encryption technologies, such as API, plug-in, or TDE. In addition, the hybrid approach (API+plug-in), proxy-based approach, and many other methods can be used.

① API -based approach

API-based approach is to install a module for encryption and decryption within an application program server, and this approach requires a lot of application modifications. The communications between the AP server and the DB server is encrypted. This approach is not likely to generate a burden on the DB, but highly likely to impose the loads on the AP server.

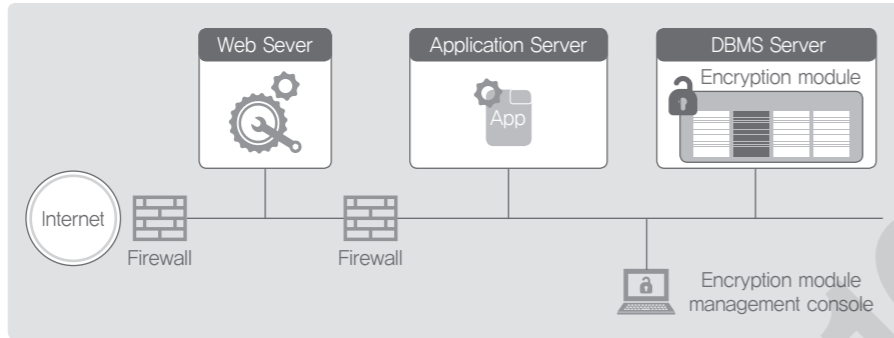


<Figure 68> Database encryption: API-based approach

This approach can be recommended when it is easy to modify application programs and the DB server performance is not good, because encrypted data is sent and received securely even on the network segment.

② Plug-in approach

Plug-in approach is to install a module for encryption and decryption within a DB server. This approach can cause a burden on the DB server when encryption and decryption are applied to the DB, and the data between the AP server and the DB server is transferred in plain text.

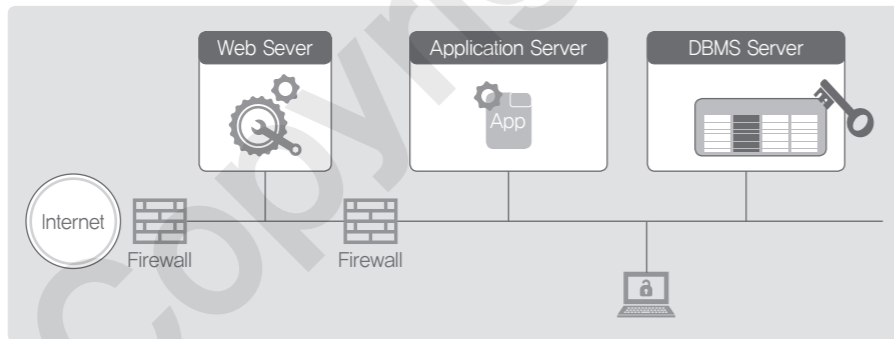


<Figure 69> Database encryption: plug-in approach

This approach can be recommended when it is difficult or impossible to modify application programs and the DB server performance is good.

③ TDE approach

This approach uses the encryption and decryption functions embedded or come as an option within the DBMS. Those functions can vary, depending on the types and versions of the DBMS. As these functions are operated at the DBMS kernel level, there is no modification required at the application level. However, these functions might not be supported for a certain type or version of the DBMS. This approach can be considered when an organization decided to introduce a new DBMS.



<Figure 70> Database encryption: TDE approach

How to Apply Encryption Algorithms for Database

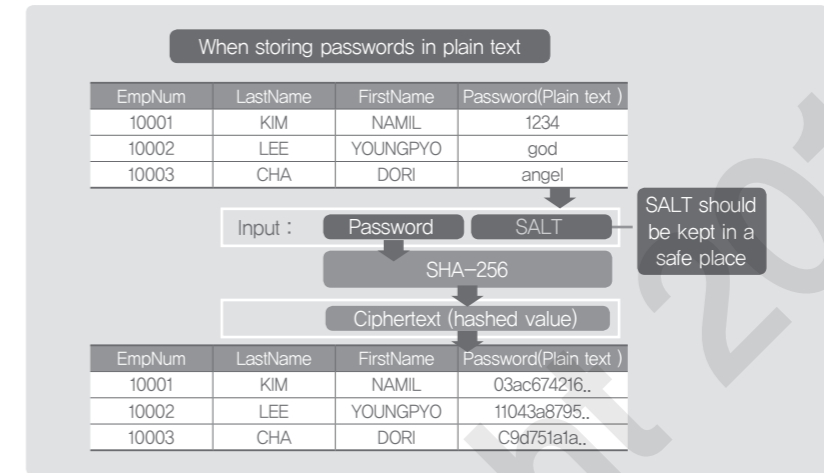
One directional and bi-directional encryption algorithms can be employed in a database as explained below.

① One directional encryption algorithm

Data, such as passwords, need to be stored by using the hash function algorithm (one directional) so that it is not computable to predict the original text. The commonly used hash algorithms are the SHA-256 or higher versions. At a high level, there can be two main cases when one directional encryption should be used: 1) data are stored in plain text in the existing database; and 2) insecure algorithms are in use (such as MD5 or SHA-1)

• When passwords are stored in plain text

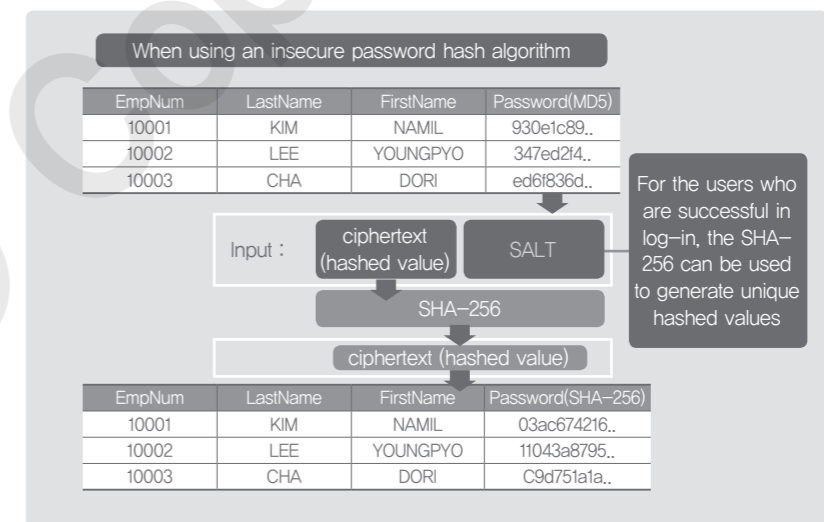
When passwords are stored in plain text, the passwords can be vulnerable to the dictionary attacks (such as rainbow attacks) even when the passwords were hashed. Hence, it is recommended to add the SALT (a random value) to the password before the hashing and the list of SALT values should be managed in a secure location.



<Figure 71> When passwords are stored in plain text

• When insecure hash algorithms are in use

When insecure hash algorithms, such as MD5 or SHA-1, are in use, the first hashed values need to be hashed again with the SHA-256 algorithm and these double-hashed values should be stored. For users who are successful in log-in, the SHA-256 can be used step-by-step in order to authenticate the users with unique hashed values. During this process, the valid log-in time or another added column can be used in order to identify single-hashed values from double-hashed values.



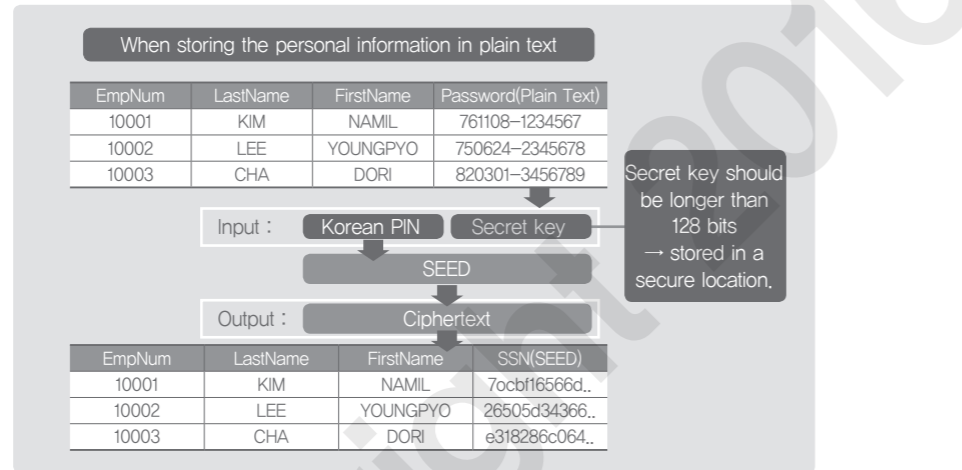
<Figure 72> When insecure hash algorithms are in use

② Bi-directional encryption algorithm

Data, such as personal information, should be encrypted and decrypted by using bi-directional encryption algorithms. Secure block encryption algorithms are commonly in use, such as SEED, ARIA, AES (Rijndael). At a high level, there are two main cases when the secure block encryption algorithm should be used: 1) data are stored in plain text in the existing database; and 2) insecure algorithms are in use (such as DES or 3-DES).

- When personal information are stored in plain text

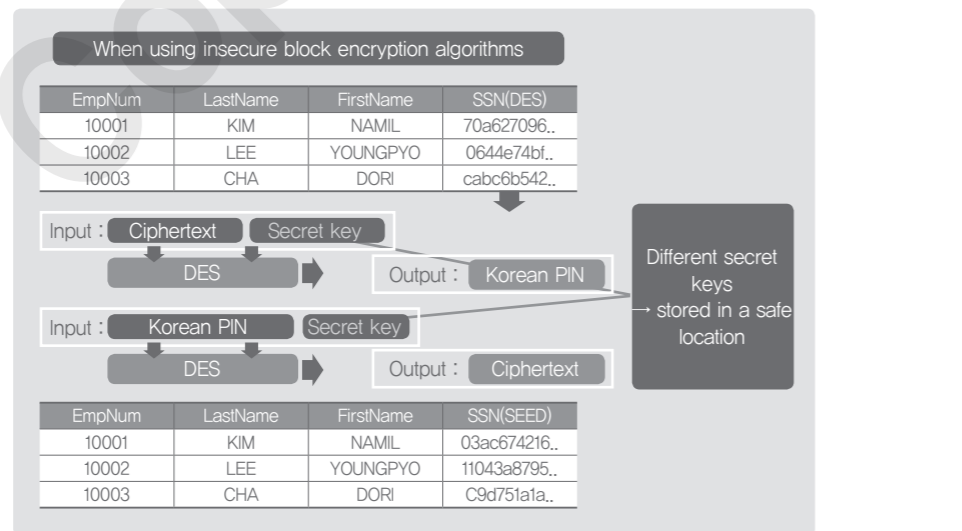
When personal information is stored in plain text, a secret key should be longer than 128 bits, and the secret key should be managed in a separate and secure location.



<Figure 73> When personal informations are stored in plain text

- When insecure block encryption algorithms are in use

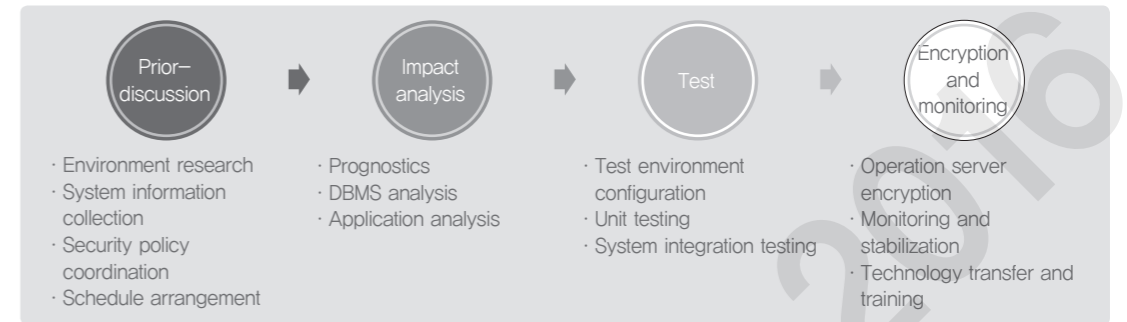
When insecure block encryption algorithms, such as DES or 3-DES, are in use, the encrypted data should be decrypted with a batch job, and a secure block encryption algorithm should be applied again for the safe encryption.



<Figure 74> When insecure block encryption algorithms are in use

Processes of Database Encryption

The actual encryption for the databases is conducted in the following processes described below: prior-discussion, impact analysis, test / verification, implementation, and stabilization.



<Figure 75> Steps of database encryption implementation

① Prior-discussion for DB encryption

A prior-discussion should be held among all the project stakeholders in order to share the information fully before security measures are applied to the database applications. The agenda for the discussion should cover: objects to be encrypted, which environment is subjected to the encryption, security policies, and any other necessary topics.

② DB encryption impact analysis

Impact analysis is an important diagnostic step where the objects for encryption and SQL queries are identified in advance and a performance test is conducted within the test environment before the new configuration is applied to the production environment. In general, the DBMS analysis and application analysis are conducted first in order to analyze the changes or impacts on the performance and system resources after the encryption.

- Selecting the objects for encryption
 - To search all the DBMS tables and columns in the production environment in order to extract the columns subjected to the encryption and finalize the list of objects for the encryption
- Query analysis
 - To extract all the queries that are currently used in the production DBMS: to analyze the data volume and query running time, and to select the queries that are deemed to need optimization
- DBMS analysis
 - To identify the resources used for the DBMS (CPU, memory, storage, etc.) and to predict the additional resources that may be required after the encryption
- Application analysis
 - To identify the application modules that will be affected by the encryption, to analyze the common modules that may be additionally required for the encryption and the application logics that need to be changed, and to select the application modules that need optimization

③ Test and verification for DB encryption

A test environment, which is identical to the production environment where the DB applications run, is built in order to run tests, including the application level testing, after the encryption is applied. The goal of this test is to identify

potential issues that may occur in the production environment and to resolve all those potential issues in advance.

The test scope covers all the applications and all the queries.

④ DB encryption and monitoring

This step is intended to actually apply security measures to the DB applications in the production environment based on the verifications made in the test period. The encryption job completed with the data, modified source code, optimized queries, and the issues identified and resolved in the test period are all put into the production environment. Monitoring activities should be continuously performed under the goal of: identifying any possible failures coming from applications and queries; and assessing the application performance.

04 Database Encryption Key Management

Types of Keys Used for Database Encryption

Any encryption will lose its meaning of existence when a key used for the encryption or decryption is exposed to outside. Hence, it is necessary to manage the keys safely with a two-way scheme: having a master key and encryption/decryption keys; and ensuring only the authorized personnel to have access to the keys.

〈Table 35〉 Database encryption keys

Type	Details
Encryption/decryption key	A key that is used to encrypt data and to decrypt the encrypted data
Master key	A key used to encrypt the encryption/decryption key and to store /distribute the encrypted key.

How to Manage Encryption Key in Each Stage of Key Lifecycle

① Key generation

A secure random number generator needs to be used for key generation. For the encryption keys generated by user input, a secure algorithm should be used.

② Key distribution

Key distribution should be conducted securely: an asymmetric encryption algorithm or similar algorithm should be used to encrypt the encryption key, so that only the authorized personnel can have access.

③ Key storage

Rather than hard-coding the encryption key into an application program, saving the encryption key in a file system as a file format, or storing the encryption key in the DBMS, it is recommended to store the key in a hardware: in a dedicated server for the key management or in the HSM (Hard Security Module).

④ Key usage

A DB administrator and security manager should comply with the principles of the "Least Privilege" and "Separation of Duty", so that the rights to gain access to and to modify the master keys should be given only to a limited

number of authorized personnel.

⑤ Key backup and recovery

When the encryption key is lost or damaged, the key should be recovered. To that end, a policy should be in place for the back-up and recovery of the encryption key. The backup job should be periodically carried out in accordance with the policy.

⑥ Key replacement

The encryption key should be periodically replaced following the organizational policy in order to make sure that the key is securely managed. When the encryption key is replaced, the data should be decrypted first with the existing encryption key, a new encryption key should be generated, and the data should be encrypted again with the newly generated encryption key.

⑦ Key disposal

When the encryption key is lost or damaged, an authorized manager defined by the organization policy should decrypt the data with the backup key. An encryption key should be newly generated, and the data should be encrypted again with the newly generated encryption key. The lost or damaged key should be disposed.

Example Question

Question type

Descriptive question

Question

Company A and Company B made inspections on their status of password management and found out the issues listed below. Please refer to the findings and answer the questions.

- (1) What is the problem that Company A has and how can it be resolved?
- (2) What is the problem that Company B has and how can it be resolved?

Company A stores user passwords with the SHA-1 hash algorithm.
Company B applies the SHA-256 hash algorithm only to user passwords.

Intent of the question

To evaluate the level of understanding about the access control model and practical skills about the same.

Answer and explanation

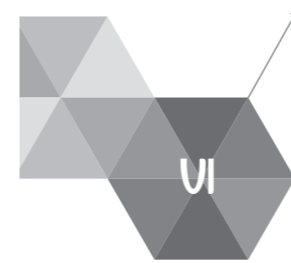
- (1) The issue with company A is that it is using an insecure algorithm (SHA-1) and the company is recommended to use secure hash algorithms such as SHA-256.
- (2) The issue with Company B is that it is using the hash algorithm only to user passwords. If only user passwords are hashed, they can be vulnerable to the dictionary attacks like rainbow attacks. Hence, it is recommended to use the SALT (a random value added to the password) for encryption.

If passwords are stored in plain text and only passwords are hashed, they can be vulnerable to dictionary attacks such as rainbow attacks. Hence, it is recommended to use a random value SALT in the hash algorithm and the SALT values should be stored in a safe location.

When insecure hash algorithms, such as MD5 or SHA-1, are in use, the first hashed values need to be hashed again with the SHA-256 algorithm and the double-hashed values should be stored. For users who are successful in log-in, the SHA-256 can be used step-by-step in order to authenticate the users with unique hashed values. During this process, the valid log-in time or another added column can be used in order to identify single-hashed values from double-hashed values.

Related E-learning Contents

- Lecture 6 Database security



Understanding Information Security Management System and Risk Management

▶▶▶ Latest Trends and Key Issues

K-ISMS (Information Security Management System), which is the domestic certificate for the information security management system, has been in effect as a mandatory requirement since Feb 18, 2013. A total of 126 certificates were issued in 2013 alone when the ISMS certification system mandate took effect. It shows a sharp contrast to 151 certificates that have been issued for the last 11 years, starting from 2002. In 2014 and 2015, a growing number of companies voluntarily have obtained this certificate to secure the stability in the information security, even if they are not obliged to do so.

▶▶▶ Study Objectives

- * To be able to explain about the information security management processes of the ISMS and relevant standards
- * To be able to explain about the risk identification, risk assessment, and risk management methodologies

▶▶▶ Practical Importance Medium

▶▶▶ Keywords

Information security management system, Information security management process, Information security measures, Certification evaluation criteria, Control areas, ISO27001, Risk identification, Risk assessment, Quantitative method, Qualitative method, Baseline approach, Detailed risk approach, Expert judgment, Combined approach

+ Practical tips

Mr. Kim, who is responsible for the information security at Company A, has prepared for months to get certified for the K- ISMS this year.

Starting from last January, Mr. Kim joined the Information Security Team and has taken a role responsible for establishing and operating the information security management system. Mr. Kim established a corporate policy and then, defined the scope of the information security management system to be subject to the certification. After forming the information security organization, he checked major activities that should be considered in the processes of the information security management, such as identifying internal assets, figuring out its weakness, and conducting risk assessment.

- To establish an information security policy and define the scope of the information security
- Management responsibility and organization structure
- Risk management
- To put information security measures in place
- Follow up

Mr. Kim established and operated the information security management system. He has monitored issues for the last two months and has conducted internal audits for its enhancement.

After that, he applied for the certificate, which is valid for 3 years. In addition, he needs to have a follow-up evaluation every year to make sure that the information security management system continues to work as expected in his organization.

In this chapter, we will study the definition of the information security management system, the risk management methodologies, and other certificates available.

01 Information Security Management System

Outline of Information Security Management System

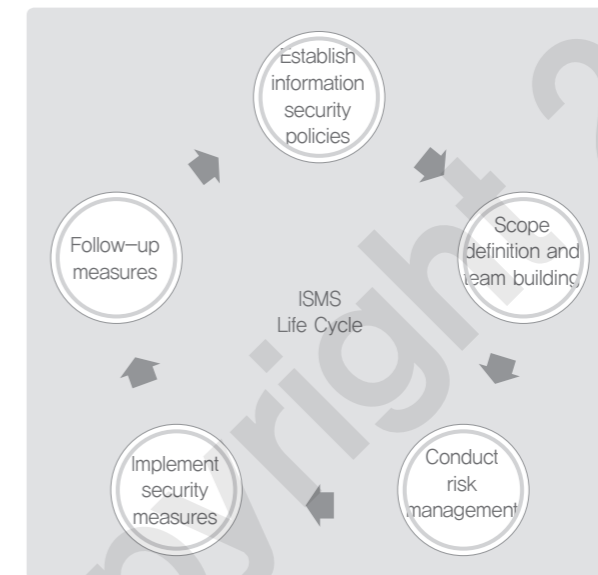
① Concept of information security management system

Information Security Management System (ISMS) is a set of processes that govern the management of the information security policies and procedures to preserve confidentiality, integrity, and availability of the information assets. It is a system that continuously manages and operates the processes for information security in its

establishment, implementation, operation, monitoring, review, and improvement with a risk-based approach. ISMS can be defined as a way for a company to take a holistic approach to implement security measures to make sure that the company-wide information security is in place so that it is able to quickly respond to any potential security incidents and minimize possible losses.

② Life cycle of information security management system

Life cycle of the ISMS consists of five phases: 1) Establish an information security policy; 2) Define the ISMS scope; 3) Conduct the risk management; 4) Implement security measures; and 5) Perform follow-up measures.



(Figure 76) Life cycle of ISMS

In the first phase, *Establish an information security policy*, an organization establishes high-level information security policies and specifies roles and responsibilities for each function of the organization for the implementation of the information security. In the second phase, *Define the ISMS scope*, the organization needs to identify information assets that fall into the ISMS scope, considering the internal/external environments the organization encounters.

In the third phase, *Conduct the risk management*, the organization establishes strategies and plans for the risk management, in accordance with the organization's characteristics and the type of information assets it possesses. In the next phase, *Implement security measures*, the information security measures should be effectively established and implemented in accordance with the information security plans specified in the previous phase.

In the final phase, *Perform follow-up measures*, the organization performs continuous monitoring activities and regular internal audits during the operation of the information security management system. Based on the results of such activities, the organization can verify whether they are in compliance with the security policy. In the process of establishing and operating the information security management system, the organization is required to review the current state of its information security and address the identified problems for the better.

Risk Management

Risk Management is a set of processes in which an organization's information assets are identified and categorized by their values, and then, the risk of each asset is identified from legal, managerial, physical, and technical perspectives. As for the risks which exceed the level of risk acceptance, which is called the DoA¹, preventive actions are taken as a part of the risk management to resolve the risks effectively.



① Risk identification

Risk refers to the likelihood or possibility of an organization to suffer from an adverse effect or loss caused by an unexpected incident. A risk can be expressed with a function that covers three elements: asset, threat, vulnerability. The risk identification is a process in which a value is assigned to each information asset and the risk entailed in each asset is identified.

② Risk assessment

Risk assessment is a process in which the scope of the risk analysis is defined in accordance with tasks-related, organizational, location-based, asset-related, and technical features and based on the predetermined scope of the ISMS.

To effectively perform the risk analysis, various risk assessment methodologies can be selectively used to meet the specific needs. Depending on whether a risk should be quantitatively measured or not, a quantitative method or a qualitative method can be selected. In addition, the methodologies can be divided based on the approach a methodology takes, such as Baseline Approach, Detailed Risk Approach, Combined Approach, or the like.

③ Risk assessment methodology

- Depending on whether the risk can be numerically measured or not, one among the two methods can be used.

¹ DoA : Degree of Assurance

〈Table 36〉 Quantitative method vs. Qualitative method

Classification	Quantitative method	Qualitative method
Features	<ul style="list-style-type: none"> • Used when the magnitude of the loss can be measured in monetary terms • Historic data approach, mathematical formula approach, probability distribution estimation 	<ul style="list-style-type: none"> • The magnitude of the loss cannot be numerically measured, so the risk is expressed with categories or variables (e.g. H:3, M:2, L:1) • Experiences and knowledge of an analyzer are used to analyze the risk • Delphi method, scenario method, ranking method
Pros	<ul style="list-style-type: none"> • Assessment is based on quantitative data, so a credible basis for the cost/benefit analysis and budget decision-making can be provided. • Calculation is based on mathematical techniques, making it more logical and rational 	<ul style="list-style-type: none"> • Suitable for the assessment of information that cannot be quantified • Terms are readily understood • Calculation is simple and readily executed within a short period of time
Cons	<ul style="list-style-type: none"> • Hard to provide accurately quantified values • Too much time and effort are required for the calculation 	<ul style="list-style-type: none"> • Risk assessment can be subjective • The basis for the cost/benefit analysis cannot be provided

- Risk assessment methods classified depending on the analytical approach

〈Table 37〉 Risk assessment method

Classification	Details
Baseline approach	<ul style="list-style-type: none"> • This approach sets the basic level of information security which is applicable to all the systems and establishes security measures to achieve the basic level of protection. • It needs a small amount of time and money, and can choose the basic level of security measures for the entire organization. • No special consideration is given to the variations within the organization, so the security controls can be set too high or too low to some departments.
Expert judgment	<ul style="list-style-type: none"> • This approach conducts the risk analysis by using an expert's knowledge and experiences, instead of a structured analysis. • Suitable to small organizations and cost-effective • Since there is no structured approach used, it is hard to analyze risks on an objective basis.
Detailed risk approach	<ul style="list-style-type: none"> • It involves the valuation of all information assets, the assessment of threats to those assets, and the assessment of associated vulnerabilities. • It can establish security measures best suited for the organization. • It requires a considerable amount of expertise, time, and effort to obtain the results.

Classification	Details
Combined approach	<ul style="list-style-type: none"> For the systems that are identified as being important or exposed to high risks, "detailed risk approach" is used, while for the other systems, "baseline approach" is applied. Security strategies are implemented early on, so resources, such as time and effort, are likely to be effectively used. When the target identification for the two approaches is not good enough, it can waste resources.

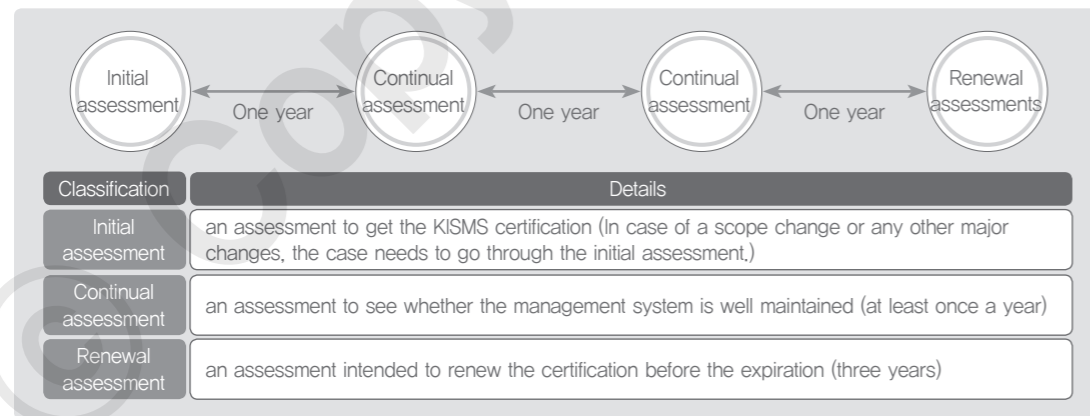
Standards Related to Information Security Management System

① Outline of standards for information security management system

K-ISMS and the international standard ISO 27001 are the most widely known certifications in Korea. The K-ISMS is similar to the ISO27001, but customized for the domestic environments. The K-ISMS includes all the requirements specified in the ISO 27001, while reinforcing the security requirements to accommodate the domestic circumstances. Therefore, the acquisition of the K-ISMS certification can guarantee that: all standards required by the ISO 27001 are met; and the information security management system befitting the Korean community is established solidly.

② K-ISMS certification system

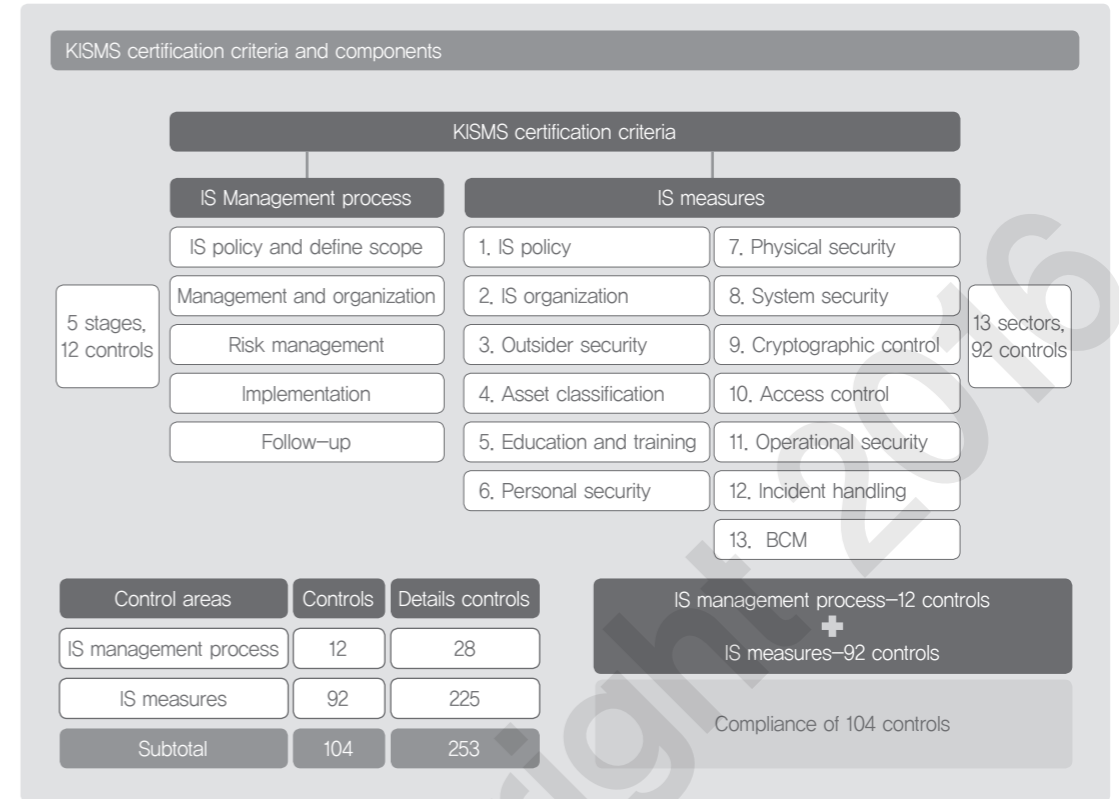
K-ISMS certification is intended to assess whether an information security and management system, which an organization has established and operated, complies with a certain certification criteria and to issue the certification accordingly. Documents reviews and on-site inspections are conducted in the process of the assessment by the Korea Internet and Security Agency or certification bodies.



<Figure 77> Types of assessments (Source: KISA)

<http://isms.kisa.or.kr>

There are initial, continual, and renewal assessments. The K-ISMS certification is valid for the period of three years once an organization passes the initial assessment.



<Figure 78> K-ISMS assessment criteria (Source: KISA)

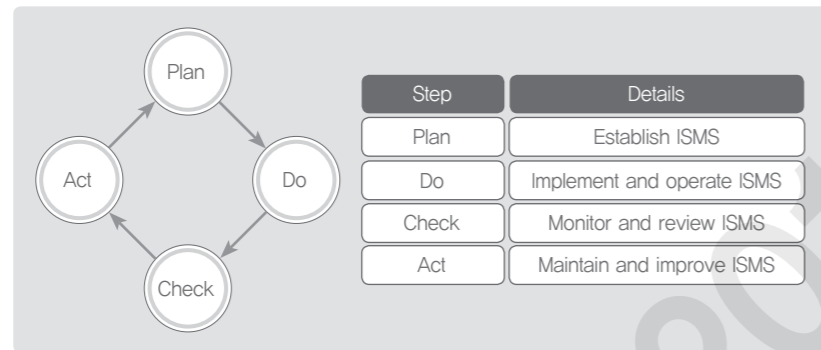
<http://isms.kisa.or.kr>

The K-ISMS certification criteria consist of the information security management process and the information security measures. A total of 104 security controls are utilized to assess the information security management system against the requirements of the K-ISMS certification. Among them, 12 security controls are used for the assessment of the management process and 92 security controls are used for the assessment of the information security measures.

③ ISO27001

ISO 27001 standard follows four phases under the PDCA (Plan-Do-Check-Act) model: 1) Establish the ISMS; 2) Implement and operate the ISMS; 3) Monitor and review the ISMS; and 4) Maintain and improve the ISMS. In the first phase, Establish the ISMS, an organization defines the security policy and ISMS scope, and identifies information assets that fall into the scope of the ISMS. Then, the organization identifies, analyzes, and assesses risks. In order to deal with the identified risks, the organization should select appropriate control objectives and control areas from the list of security controls and should prepare a plan for actions and implementation. In the next phase, Implement and operate the ISMS, the organization effectively implements and operates security countermeasures in accordance with the plan written in the previous phase. If and when necessary, trainings and drills are provided. In the phase, Monitor and review the ISMS, the organization executes monitoring procedures and undertakes regular reviews of the overall operation of the ISMS. In the final phase, *Maintain and improve*

the ISMS, the organization acts on the identified improvement opportunities and takes appropriate corrective and preventive actions for the continuous improvement of the ISMS.



(Figure 79) PDCA cycle of ISO 27001

ISO 27001: 2013 is an international standard used for the information security management system and the information security management system certification. It has been updated to grant the existing quality management system certification (ISO 9001) and the environment management system certification (ISO 14001) together with the attainment of the certifications available for information security, such as ISO/IEC 27001 and 27002 (ISMS2.0). The number of security controls/control groups listed on the checklist of the Annex reduced from 133 controls in 11 groups to 114 controls in 14 groups.

ISO/IEC 27001:2005 1.0		ISO/IEC 27001:2013 2.0	
System acquisition, development and maintenance	16	System acquisition, development and maintenance	13
Information security incident management	5	Information security incident management	7
Business continuity management	5	Business continuity management	4
Compliance	10	Compliance	8
–	–	Supplier relationship	5
–	–	Cryptography	2
–	–	Operations security	14
Total	133	Total	114

(Table 38) Changes in security control areas of ISO 27001

ISO/IEC 27001:2005 1.0		ISO/IEC 27001:2013 2.0	
Control group	No. of controls	Control group	No. of controls
Information security policies	2	Information security policies	2
Organization of information security	11	Organization of information security	7
Asset management	5	Asset management	10
Human resource security	9	Human resource security	6
Physical and environmental security	13	Physical and environmental security	15
Communications and operation management	32	Communications security	7
Access control	25	Access control	14

Example Question

Question type

Descriptive question

Question

Information Security Management System (ISMS) certification is designed to systemically manage the ISMS of an organization based on a risk-based approach. Depending on the type of analysis approach, it can be categorized into baseline approach, detailed risk approach, combined approach, and so on. Briefly explain about 'detailed risk approach' and its characteristics in the risk assessment.

Intent of the question

To check whether a learner understands the risk assessment methodologies which form the foundation of the information security management system.

Answer and explanation

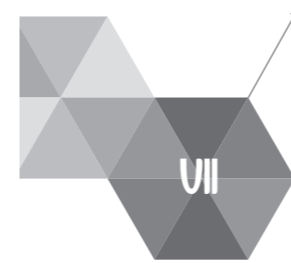
- It is a risk assessment method that involves the valuation of all information assets and the assessment of threats to the assets and their vulnerabilities. It defines the level of risk acceptance (DoA) and then identify security measures best suited for the organization. The objective of this approach is to minimize risks and conduct continuous risk management.
- This approach requires a considerable amount of expertise, time, and effort.

Baseline approach is a method that sets the basic level of information security applicable to all information systems and develops security countermeasures required to achieve the basic level of protection. The basic level of measures can be implemented for all the systems in the organization with a small amount of time and effort.

The combined approach is a method that applies "detailed risk approach" for a system that is identified as being important or exposed to high risks. For the remaining systems, "baseline approach" is applied. It is of importance to clearly choose which approach between the two is appropriate for the scope.

Related E-learning Contents

- **Lecture 3** Application Security
- **[Advanced]** Operation of Application Security



Building Disaster Recovery System that Reflects Organizational Circumstances

▶▶▶ Latest Trends and Key Issues

Potential disruptive events, such as crises in the business environment, natural disasters, failures in the computing systems, and technical disasters, are unrivaled to those of the past in terms of its implications and consequent losses. They are now regarded as factors that can affect the very existence of a company within a short period of time. In reality, we have witnessed some cases in which such disruptive events – not only general disasters (including wars, terrorism, and natural disasters), but also a labor strike caused by strained industrial relations, failures in computing devices/communications, and service outage in the main systems – occur locally or globally, resulting in suspending business operations or wreaking havoc on the provision of customer services. Against this backdrop, the availability of information systems has emerged as an important issue and there are growing demands for disaster recovery systems as well as various contingency plans for the disaster recovery of information systems.

▶▶▶ Study Objectives

- * To be able to understand the concept and scope of disasters and disaster recovery
- * To be able to explain about the types and technologies of disaster recovery systems
- * To be able to explain about the BCP and the BIA.

▶▶▶ Practical Importance High

▶▶▶ Keywords

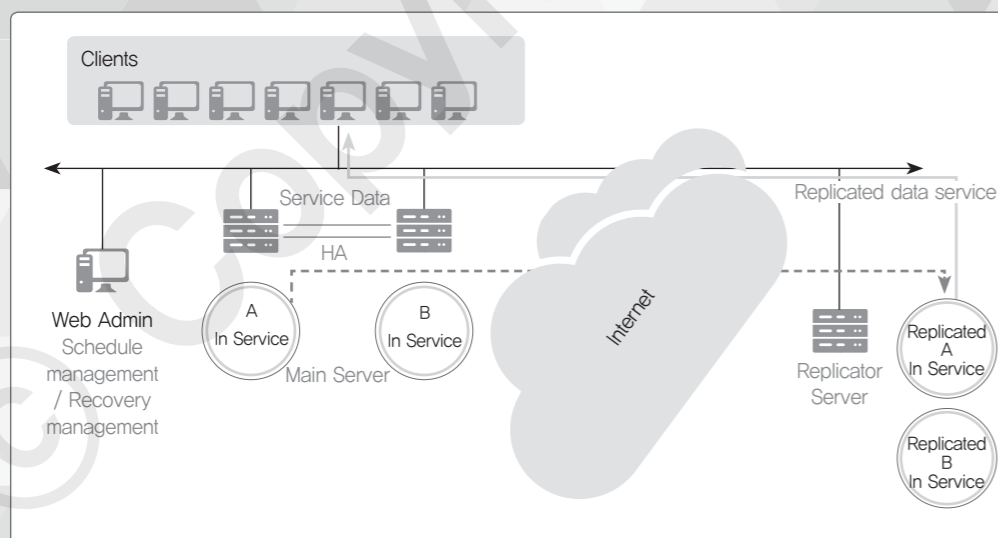
Disaster, Disaster Recovery, Mirror Site, Hot Site, Warm Site, Cold Site, Recovery Time Objective, Recovery Point Objective, Business Continuity Planning (BCP), BCM, Business Impact Analysis (BIA)

+ Practical tips

It is required that a system user continue its business operation without a hitch even though a failure takes place in the corporate computing system. To ensure the seamless business continuity, it is the top priority to have a comprehensive understanding about how to implement disaster recovery systems and about the relevant technologies. A failure in the IT infrastructure is not a matter of simple disaster recovery on the system level. It can affect the entire business. If a failure occurs in major IT systems in the financial, retail, and manufacturing businesses and if the disaster recovery is delayed for 2 days, 3.3 days, and 5 days respectively, 25% of those businesses will promptly go into bankruptcy and 40% of them are highly likely to become bankrupt within 2 years.

Suppose that you work at Company A that handles the stock information in real time and you are responsible for implementing a disaster recovery system, using remote storage redundancy solutions, as shown in the following figure. We will take a look at how to build a disaster recovery system that meets the following objectives, considering the speed requirements and the importance of the stock information.

- RTO (Recovery Time Objective): 3 hours
- RPO (Recovery Point Objective): Just before a disaster occurs, a point in time when the latest transaction log is duplicated in the DR system
- Network recovery method: recovery, using the VPN (Virtual Private Network)
- Planned environment: service that duplicates transaction logs in real time



01 Disaster Recovery System

Outline of Disaster Recovery

① Concept of disaster recovery

Disaster Recovery is a process of resuming the service operation of a company to the state of normality after the occurrence of a disastrous event. There are three types of disasters: man-made disasters (intentional or unintentional); natural disasters (caused by fires, earthquakes, or floods); and failures in the computing systems, including systems or network facilities. It is necessary to establish a plan and to prepare the systems for the disaster recovery, so that effective disaster responses can be made. The aforementioned factors are called the Disaster Recovery Planning and the Disaster Recovery System respectively.

Disaster Recovery Planning (DRP) is composed of a set of activities to minimize the possibility of a disaster occurring in major business processes and its consequent losses.

② Standards related to disaster recovery

Locally used standards related to the disaster recovery follow the guidelines recommended by the Financial Supervisory Service. It includes the IT contingency plan for financial institutions, the TTA guidelines, and the guideline for the management and operation of integrated data centers. The global standards for the disaster recovery include the guidelines on the business continuity planning in preparation for disasters issued by the international standardization bodies and international financial bodies, such as Basel II, BS7799, ISO17799 and ISSA.

③ Types of disaster recovery systems

In order to effectively build a disaster recovery system, no matter how big an organization is, the following factors need to be considered: operation type of disaster recovery systems, type and location of disaster recovery systems, technologies used for the implementation (data replication/transfer method), disaster recovery networks, and so on.

Operational type of disaster recovery systems can be categorized in accordance with the type of implementation and operational ownership. The operational type of disaster recovery systems can vary, depending on the size of the organization and characteristics of the operating organization.

<Table 39> Types of implementation and operational ownership of disaster recovery systems.

Classification	Type	Description	Cost of implementation	Cost of operation	Security level	Recovery reliability
Types of implementation	Unilateral implementation	• Implement its own disaster recovery system with its own capability	High	High	High	High
	Joint implementation	• Two or more organizations jointly implement the disaster recovery system	Medium	Medium	Medium	Medium
	Reciprocal implementation	• Arrangement among multiple organizations. They use another organization's equipment as the disaster recovery system and vice versa.	Low	Low	Low	Low

Classification	Type	Description	Cost of implementation	Cost of operation	Security level	Recovery reliability
Operational ownership	In-house operation	• Operate the system on its own	–	High	High	High
	Joint operation	• More than two organizations jointly operate the system	–	Medium	–	–
	Outsourced operation	• The operation of the system is outsourced to a third-party.	–	Low	–	–

In general, the disaster recovery system can be categorized into Mirror Site, Hot Site, Warm Site, and Cold Site. This categorization was made in accordance with the level of recovery.

〈Table 40〉 Type of disaster recovery systems in accordance with recovery level

Type	Description	RTO	Pros	Cons
Mirror Site	<ul style="list-style-type: none"> • The system identical to the main data center is built in a remote site. • Both are running in an active-active mode, providing the same services in real time 	Real-time	<ul style="list-style-type: none"> • Data freshness • High stability • Fast in resuming business 	<ul style="list-style-type: none"> • High CAPEX • High maintenance cost • Possibility of overload when too much data update is required
Hot Site (Data Mirroring Site)	<ul style="list-style-type: none"> • After building the system identical to the main data center in a remote site, it is running in a standby mode. (Active-Standby) • The alternative system located in a remote site is changing its operation to an active mode, when a disaster takes place in the main data center. The data is mirrored synchronously or asynchronously in real time. 	Within hours	<ul style="list-style-type: none"> • Data freshness • High stability • Fast in resuming business • Suitable when many data update requests are made 	<ul style="list-style-type: none"> • High CAPEX • High maintenance cost
Warm Site	<ul style="list-style-type: none"> • Some important information resources are partially duplicated in the disaster recovery center. • Data is backed up on a regular basis. 	Within days or weeks	<ul style="list-style-type: none"> • Costs required for the establishment and maintenance is lower than that of a hot site. 	<ul style="list-style-type: none"> • Some data losses occur • Only some parts are recovered at an initial stage. • The time required for the recovery is relatively long.
Cold Site	<ul style="list-style-type: none"> • Only data are stored in the alternative system. • In the event of a disaster, necessary information resources are retrieved and recovered. • Back up performed to a remote site with the data of the main center. 	Within weeks or months	<ul style="list-style-type: none"> • Lowest in costs for the establishment and maintenance 	<ul style="list-style-type: none"> • Data losses occur • The time required for the recovery is very long. • The recovery reliability is low

When establishing a disaster recovery system, the following objectives should be taken into consideration.

〈Table 41〉 Objectives to be considered for building disaster recovery systems

Objectives	Details
RSO: Recovery Scope Objective	<ul style="list-style-type: none"> • Legacy system, information system, Web, Mail, etc. • Backup for the system recovery in the event of a disaster
RTO: Recovery Time Objective	<ul style="list-style-type: none"> • 3 hours, 12 hours, 24 hours, etc.
RPO: Recovery Point Objective	<ul style="list-style-type: none"> • Data is restored at a specific point when backup is performed • Data is restored at a point in time when a disaster occurs
RCO: Recovery Communication Objective	<ul style="list-style-type: none"> • The level of network recovery • Main branches, all branches, etc.

Business Continuity Planning

① Concept of Business Continuity Planning (BCP)

Business Continuity Planning (BCP) is the process that helps a company prepare for disruptive events, so that it can keep its operations running smoothly when a disaster occurs and interrupts its normal operations. The BCP is an overarching concept that covers the Disaster Recovery (DR). For the effective implementation of the business continuity planning, core business processes of a company, including key human resources and technologies, should be identified first, and how to respond to disasters should be defined in detail for each type of disasters. In addition, the BCP should include a plan for the duplication of core systems, including servers, storages, and networking and security facilities. In general, all critical work streams should be taken into consideration for this process, such as human resources, facilities, and funds.

② BCP, BCM, BIA

Business Continuity Management (BCM) is a set of processes intended to perform the Business Impact Analysis (BIA), to build a strategy based on the results of the BIA, and ultimately to establish the BCP. The objective of the BCM is to minimize the downtime and resume the normal operation of business processes from a disruptive event.

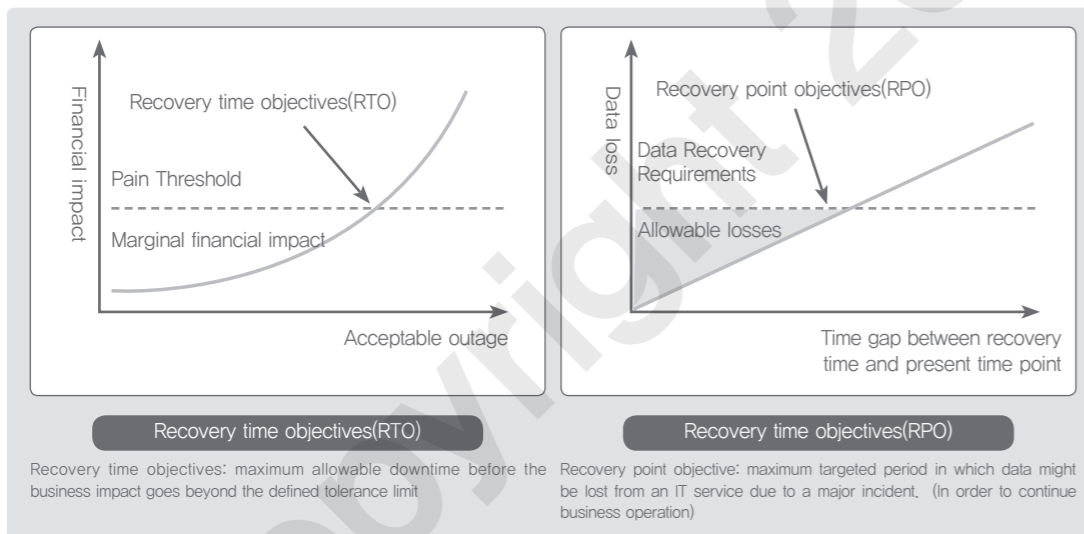
Classification	Impact item	Estimated impact					
		Size of impact from service disruption (in time scale)					
		1Hr	5Hr	1 day	5 days	1 week	1 month
Quantitative	Financial impact	<ul style="list-style-type: none"> • Reduced sales • Reduced income Identifying monetary value					
	Business impact	<ul style="list-style-type: none"> • Business delays – Increase in business stream processes – Delays in completing each work and task Identifying the amount of time delayed					
Qualitative	Tangible	<ul style="list-style-type: none"> • Customer churn, lost future sales opportunities • Compensation for damages and class actions from customers (potential) • Delay in performing relevant works • Loss of data (irrecoverable) Identifying impacts in quantitative terms					
	Intangible	<ul style="list-style-type: none"> • Trust, confidence, reputation damage • Sanctions by supervisory authorities and investigations by prosecutors • Other losses Identifying probabilities					

〈Figure 80〉 Impact analysis using quantitative/qualitative approach (example)

Business Impact Analysis, which comes before devising the strategies for disaster recovery, is performed in the following manner.

- Identify core business processes
- Identify the type of disasters, and calculate the likelihood of the occurrence of disasters and how long it will take to resume the normal operation of business processes after a disaster hits
- Measure the importance of each business process and calculate the loss caused by the business discontinuation in the event of a disaster
- Set the priority and define the scope of recovery for each business process
- Define the RTO of each business process and set the priority among the business processes in the event of a disaster

When defining the recovery scope, the maximum tolerable length of time is measured and evaluated for each business process, and the outcome constitutes the RTO for each process.



〈Figure 81〉 RTO and RPO

A company is required to fully understand the procedures for disaster recovery and check whether its disaster recovery system operates normally or not. It should also prepare itself against any emergency situations by conducting regular mock drills in response to disasters.

Example Question

Question type

Descriptive question

Question

Disaster recovery system is categorized in accordance with the level of recovery: mirror site, hot site, warm site and cold site. Explain the differences between the mirror site and the hot site, and choose which one is more suitable for a case in which many data update requests are made.

Intent of the question

To check whether a learner understands the types of disaster recovery systems and their differences

Answer and explanation

Mirror site is a method of implementing a disaster recovery system that establishes the system identical to the main data center in a remote site (Active-Active), so that it can provide the same service in real time. In contrast, the hot site is a method that establishes the system identical to the main system in a remote site and runs its alternative system in a standby mode (Active-Standby). In the event of a disaster, this alternative system located in the remote site provides services in an active mode. Therefore, the hot site is more suitable for this case, because many requests can cause system overload in the mirror site.

Disaster recovery system is categorized in accordance with the level of recovery: mirror site, hot site, warm site, and cold site.

Mirror site and hot site have strengths in the data freshness and high stability, while they require high costs in their establishment and maintenance.

Warm site stores only important information resources in the disaster recovery center and recovers with the backup data in the event of a disaster. The data can be partially lost, but its cost for the establishment and maintenance is lower than that of the hot site.

Cold site is a method that stores the data in a remote site and retrieves necessary information resources only in the event of a disaster. Therefore, the data can be lost and the time required for the recovery is long. However, its cost for the establishment and maintenance is low

Related E-learning Contents

- Lecture 7 Administrative Security

VIII

Understanding Personal Information Protection

▶▶▶ Latest Trends and Key Issues

Once the personal information is leaked, it can be continuously misused for unwanted advertisements, such as spam mails or illegal marketing activities. It can be also exploited for crimes, such as an account theft or a voice phishing. It can inflict enormous harm on a subject of the personal information, making the subject suffer physically and mentally. Worse yet, the leaked information is hardly retrieved, adding to the severity of its damage.

▶▶▶ Study Objectives

- * To be able to explain about the personal information protection
- * To be able to explain about the process of the personal information management and how to develop the personal information management system
- * To be able to explain about the certification systems related to personal information protection

▶▶▶ Practical Importance High

▶▶▶ Keywords

Personal information, Collection, Use, Storage, Provision · Entrustment, Destruction, Unique identifying information, Personal information management system, Consent on collection · use, Access control, Encryption, PIMS, PIPL, PIA

+ Practical tips

Recently, news on personal information security issues, such as the leakage of customer information and system hacking, are easily found. After conducting research on several incidents, it was found that some companies violated laws and regulations stipulated in the Personal Information Protection Act as follows.

- Company A obtains the consents from a subject of information when he/she joins the membership of its Internet website, but without any distinction from other personal information.
- Company B transmits passwords without encryption—which are transferred upon logging in.
- Company C obtains the consent on the collection and use of the Korean PIN, and stores the Korean PIN.

In this chapter, we will look at the scope of the personal information protection stipulated in the legislations, and major security issues that an engineer is required to take into consideration during the development of the system.

01 Personal Information Protection

Outline of Personal Information Protection

① Concept of personal information protection

According to the definition of the laws, “personal information” means the information with which an individual can be identified, such as names, Korean PIN, and video information (including the information that can be easily combined with other information to identify an individual even though the information cannot be solely used to identify a person on its own).

The types and examples of personal information are listed below.

<Table 42> Types of personal information and their examples

Types	Examples of personal information
Personal Information	• name, Korean PIN, address, domicile of origin, phone number and other contact information, date of birth, place of birth, e-mail address, family relationships and family members
Biological Information	• (Biometric information) face, fingerprint, iris, voice, genetic information, height, weight, etc. • (Medical and health information), health status, medical record, physical disability, disability level, medical history, etc.
Mental Information	• (Preference and tendency) rental records of books and videos, magazine subscriptions, goods purchased, website search history, etc. • (Inner secrets) ideology, creed, religion, values, political parties, trade union membership and activities, etc.
Property Information	• (Personal financial information) income, credit card number, account number, moveable assets, real estate, savings, etc. • (Credit information) credit rating information, loan statement or collaterals, credit card statement, etc
Social Information	• (Education information) education, grades, attendance, certifications, merit/demerit records, student records, etc. • (Legal information) criminal records, court records, penalty payment history, etc. • (Employment information) workplace, employer, place of work, working experience, merit/demerit records, job evaluation records • (Military information) service status, service number, rank, service place, etc.
Others	• phone call history, website access history, e-mail or telephone messages, location information (by GPS or other technologies), etc.

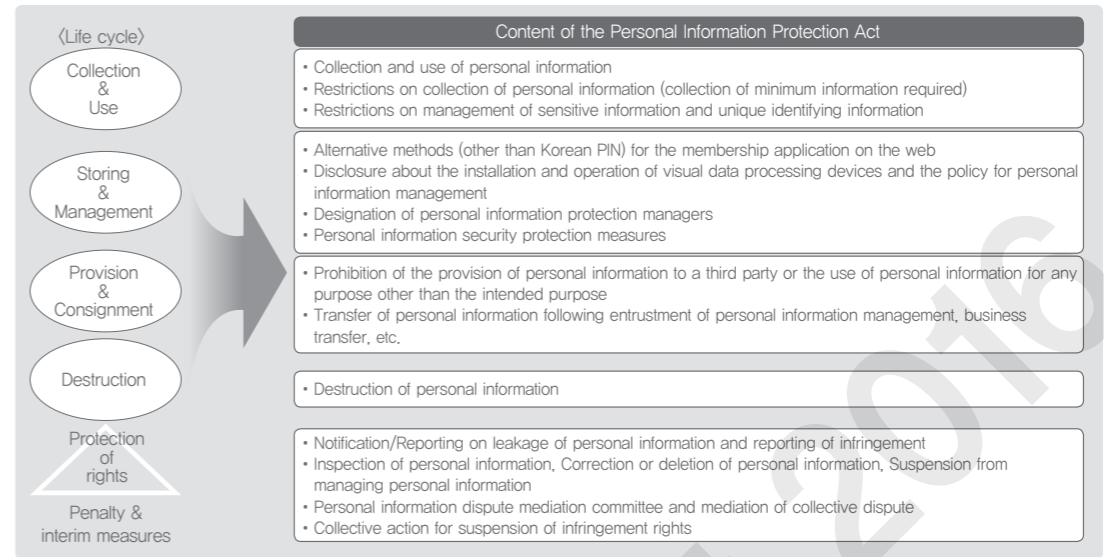
When building a system for the personal information management, it is necessary to review and accommodate the requirements stipulated in the legislations and guidelines pertaining to the personal information protection. As for the legal compliance, the Personal Information Protection Act is the one to comply with unless specified otherwise by any other sectoral or special laws.

<Table 43> Laws and notifications pertaining to personal information protection

Classification	Name
Legislations	Personal Information Protection Act
	Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.
	E-Government Act
	Information & Telecommunication Infrastructure Protection Act
	Law on the Protection and Use of Location Information (Location Information Law)
Notice	Act on the Use and Protection of Credit Information
	Standard for Measures to Secure the Safety of Personal Information (MOI notice, 2014-7)
	Standard Guideline for Personal Information Protection (MOI notice, 2011-45)
	Notice on Privacy Impact Assessment (MOI notice, 2012-59)
	Standard for Technical and Managerial Protection Measures for Personal Information (KCC notice, 2012-50)

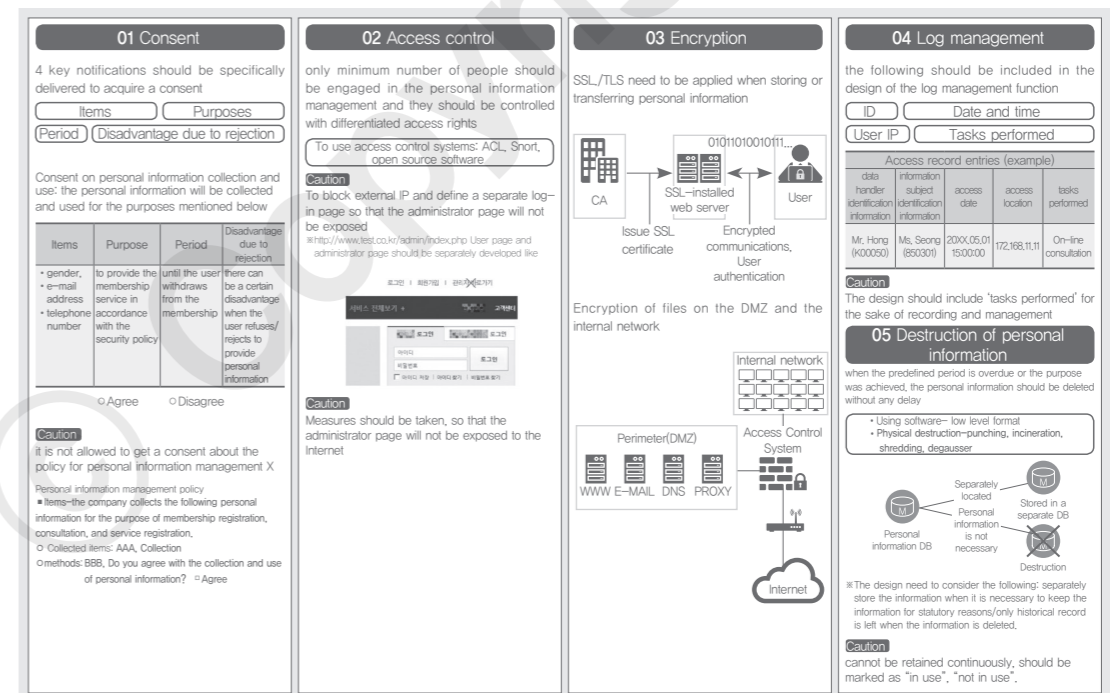
② Process of personal information management

The Personal Information Protection Act defines the mandates for each phase of the personal information management activities.



<Figure 82> Phase-wise legal mandate for personal information management

In case when planning and developing a system for the personal information management, the following principles should be respected in the process of the development. The diagram below shows the summary of critical principles. It is, hence, recommended to refer to the relevant laws for more details.



<Figure 83> Principle of personal information protection for system developers

- To include: how to acquire a consent

The consent on the collection of personal information should be notified to a subject, before the subject types in the personal information. The subject should have an option to reject to give a consent.

The following information should be notified during the process for the acquisition of consent. The purposes for which personal information is collected and used; Items of personal information to be collected; Period for which personal information is held and used; and details of a disadvantage, if any, due to his/her rejection to give a consent.

- To include: how to discard personal information

When personal information becomes unnecessary as its holding period expires, its management purpose is achieved and by any other ground, the personal information should be destroyed irreversibly without delay: Provided that, this shall not apply where the personal information must be preserved pursuant to any other statutes. In this exceptional case, the information should be stored separately from the personal information which is currently in use.

A separate DB should be created to store the information, or the information should be stored in a physically separated server. For the separate DB, a set of new access rights should be established, as opposed to the personal information DB currently in use, in order to forestall unnecessary access, inquiry, and leakage.

- Access control to the personal information management system

A personal information manager should: put access rights control in place to stop any unauthorized access to prevent the accident and illegal access; and should analyze the IP addresses to detect illegal attempts to leak out the personal information. The ACL (Access Control List), firewalls, a free open source intrusion detection system (Snort), and the like are currently available for the access control.

- Encryption should be used when storing and transferring the personal information

When storing the personal information in the personal information management system or transferring the personal information over the network, the data should be encrypted in order to prevent the unauthorized exposure, manipulation, or forgery.

- ① One-directional encryption algorithm should be used for passwords, so that the passwords cannot be decrypted.
- ② Passwords cannot be decrypted even when the passwords are lost or forgotten, therefore, a function should be in place to provide a randomly-generated password or enable the user to create a new password.
- ③ The following information should be encrypted with safe algorithms and stored: unique identifying information (Korean PIN, passport number, driver license number, foreigner registration number) and biometric information (finger print, iris, voice, handwriting pattern).
- ④ Encryption methods, such as SSL/TLS, should be applied to the section where the personal information is transferred.

- Management about access record and permission changes

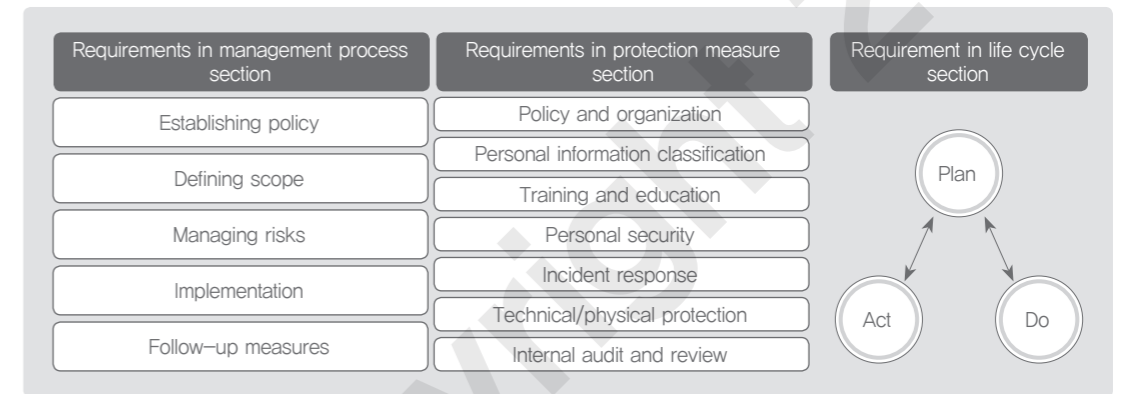
A personal information manager should keep and manage the access records to the personal information management system for at least 6 months. The access records can be used to generate a log file which contains the history about input/output of, modification of, and the access to the personal information, and such information can be used to verify unauthorized accesses.

Certification System for Personal Information Protection

- ① PIMS (Personal Information Management System)

PIMS (Personal Information Management System) means a system which grants a certificate to a corporation which can meet a certain criteria in the personal information protection. The system is designed to conduct reviews in order to evaluate whether a corporation has fully established a scheme that can continuously and systematically carry out activities for the personal information protection.

PIMS is composed of a set of requirements in the management process, protection measures, and life cycle. The requirements in the management process section are intended to verify whether the activities for the personal information protection are conducted systematically and periodically. The requirements in the protection measures section are aimed to assess managerial, physical, and technical protective measures for the personal information. The requirements in the life cycle section are intended to look into legal compliance issues throughout the life cycle, from generation to disposal, of the personal information.

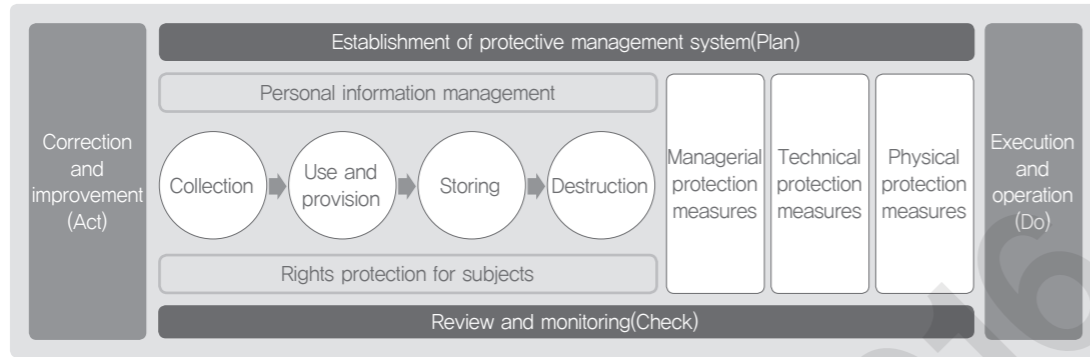


(Figure 84) Personal Information Management System

- ② PIPL (Personal Information Protection Level)

PIPL (Personal Information Protection Level) is a scheme which grants a certificate to a party that establishes a management system for the personal information protection, acts on the protective measures in accordance with the objectives of the Personal Information Protection Act, and meets a certain level of protection requirements. This certificate can be applicable to all the parties that manage the personal information, such as public organizations, private companies, corporations, associations, and individuals.

The assessment criteria can be divided into "management system for personal information protection" and "measures for personal information protection".



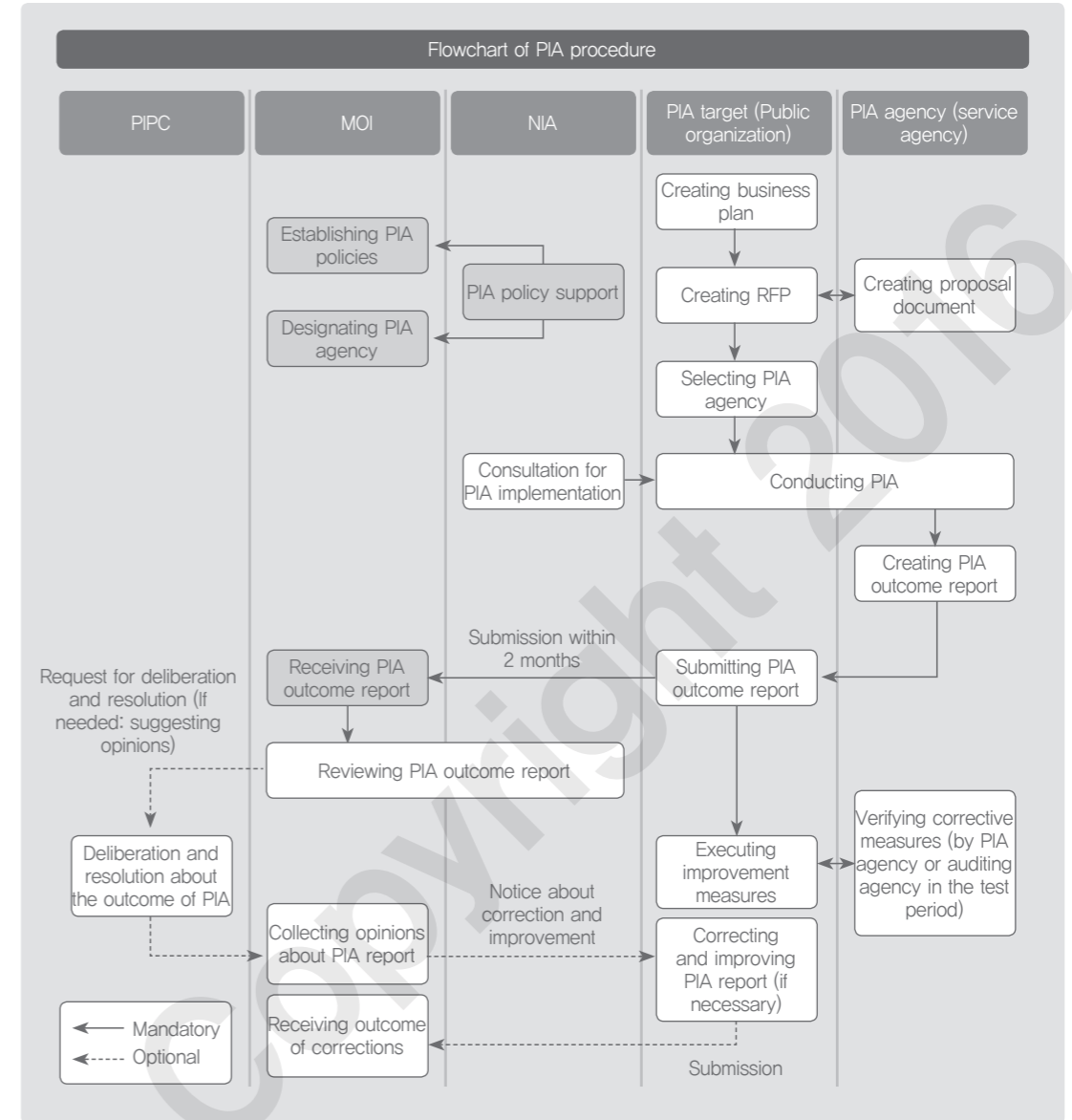
〈Figure 85〉 Framework of Personal Information Protection Level

The area of “management system for personal information protection” shall be assessed from a PDCA (Plan–Do–Check–Act) perspective: establishment of the protective management system (Plan); execution and operation of the plan (Do); review and monitoring (Check); and correction and improvement (Act). The area of “measures for personal information protection” covers: protective measures for ‘managerial, technical, and physical security’; and legally binding matters, such as ‘management of personal information’ and ‘rights for information subject’.

③ PIA (Privacy Impact Assessment)

PIA (Privacy Impact Assessment) refers to a systematic procedure that is intended: to assess the potential impacts on the personal information management in advance of the event of the adoption of a new system for personal information files or a major change in the existing system; and to come up with an improved method for the personal information management, based on the analysis, forecast, and review of the potential impacts.

The parties subjected to the Privacy Impact Assessment are public organizations that handle a certain volume of personal information files. The assessment shall be conducted following the rules stipulated in the Article 33 of the Personal Information Protection Act and the Article 35 of the Enforcement Decree of the Personal Information Protection Act. The detailed procedure is described below.



〈Figure 86〉 Procedure of PIA

Example Question

Question

Descriptive question

Question

When developing a system for the personal information management, the system should be developed in compliance with the legally required personal information protection measures. Please describe when the collected information, after getting a consent from information owners, should be discarded and how the information should be discarded.

Intent of the question

To evaluate whether a learner understands legal compliance requirements about the personal information protection.

Answer and explanation

When personal information becomes unnecessary as its holding period expires, its management purpose is achieved, and by any other ground, a personal information manager shall destroy the personal information irreversibly without delay: Provided that, this shall not apply where the personal information must be preserved pursuant to any other statutes. In this exceptional case, the information should be stored separately from the personal information which is currently in use: a separate DB should be created to store the information or the information should be stored in a physically separated server.

There are rules to be followed in the process of developing a system for the personal information protection: how to acquire the personal information after an informed consent is signed, access control, encryption, log management, and the disposal of personal information.

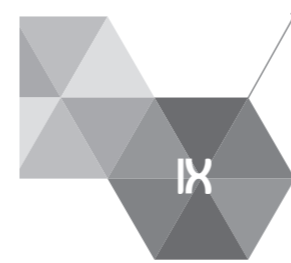
When a personal information manager obtains a consent, he/she shall notify a subject of information of the following matters.

Purposes for which personal information is collected and used; Items of personal information to be collected; Period for which personal information is held and used; and details of a disadvantage, if any, due to his/her rejection to give a consent.

A personal information manager should control the access to the personal information management system. In addition, encryption should be applied to the personal information in order to avoid unauthorized exposures, manipulations, and forgeries when it is stored in the personal information management system or transferred over the network. The personal information manager is required to keep and manage the access records to the personal information system at least for 6 months.

Related E-learning Contents

- Lecture 8 Latest Trend and Standards in Information Security
- [Advanced] Lecture 4 Latest Technologies and Standards in Information Security



Understanding About the Latest Threats to Information Security

▶▶▶ Study Objectives

- * To be able to explain about the terminologies related to the latest security threats and the information security technologies to address those threats
- * To be able to explain about security threats in the cloud and big data environment and the information security technologies to address those threats
- * To be able to explain about security threats in the web and mobile environment and the information security technologies to address those threats
- * To be able to explain about security threats in the IoT environment and the information security technologies to address those threats
- * To be able to explain about the latest trend in the laws and standards related to information security.

▶▶▶ Practical Importance High

▶▶▶ Keywords

APT, Smishing, Open SSL, Heart bleed, NTP, Network separation, Network bridge, MDM, MAM, WIPS, Fraud Detection System (FDS), Personal Information Protection Act, Information and Communications Network Act (ICN), Privacy Act for Location Information, Standardization

+ Practical tips

Company A has recently developed a range of home appliances, such as refrigerator and TV, but they were hacked. A lot of consumers claimed that they got millions of spam mails, and made their cases to the customer center.

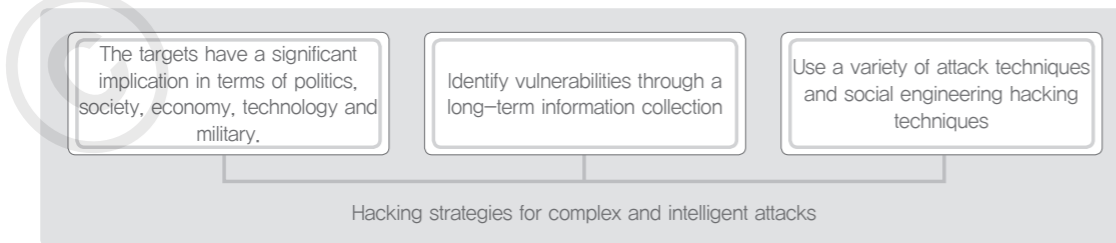
Company B has recently launched a new smart phone model, but the new phone model was infected with a malicious application. The company, therefore, suffered from IoT-related security breaches, such as unauthorized remote access to the ECU (Electronic Control Unit) of automobiles.

As such, new appliances and wired/wireless communication devices are launched thanks to the latest technologies, but hackers make various attempts to utilize those new devices with a malicious intent. We will look at what are the latest threats in information security and what kind of measures can be taken. In addition, there have been continuous efforts of technical development for information security to prevent security incidents in advance and eventually to standardize such technologies globally. This chapter will introduce the trend of international standardization and the Korean legislations related to information security.

01 Latest Threats in Information Security

APT (Advanced Persistent Threat)

① Introduction to APT attacks



<Figure 87> Introduction to APT attacks

② APT attack scenario

APT attacks generally go through four phases: incursion, discovery, capture, and exfiltration.

- Phase 1: an attacker infects vulnerable systems or employees' PCs with malicious codes
- Phase 2: the attacker breaks into the internal network, using the malicious codes
- Phase 3: the attacker discovers and captures the information about the internal systems and infrastructure and gets ready for an attack
- Phase 4: the attacker steals the core information from the vulnerable systems, and launches attacks for the destruction of the system or denial of service

③ Cases for APT attacks

- In Korea, financial institute N was hacked in 2011: data deletion led to entire computer network shut down
- Financial institute H was hacked: 1.75 million personal information stolen
- Portal site N was hacked: 35 million personal information stolen

④ Defense against APT attacks

<Table 44> Defense against APT attacks

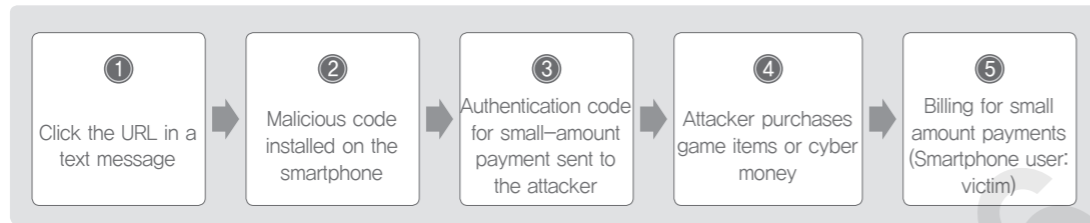
Defense measures	Details
Reinforcement of security management, operation, and training	<ul style="list-style-type: none"> • To analyze the security readiness of the potential targets to discover a range of vulnerabilities; the organization-wide security analysis and the security readiness realignment • A dedicated security management organization should be at the center for the sustainable operation, including all-time managed security and regular mock hacking drills
Endpoint security	<ul style="list-style-type: none"> • Endpoints are the first line of target for APT attacks. At the end point, there are multiple paths through which malicious codes can come in, such as the Internet, e-mail, SNS, messenger P2P, USB, and the like. • OS security update, security software installation, application control based on the white list
Access rights management	<ul style="list-style-type: none"> • Access rights management for the important information, minimized access privilege, access rights segmentation according to the importance of information • For high priority information: personal and device-based authentication, strategic implementation of rights management, automatic allocation and withdrawal of permissions and authorities
Encryption for critical information and DLP	<ul style="list-style-type: none"> • The final target of APT attacks is data; data should be stored after encryption. • Depending on the way important data are stored, the types of leakage incidents can vary: need to introduce solutions like the DLP (Data Loss Prevention)

Smishing

① Introduction to smishing

Smishing is a newly coined word from SMS+ Phishing. With the higher penetration of smart phones and widespread financial services like a small-amount payment, a new way of scam has emerged, such as providing a fake coupon or an event winning notice on an SMS to make users click on the small amount payment service on their phones.

② Smishing attack scenario



③ Defense against smishing

- Not to click the link on the marketing SMS, especially when the source is unknown
- To double-check the URL when clicking the website address written on the SMS
- To install an anti-smishing application
- To cancel download/installation when an application is being installed without a consent
- To erase the application (in the administration menu) when an unauthorized application is identified
- To review the cell phone-based payment statement in case when a suspicious approach was made. (Mobile carrier or payment company)

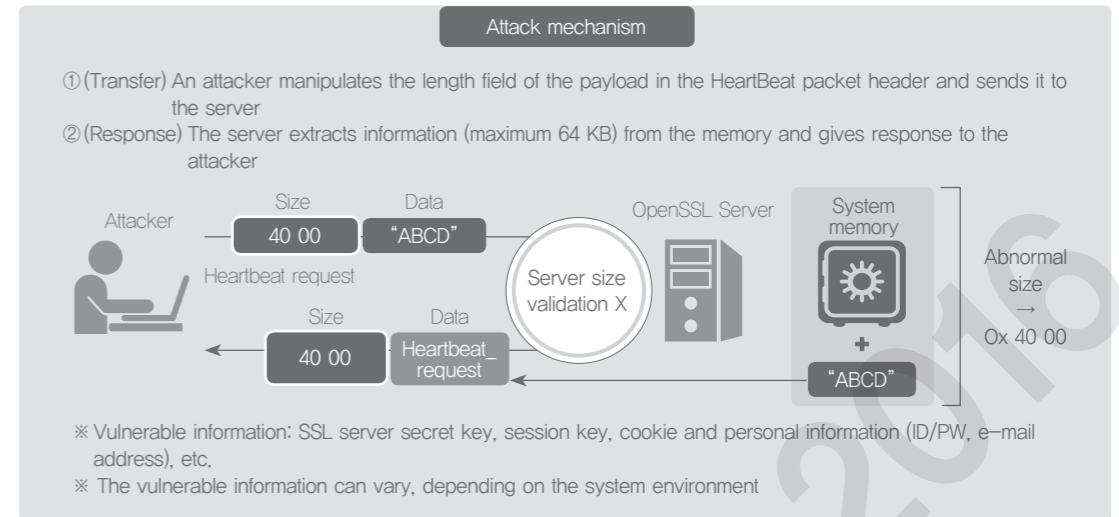
Open SSL Vulnerability (HeartBleed)

① Introduction to Open SSL vulnerability

Heartbeat² extension of the OpenSSL encryption library does not validate the data length when processing the request message from the client. This vulnerability in the Open SSL allows attackers to obtain up to 64KB chunks of memory from outside and repeat the process as many times as they wish.

② Scenario of attacks

When an attacker manipulates the message length information of the HeartBeat Request packets and sends them to a server which uses a vulnerable OpenSSL version, any data beyond the boundary of the predefined buffer shall be transferred to the attacker. Thanks to this information, the attacker can steal the personal information and authentication information stored on the system memory.



<Figure 88> Open SSL attack scenario

③ Defense against Open SSL attacks

<Table 45> Defense measures against Open SSL attacks

Defense measures	Details
For system	<ul style="list-style-type: none"> • OpenSSL version to be updated to 1.0.1g • Software dependency should be considered first in the production service environment(service production environment?), and an update testing should be conducted first before the deployment.
For network security equipment	<ul style="list-style-type: none"> • Need to use the vulnerability attack detection and blocking patterns on the network ※The blocking pattern should be applied after fully considering its impact on the service and network.
For service management	<ul style="list-style-type: none"> • Need to carefully consider the re-issue of the certificate: it is possible that the server side SLL secret key might have been exposed. • To encourage users to reset the password after measures against the vulnerabilities are completed.

GNU Bash Shell Vulnerability (Shell Shock)

① Cause of vulnerability

GNU Bash vulnerability can be summarized as below.

² OpenSSL extension module intended to check out the connection between a client and a server.

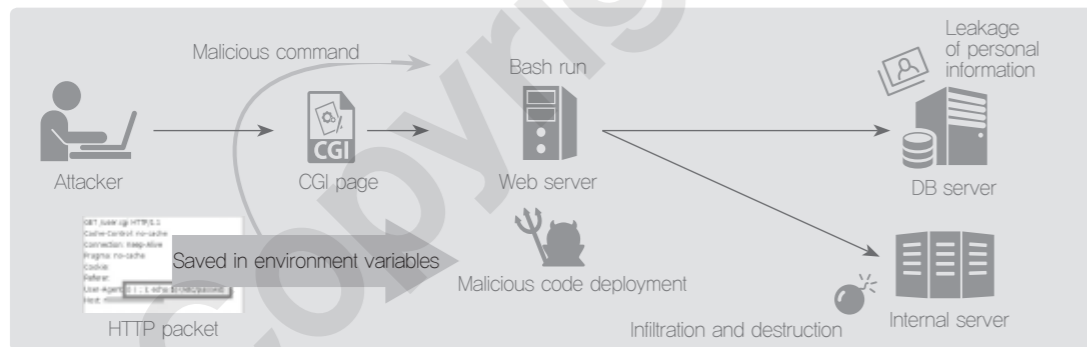
〈Table 46〉 Summary of GNU Bash vulnerabilities

CVE ID	Vulnerabilities
CVE-2014-6271	Remote command execution
CVE-2014-7169	Function definition parsing errors
CVE-2014-7186	Invalid memory access
CVE-2014-7187	Invalid memory access
CVE-2014-6277	Function definition parsing errors
CVE-2014-6278	Remote command execution

The vulnerabilities are within the function declaration provided by the Bash shell. When a string of characters that starts with “() {” is stored in the system environment variables, the function with the same name can be declared. However, when an arbitrary command is injected at the end of the function statement, the Bash does not stop processing at the end of the function statement but processes the injected command as well.

② Possible attack scenario

In order to run the shell, the CGI sets ‘the data in the HTTP packet header’ as the environment variable. Hence, if a payload, targeting vulnerabilities, is injected into the header, it is possible to run a certain command in the operation server for the CGI page. The following shows the attack scenario, using the CGI page.



〈Figure 89〉 CGI attack scenario

③ Defense measure

〈Table 47〉 Defense measures against CGI attacks

Defense measures	Details
Bash update	Vulnerable version to be updated to the latest version
Removal of CGI pages (not in use)	To validate whether CGI services are used or not, and to stop unnecessary CGI services or remove CGI pages
Detection rules on the network	To register signatures to the network security devices (IPS/IDS/web firewall) The latest SNORT detection rules available at https://www.snort.org/download

Spear Phishing

① Introduction to spear phishing

Spear phishing does not target a system or a network of an organization whose security readiness is well defined and prepared. Rather, the usual targets are the ones who work for such organizations and have key roles (who have access to the confidential information or important systems. An attacker sends out spear phishing e-mails based on the information about the potential victim the attacker acquired during the preparation phase. By using these kinds of social engineering techniques, the attacker can gain access to the key persons' terminals and monitor those terminals for more than a few months. The attacker can steal the account information (ID, password, etc.) and have control over mission critical systems and the network, using remote control tools.

② Defense against spear phishing

It is necessary that the key persons, such as a security manager or a web server operator, and the end users get trained about the threat that may be posed by the spear phishing and about how to respond to the attacks. Especially in the case of a web server operator, he/she should come up with various measures, such as detecting malicious code, operating a web firewall, and taking web server security measures. In the case of application programs and operating systems, it is recommended to continuously monitor security vulnerabilities and to periodically update the security patches.

NTP (Network Time Protocol) Vulnerability

① NTP vulnerability

NTP (Network Time Protocol) is intended to be used for the time synchronization between the computers connected to the network. However, the NTP packets do not have an encrypted signature which can be used for the authentication. Hence, the NTP packets are weak to the MITM (Man in the Middle) attacks; and can be used to manipulate the message to change the time settings on client PCs. However, in spite of some of the issues, the impact of the attacks using NTP vulnerabilities is not considerably high.

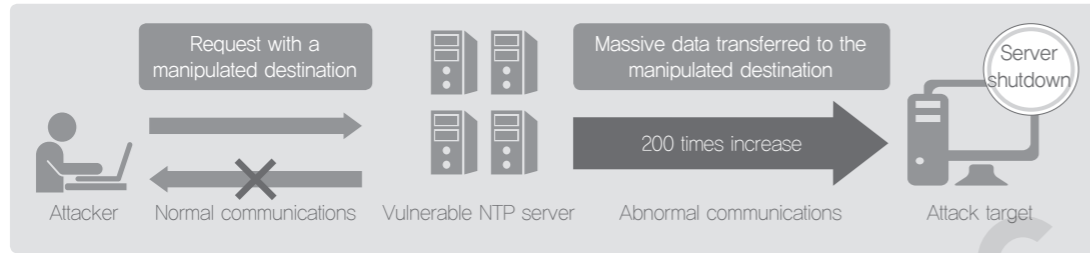
However, the distributed DoS and stack overflow vulnerabilities have caused a significant issue globally.

② Types of NTP vulnerabilities

- NTP vulnerability to distributed DoS

A query can be made to an NTP server, using the ‘monlist’ command, to get the list of the 600 hosts which made access to the server recently.

However, there is no IP verification process in place for the ‘monlist’ command and it is possible to launch a DDoS attack against a certain target.



<Figure 90> DDoS attacks exploiting NTP vulnerability

- Stack overflow of NTP
An unauthorized user can launch a ntpd-related function 'crypto_recv()', 'ctl_putdat()', 'configure()' remotely to trigger a stack overflow.

③ Defense against NTP vulnerabilities

In general, it is recommended to remove NTP services unless they are proven necessary based on the security policy. If and when NTP services should be implemented and operated for the business, it is safer to place the NTP server within a private or a corporate network.

There is a certain set of actions required for the defense: NTP version update, configuration file modification, and checking vulnerabilities are required for an NTP server; and the check-up for a firewall and security device configuration are required for a networking or security device.

02 Latest Information Protection Technologies

Network Separation/Bridge

① Introduction to network separation

Network separation literally means to separate an internal network from an external network (the Internet) in order to prevent the unauthorized access and information leakage. There are two types of network separation: logical and physical separation.

② Logical and physical network separation

<Table 48> Logical and physical network separation

Classification	Physical network separation	Logical network separation
Operation method	A network for the internal business and a network for the Internet are physically separated (Using two PCs).	A logical separation using virtualization or the like. (Using one PC)
Cost	High (additional PC, network building)	Low (varies with the implementation conditions)

Classification	Physical network separation	Logical network separation
Security	High security (fundamentally separated)	Low security (Vulnerabilities may be found)
Efficiency	Low efficiency (business perspective)	Easy management (security policy)
Details	2PCs, multiple PCs, network switching device	Server-based, PC-based

MDM (Mobile Device Management)

① Mobile device management (MDM)

MDM provides a remote controlling function to manage and register mobile devices. It also provides general security policies and functions, such as password level setting, VPN configuration, screen lock time setting, inactivation of a certain application (access to the app store), and blocking a behavior that may cause threats. In addition, an administrator can carry out some security related activities, such as finding a lost/stolen device or deleting the data from the device.

MDM is suitable for a company that needs an integrated mobile solution that can cover an internal app store and a document sharing library. If the application of the MDM is extended to the wider area beyond its general use for the mobile access, such as emails and calendar services, it can significantly contribute to the productivity enhancement.

② Mobile application management (MAM)

MAM is drawing increasing attention due to its functions intended to replace or to supplement the roles of the MDM. The MAM can be regarded as a set of software and services that can help a company develop and deploy mobile applications for the company in an easier and faster way.

WIPS (Wireless Intrusion Prevention System)

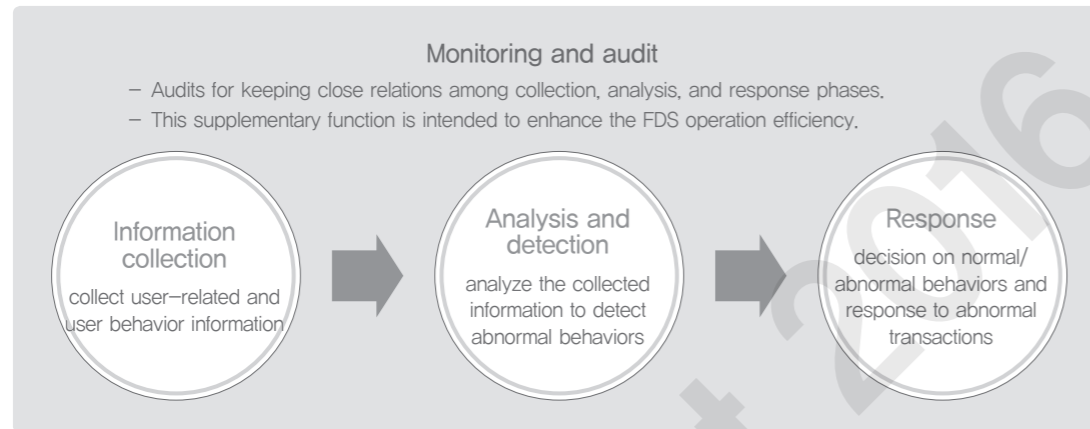
WIPS is capable of: monitoring the wireless LAN within a certain organization in order to automatically detect and prevent the access from unauthorized wireless devices; enhancing wireless LAN stability; and providing an integrated management. The WIPS detects and prevents attempts to break into the system through unauthorized APs or user terminals.

FDS (Fraud Detection System)

① Introduction to fraud detection system

FDS is a comprehensive set of systems which are composed of four components which are intended to holistically

analyze the information from various sources under the purpose of filtering out fraudulent financial transactions. The four components described below should be implemented in a way that each and one of them can be compatible and interconnected.



〈Figure 91〉 Four components of fraud detection system

② Functions of FDS

- (Information gathering) To collect the 'information of a user environment' and 'incident type information' for better detection rate of fraudulent financial transactions.
- (Analysis and detection) To detect any abnormal behaviors based on a range of correlation analysis of user types and of transaction types and based on a set of rule checks
- (Response) To respond to the potential fraudulent financial transactions, such as blocking the transaction
- (Monitoring and auditing) To monitor functions to enforce an overarching management of the transaction with a series of actions, such as information collection, analysis, and response, and auditing functions to audit various types of attacks and infiltrations.

02 Latest Standards for Information Security

Legislations and Regulations Related to Information Security

The legislations and regulations pertaining to information security can be divided into: information security and personal information protection.

〈Table 49〉 Legislations and regulations pertaining to information security

Classification	Name
Information security	Act on Promotion of Information and Communications Network Utilization and Data Protection, etc. (ICN Act)
	Information & Telecommunication Infrastructure Protection Act
	Digital Signature Act
	Framework Act on National Informatization
	E-Government Act
Personal information protection	Personal Information Protection Act
	Act on Promotion of Information and Communications Network Utilization and Data Protection, etc.
	Law on the Protection and Use of Location Information (Location Information Law)

As far as the personal information protection is concerned, there are a series of "sectoral laws" that are specific to the telecommunication, healthcare, education, and many other sectors. The articles about the personal information protection within the ICN Act define the relationship between the information and telecommunication service providers and the users³.

The Personal Information Protection Act is a general law which can be generally applicable to the public and private sectors. Therefore, sectoral laws, such as the ICN Act and the Protection of Credit Information Act, which specify the legal affairs pertaining to the information & telecommunication sector and the financial sector respectively, prevail over the Personal Information Protection Act in the accordance with the principle that a special act takes priority over a general act.

The Location Information Law covers: protection of the location information owner; permission-report-mandate scope of the businesses; and usage of the location information for public good.

Latest Trend of Information Security Standardization

The Korean national standards development process is conducted by the ETRI, KISA, universities, and information security companies. The IT Strategy Standards Forum is held to establish a set of de-facto standards and these standards are later developed as the standards of information and telecommunication organizations through the TTA. To make those Korean standards as a part of international standards: the TTA is leading the standardization process that can be applicable to the ITU-T and IETF; and the KATS is leading the standardization process that can be applicable to the ISO / IEC JTC1.

³ 'User': refers to specific users who actually use the service provided by information and telecommunication providers, not general or random users.

<Table 50> Map of Standardization – Security Common (<http://www.tta.or.kr>)

Classification	Details	
Cryptography	Next generation cryptography algorithm (~'18)	In response to the international standardization trend, which requires a high level of cryptographic technology, the ARIA and SEED (most widely used Korean block cipher) will be actively studied so that they can contribute to better security in the ICT application and convergence services. To lead the standardization process for new ICT services: using Korea's cryptography technologies which are advanced compared to the technologies used in the current international standards.
	PKI-based authentication and application technology (~'18)	In the ITU-T, ISO / IEC JTC1, and the like, the Korean community is leading the proposal for an open and integrated authentication framework where the OTP and various other authentication technologies can be accepted. To pursue the standardization process mainly driven by de-facto standards, such as non-repudiation, suitable for the mobile environment.
Authentication	Integrated authentication framework (~'16)	Since 2009, the Korean community has been leading the study for the secure application protocol (Q. 7) within the ITU-T SG17. In 2011, the management framework of the onetime password-based authentication service (ITU-T X. 1153) was approved as a standard. As a part of new tasks during 2012~2014, in the ITU-T, ISO / IEC JTC1, and the like, the Korean community has been leading the proposal for an open and integrated authentication framework where the OTP and various other authentication technologies can be accepted. To pursue the standardization process mainly driven by de-facto standards, such as non-repudiation, suitable for the mobile environment. In 2015~2016, the Korean community is planning to have a parallel review for the standardization of the detailed technologies that can be useful in effective implementation of the integrated authentication via the ISO/IEC JTC1, IETF, and the like.
	Structure and features for integrated response against malicious code (~'18)	TTA, Cyber Security Forum, vaccine manufacturers, carriers, and other domestic relevant parties will work together to create standard items, and proceeds with the national standardization via the TTA's Cyber Security Project Group (PG503) under the goal of standardization in Korea in 2015 and proposal of standards to the ITU-T in 2016.
Malicious code analysis	Malicious code analysis and reporting (~'18)	To utilize domestic technologies which are advanced in malicious code analysis and reporting, in order to take the lead in international standardization and secure the IPR through the joint contribution and joint development with rival standards organizations, such as IETF and ISO / IEC JTC1. In terms of malicious code analysis, the non-Korean contribution is very high. To be more prepared with the cooperation and competitions in the international standardization, the Korean community needs to focus on developing practical technologies and validating those technologies and to work actively to overcome relative disadvantages in the IPR.

Classification	Details	
Security management/ security assessment	Common Evaluation Criteria/ Common Methodology for Information Technology Security Evaluation (~'15)	To update the revised version of the Common Evaluation Criteria/ Common Methodology for Information Technology Security Evaluation onto the Korean standards, to actively participate in the community activities in cooperation with relevant domestic parties in developing the evaluation criteria and methodologies for each of the technologies, to develop supporting documents for each technology and to contribute to the standardization process.
	Criteria for Competencies for Information Security Management Professionals (~'17)	The criteria for the Competencies for Information Security Management is being developed in the ISO with three years of time line: need to actively participate in the revision process of the international standards in order to standardize the process and requirement; domestic certificates need to be accommodated within the international standards; and overseas best practice needs to be adopted.
	Information security audit management guideline (~'18)	The information security audit management guideline was partially standardized by the ISO, but still standards development is going on in many other segments. Need to actively participate in the establishment/revision process of the international standards in order to standardize the process and requirement, domestic guideline needs to be accommodated within the international standards

<Table 51> Map of standardization – network/device security (<http://www.tta.or.kr>)

Classification	Details	
Wired network	Security requirement for cloud service in the network environment (~'17)	In cooperation with the United States to jointly develop the ITU-T SG13 international standards for providing cloud services on the future network environment, and to improve the quality in cooperation with external standardization bodies like the OCC (Open Cloud Consortium)
	SDN security framework and mechanism (~'17)	In cooperation with the United States to jointly develop the ITU-T SG13 international standards for providing cloud services on the future network environment, and to improve the quality in cooperation with external standardization bodies like the OCC (Open Cloud Consortium)
Wireless network	M2M (IoT) communications infrastructure protection framework (~'17)	As the M2M has a lot of open opportunities in the market for the next 10 years or so, there will be a fierce competition in and out of Korea as standardization efforts will be made in various perspectives. The Korean standardization was made even before the industry use the technologies in earnest. However, the standards need to be enhanced after going through the comparison and validation process against the international standards.
	M2M (IoT) gateway and access network protection framework (~'18)	In the advanced countries, the standardization work was already initiated regarding the M2M gateway and access network, but the Korean community cannot catch up with that. Need to fine-tune and diversify the standardization tasks to catch up with the international standardization level as soon as possible.

Classification	Details	
Device security	Smartphone application security validation frameworks (~'15)	To jointly develop the ITU-T SG17 international standards along with Japan, so that a certain level of security can be provided for smartphone applications. To cooperate with the external standardization bodies like the GSMA to improve the quality.
	Security measures for smartphones (~'17)	Among the smartphone-related security measures, the Korean community is around one year advanced in multi level security technology and standardization. Needs to take the area as a next generation strategic target and to take the lead in the international standardization.

Classification	Details	
Personal information protection	Foundation technology for identity management (~'17)	With regard to mobile ID, on smartphones, there are not many commercialized technologies even in the overseas market. It should be helpful to gain the competitive momentum if we can work on the international standard development and product development at the same time.
	Mobile payment technology (~'16)	In the initial stage of the mobile payment development, each of the service providers tends to try and use different methods and technologies, and it can be a major stumbling block for the industrial development. In particular, if the technology development and standardization can be initiated in the commonly applicable areas based on the major cases and lessons learned from Korea, it can be of great contribution to the international standardization process
Financial security	Mobile financial security framework (~'16)	To make proposals to the ISO TC68, by integrating the existing standards of Korea (Micro SD & USIM-based mobile payment, TEE-based framework) A wide range of mobile payment services, using wireless technologies (like the NFC), are on the rise. Need to develop security criteria, test criteria, and methods that can be used to ensure the service security, and need to make them exchanged with the international criteria for better compatibility.
Smart grid security	Security functional architecture for smart grid (~'15)	To promote the security functional architecture for smart grid recommendation as an international standard via the ITU-T SG17. At the same time, need to listen to opinions from smart grid and information security experts to develop a Korean standard and to work on the international standardization based on the Korean standards. (In parallel)
Healthcare security	Medical information security (~'18)	The Korean community is a late comer in the area of the international patent for medical the information security: need to nurture talented resources, need to respond to the international standardization based on the Korean standards that were already proven by the domestic services. In cooperation with government agencies and government-funded research institutes, it is necessary to work on the security standardization of data communications between the information systems and for smart medical devices within Korea.
Convergence: security for vehicles	Security framework For V2X communication (~'18)	The ITU-T SG16 is in progress for the standardization of the Intelligent Transport System (ITS) and the SG17 is working on the development of the ITS security standards. It is necessary to come up with standard contributions and proposals of work items.

<Table 52> Map of standardization – service/convergence security (<http://www.tta.or.kr>)

Classification	Details	
Cloud/ big data security	Cloud privacy protection guidelines (~'17)	To develop the technology for cloud privacy protection and to work on the international standardization in cooperation with influential forums like the CSA (Cloud Security Alliance). To refer to the activities of the TTA's Cyber Security Project Group (PG503) in order to work on the domestic standardization regarding the technologies for cloud privacy protection.
	Intrusion detection analysis requirements on virtual network (~'16)	To work on international standardization in cooperation with influential forums like the CSA (Cloud Security Alliance). As for the virtual network intrusion detection analysis requirements, it is necessary to refer to the technology development for the intrusion detection and response in the virtualized system of the cloud environment. A patent application should be made with the core technologies, and an essential patent, including the core technologies, should be pursued in and out of Korea.
	Data security of big data (~'17)	To work on standardization through the ODCA and CSA, especially focusing on the data format and data applications, from the commercialization perspective. To work intensively on the tasks related to the interface standard, between the organizations and groups which provide security services, along with the official standardization bodies, such as ISO/IEC JTC1 BD-SG, ITU-T To work on the standardization that can accommodate mobile services and managed security services, considering the domestic industrial circumstances.
DB/web security	Next generation web security (~'17)	An international standard regarding the next generation web-based integrated service security was developed in the ITU-T SG17, mainly driven by Korea. The security requirements of guideline standards and the web mashup information protection framework standard were approved. Need to engage in the competition of standard development for the next generation web security.
	Mobile web security (~'17)	Need to respond based on cooperation with/competition against advanced countries in the international standardization process. The W3C is pushing for the standardization with the One Web and multimedia security technologies. Hence, Korea needs to narrow the technological gap so that the Korean technologies can be accommodated in the standards. Need to respond to the recent development of web security technologies in the IETF, such as authentication/ authorization in constrained environment and the security standard for the datagram transmission
	Web privacy protection (~'15)	Lack of remarkable standards development since the W3C's P3P standards. Need to work on the international standardization based on domestic regulations and guidelines via the ITU-T SG17.

Example Question

Question type

Descriptive question

Question

There is an increasing number of information leakages as a wide range of attack patterns are available. GNU Bash Shell has vulnerability where an attacker can run an arbitrary command in the operating server of a web page. Please describe the procedure; how the vulnerability can be in action, and what can be the potential response to the vulnerability.

Intent of the question

To evaluate whether a learner understands what are the latest attack methods and how to address those attacks.

Answer and explanation

The vulnerabilities come from the function declaration provided by the Bash shell. However, when an arbitrary command is injected at the end of the function statement, the Bash does not stop processing at the end of the function statement, but processes the injected command as well.

To tackle the vulnerability:

The version should be updated to the latest version.

Web pages and services not in use should be disabled.

To apply detection rules on the network.

The most likely attack is the one targeting CGI pages.

In order to run the shell, the CGI sets 'the data in the HTTP packet header' as the environment variable. Hence, if a payload, targeting vulnerabilities, is injected into the header, it is possible to run a certain command in the operation server for the CGI page. The general rule to avoid this vulnerability is to update the vulnerable Bash to the latest version.

Related E-learning Contents

- **Lecture 8** Latest Trend and Standards in Information Security
- **[Advanced] Lecture 4** Latest Technologies and Standards in Information Security