정보통신망 제 15 강

네트워크 보안(II)

컴퓨터과학과
손진곤 교수

학습 목차

제 15 강 네트워크 보안(II) - 보안 강화 방법

학습 내용

- 암호 기법
- 디지털 서명
- 웹 보안 프로토콜
- 방화벽
- 프락시 서버

학습 목표

- 암호화 기술을 구분하여 설명할 수 있다.
- 디지털 서명을 설명할 수 있다.
- 웹 보안 프로토콜을 구분하여 설명할 수 있다.
- 방화벽의 기능과 종류를 설명할 수 있다.
- 프락시 서버의 기능을 설명할 수 있다.

1. 암호 기법

(1) 암호 기법의 개요

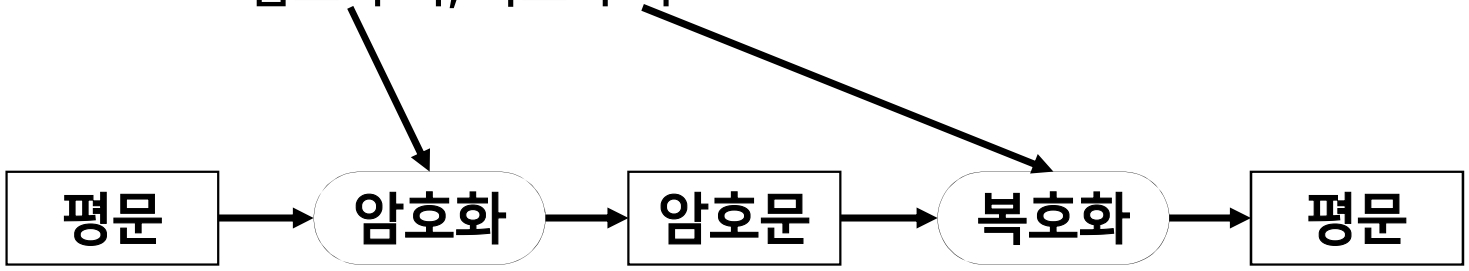
(2) 암호화 기술

(3) 키 관리

1 암호 기법의 개요

개요

- 암호화(encryption)
  - 누구나 읽을 수 있는 평문(plaintext)을 제3자가 읽을 수 없는 형태인 암호문(ciphertext)으로 변환하는 과정
- 복호화 (decryption)
  - 암호문을 평문으로 변환하는 과정
- 키(key)
  - 암호화 키, 복호화 키



1 암호 기법의 개요

암호화의 주요 기능

- 전달 과정의 기밀성 보장
- 정보의 무결성 보장
- 송신자와 수신자의 정당성 보장

※ 네트워크 보안의 5가지 요구 사항

- 기밀성 보장 – 데이터 보안성
- 무결성 보장 – 데이터 무결성
- 정당성 보장 – 실체 인증, 데이터 인증, 부인 방지

2 암호화 기술

암호화 기술 - 분류

(1) 동작 형태

- 대치 암호, 전치 암호, 혼합 암호, 대수화 암호

(2) 평문의 처리 방법

- 스트림 암호화, 블록 암호화

(3) 암호화 키

- 대칭 키 암호화, 공개 키 암호화

2 암호화 기술

(1) 동작 형태

1) 대치 암호 (치환 암호; substitution cipher)

- 메시지의 각 글자를 다른 글자로 대치하는 방식
  - 예 : Caesar 암호
  - HAL9000 (영화 “2001년 스페이스 오딧세이”)

2 암호화 기술

(1) 동작 형태

2) 전치 암호 (전위 암호; transposition cipher)

- 평문의 글자를 재배열하는 방식(문자의 위치를 바꿔 암호문을 작성)
  - 예 : 스파르타의 Lysander 장군의 암호 (2개의 원통을 사용)

http://timetravellerkids.co.uk/uncategorized/make-greek-scytale-cipher/

2 암호화 기술

(1) 동작 형태

2) 전치 암호 (전위 암호; transposition cipher)

```
KIM MUST ARRIVE SEOUL BEFORE MIDNIGHT.

    1 2 3 4 5 6 7
    K I M   M U S      352761
    T   A R R I V
    E   S E O U L
    B E F O R E
    M I D N I G T


MASFDMRORII  EISVL TUIUEGKTEBM
```

2 암호화 기술

(1) 동작 형태

3) 혼합 암호 (product cipher)

- 대치와 전치 두 방법 모두를 사용하는 방식
  - 예 : LUCIFER, ENIGMA, ADFGVX, DES 등

4) 대수적 암호 (algebraic cipher)

- 각 글자를 숫자로 바꾸어 수학적으로 처리하는 방식
  - 예 : 순환잉여검사 (CRC), Vernam 암호 방식

2 암호화 기술

(2) 평문 처리 방법

1) 스트림 암호화 (stream cipher [state cipher] encryption)

- 평문과 같은 길이의 키 스트림을 생성하여
  평문과 키를 비트 단위로 합하여 암호문을 얻는 방법
- 평문은 한 번에 한 비트씩, random하게 생성되는
  키 스트림과 XOR 연산으로 합해져서 전송됨

2 암호화 기술

(2) 평문 처리 방법

2) 블록 암호화 (block cipher [state cipher] encryption)

- 평문을 일정한 길이의 단위(block)로 나눈 뒤,
  각 block 단위로 암호화 과정을 수행하여 암호문을 얻는 방법
- 대표적인 예 : LUCIFER, DES

➢ 비교 :

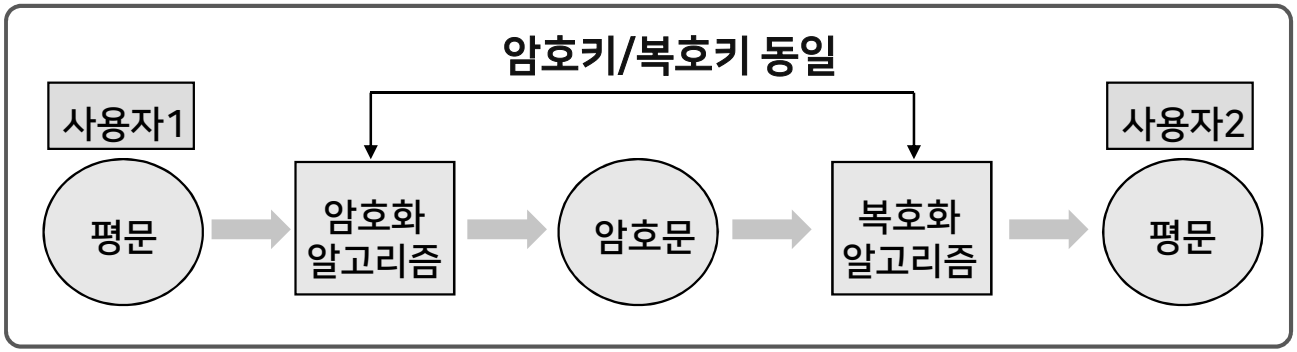
- 스트림 암호화 방식 : 비트 단위의 암호화
- 블록 암호화 방식 : 블록 단위의 암호화

2 암호화 기술

(3) 암호화 키

1) 대칭 키 암호화 (symmetric key encryption)

- 암호화 키 = 복호화 키
- 유사어 : **공통 키** (common key) 암호화
  비밀 키 (secret key) 암호화
  관용 암호화 (conventional encryption)



[그림] 대칭 키 암호화 과정

2 암호화 기술

(3) 암호화 키

1) 대칭 키 암호화 (symmetric key encryption)

- 장점 : 구현이 용이하고 실행 속도가 빠름
- 단점 : 키 분배 및 관리가 어려우며,
  인증과 송수신 부인 방지가 보장되지 않음
- 예 : RC2, RC4, RC5, IDEA, DES, Triple DES, AES

2 암호화 기술

(3) 암호화 키

1) 대칭 키 암호화 (symmetric key encryption)

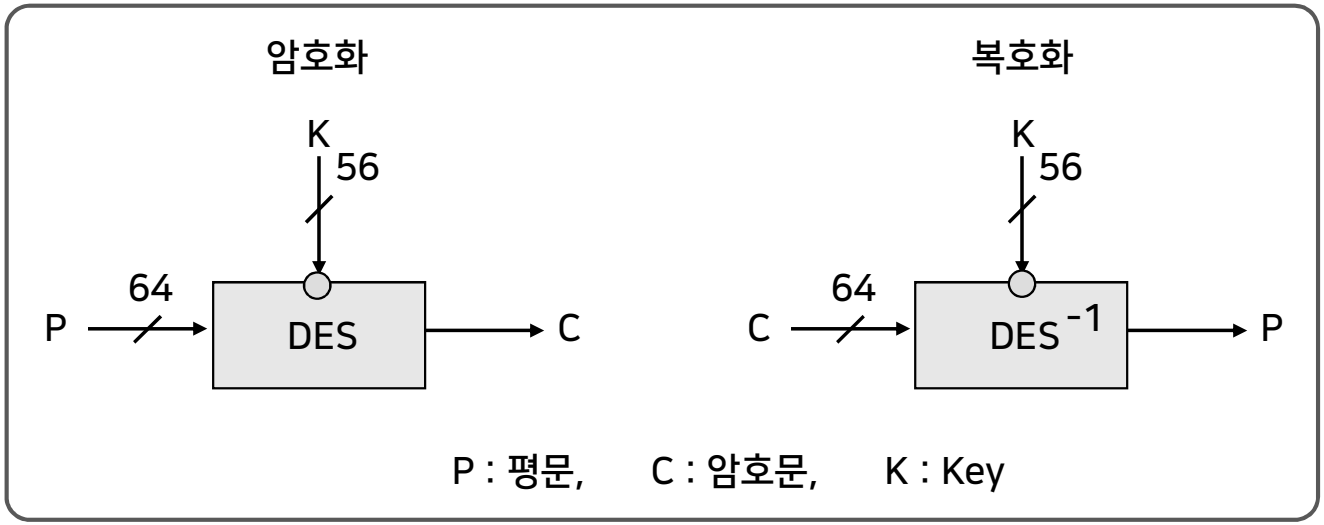
- DES (Data Encryption Standard)
  - 대칭 키를 사용하는 블록 암호화 방식
  - IBM에서 개발한 LUCIFER의 확장된 형태로 제안되어 1976년 NBS에서 미국정부 표준암호 방법으로 제정
  - 평문 한 블록 (64 비트)을 공통 키 (54 비트)를 이용, 전치, 대치, XOR 연산 등을 16회 반복하여 암호문 한 블록 (64 비트)을 완성함.
- AES (Advanced Encryption Standard)
  - 2001년 NIST에서 미국정부 표준암호 방법으로 제정

2 암호화 기술

(3) 암호화 키

1) 대칭 키 암호화 (symmetric key encryption)

- **DES** (Data Encryption Standard)



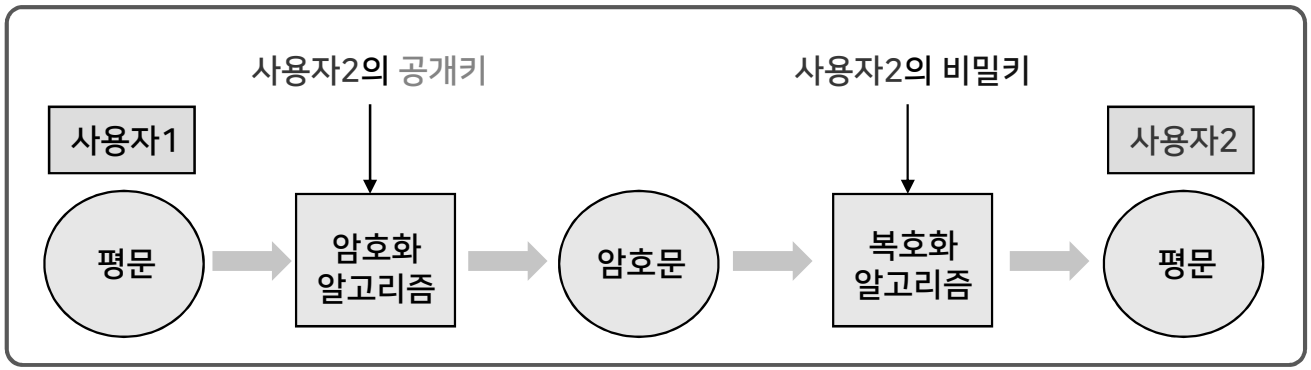
[그림] DES의 암호화와 복호화 과정

2 암호화 기술

(3) 암호화 키

2) 공개 키 암호화 방식 (public key encryption)

- 특징
  - 암호화 키 = 공개 키(public key) / 복호화 키 = 개인 키(private key)
- 유사어
  - **비대칭** 키 (asymmetric key) 암호화



[그림] 공개키 암호화 알고리즘의 암호화와 복호화 과정

2 암호화 기술

(3) 암호화 키

2) 공개 키 암호화 방식 (public key encryption)

- 장점
  - **공통 키 암호화 방식의 키 분배 문제를 해결**
  - **디지털 서명 기능 (부인 봉쇄 가능)**
- 단점
  - 구현이 어렵고, 처리 속도가 느림

2 암호화 기술

(3) 암호화 키

2) 공개 키 암호화 방식 (public key encryption)

- RSA 암호화 알고리즘
  - 1978년 MIT의 3명의 수학자(Rivest, Shamir, Adleman)가 개발
  - 가장 대중화된 공개 키 암호화 방식
  - 2개의 큰 소수 p, q를 구하고, 두 소수의 곱 n을 구해 사용하는데, 이 암호화 방식의 안전도는 n의 소인수분해 난이도에 종속됨

3 키 관리

키 관리

- 사용되는 키들을 안전하게 다루기 위해 키를 관리함
  - ✓ 키 생성, 등록, 확인, 분배, 설치, 저장,
    파생, 보관, 취소, 말소, 폐기 등

3 키 관리

공개 키 관리

- 공개 키는 공개되므로 위조, 변조가 가능함
- 공개 키 인증서 (certificate)
  - 공개 키를 인증하는 전자적 증명문서
  - 인증 만기일, 인증서 발급기관 이름, 일련번호, 인증서 발급기관의 디지털 서명
  - 인증서의 형식은 ITU-T X.509 표준에 따름

3 키 관리

공개 키 기반 구조

- Public Key Infrastructure (PKI)
  - 공개 키 인증서를 발급하고 사용할 수 있는 인증서 관리 구조
- 인증기관 (Certificate Authority; CA)
  - 일반인에게 개인 키와 공개 키를 부여하고, 인증서를 통해 상대방의 공개 키를 제공하는 서비스 기관
- 인증서
  - 기재된 통신 객체 (개인, 기관, 컴퓨터)의 신분을 보증
  - 인증기관의 디지털 서명이 포함되어 있어서 인증기관의 개인 키 없이는 위조, 변조할 수 없음

2. 디지털 서명

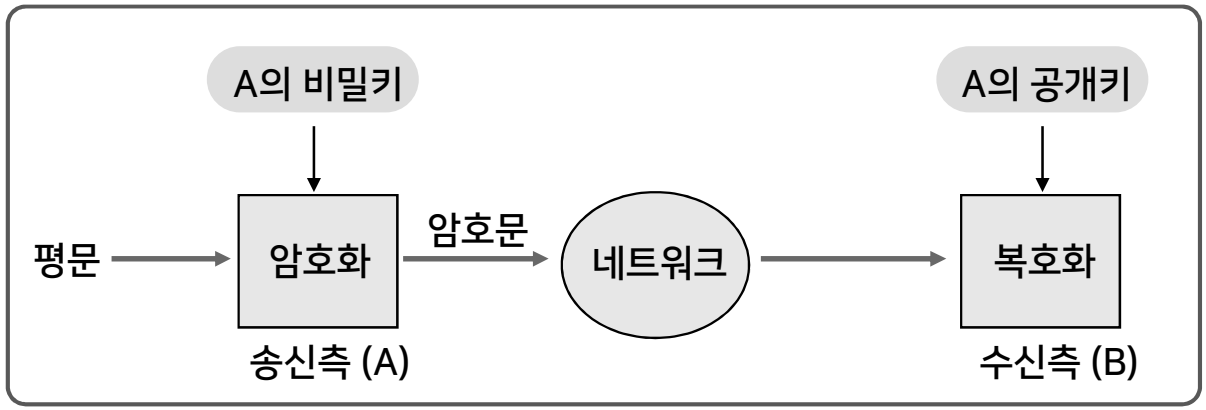
(1) 디지털 서명의 개요

(2) 디지털 서명의 유효성

2 디지털 서명

디지털 서명 (digital signature)의 개요

- 공개 키 암호화 방식에서의 메시지 암호화는
  개인 키를 이용한 메시지 작성자만이 할 수 있으므로
  이를 이용하여 메시지의 작성자 본인을 알리는 서명을 작성함.
- 서명 알고리즘 및 증명 알고리즘

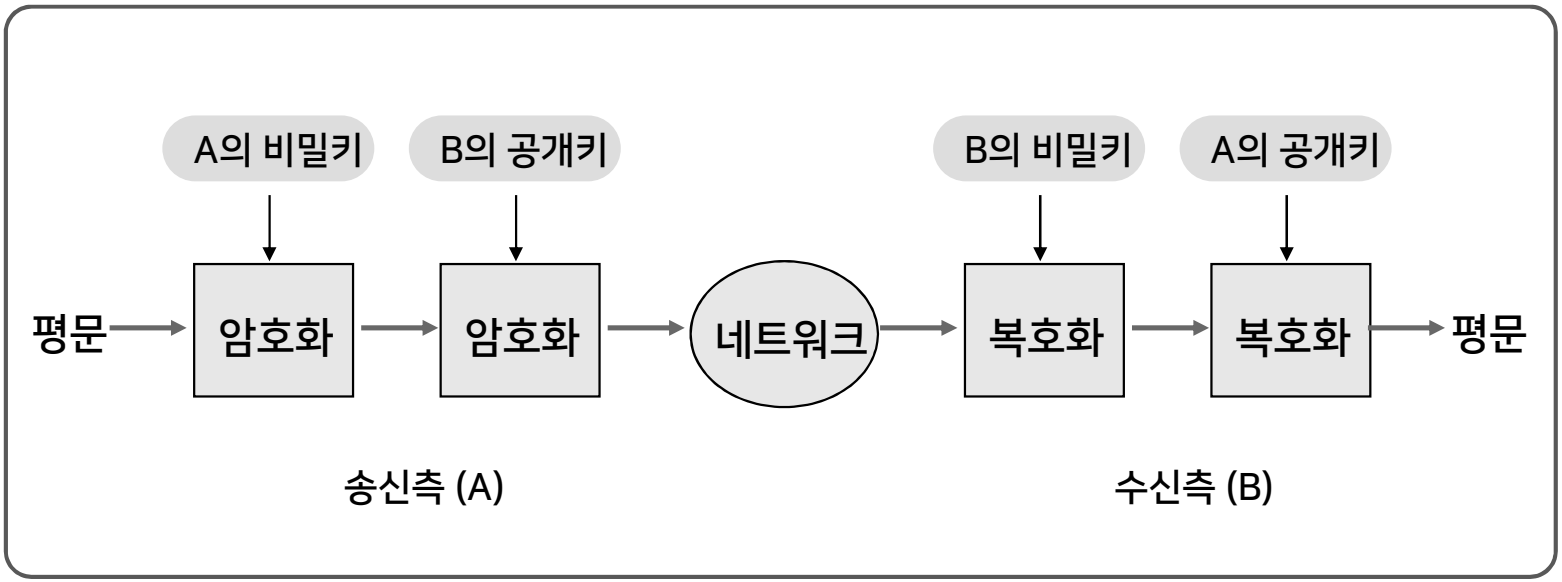


[그림] 디지털 서명에 의한 인증 예

2 디지털 서명

디지털 서명 (digital signature)의 개요

- 디지털 서명을 포함하는 메시지 전송



[그림] 디지털 서명과 메시지 암호화

2 디지털 서명의 유효성

디지털 서명의 유효성을 위한 5가지 조건

① 서명자 인증(user authentication)

- 디지털 서명의 서명자를 불특정한 다수의 사람들이 검증할 수 있어야 함

② 부인 불가(non-repudiation)

- 서명자는 서명 이후 서명 사실을 부인할 수 없어야 함

③ 변경 불가(unalterable)

- 서명한 문서의 내용은 변경할 수 없어야 함

2 디지털 서명의 유효성

디지털 서명의 유효성을 위한 5가지 조건

④ 재사용 불가(not reusable)

- 어느 한 전자문서의 디지털 서명을 다른 전자문서의 디지털 서명으로 사용할 수 없어야 함

⑤ 위조 불가(unforgeable)

- 적법적인 서명자만이 디지털 서명을 할 수 있어야 함

3. 웹 보안 프로토콜

(1) 웹 보안 프로토콜 분류

(2) 응용계층 웹 보안 프로토콜

(3) 전송계층 웹 보안 프로토콜

(4) 네트워크계층 웹 보안 프로토콜

3 웹 보안 프로토콜

웹 보안 프로토콜 – 분류

- 웹 보안을 위한 프로토콜
  - 응용계층 프로토콜
    - 이메일 보안 : PGP, PEM, S/MIME
    - HTTP 보안 : S-HTTP (Secure HTTP)
    - 원격 로그인 보안 : SSH (Secure Shell)
  - 전송계층 프로토콜
    - SSL (Secure Socket Layer)
    - TLS (Transport Layer Security)
  - 네트워크 계층 프로토콜
    - IPSec (Internet Protocol Security)

3 웹 보안 프로토콜

응용계층 웹 보안 프로토콜 - 이메일 보안

1) PGP (Pretty Good Privacy)

- 1991년 Philip Zimmermann에 의해 개발
- 공개 키 암호화 방식을 사용
- 기능
  - ➢기밀성 : 제3자는 이메일 내용을 볼 수 없음
  - ➢메시지 인증 : 메시지가 위조, 변조되지 않았음을 인증
  - ➢사용자 인증 : 이메일의 발신자가 누구인지 확인
  - ➢송신자 부인 방지 : 이메일 발송 부인의 방지

3 웹 보안 프로토콜

응용계층 웹 보안 프로토콜 - 이메일 보안

2) PEM (Privacy Enhanced Mail)

- IETF(Internet Engineering Task Force)에서 표준으로 제정한 공개 키 암호화 방식의 이메일 보안 방식
- 표준으로 제정되었으나 실제로 활용되지는 못하였음

3) S/MIME (Secure/Multipurpose Internet Mail Extension)

- MIME으로 캡슐화된 이메일에 대해 공개 키 암호와 디지털 서명을 제공해주는 이메일 보안 표준 프로토콜
- 공개 키 암호화 방식, RSA 암호 방식을 이용

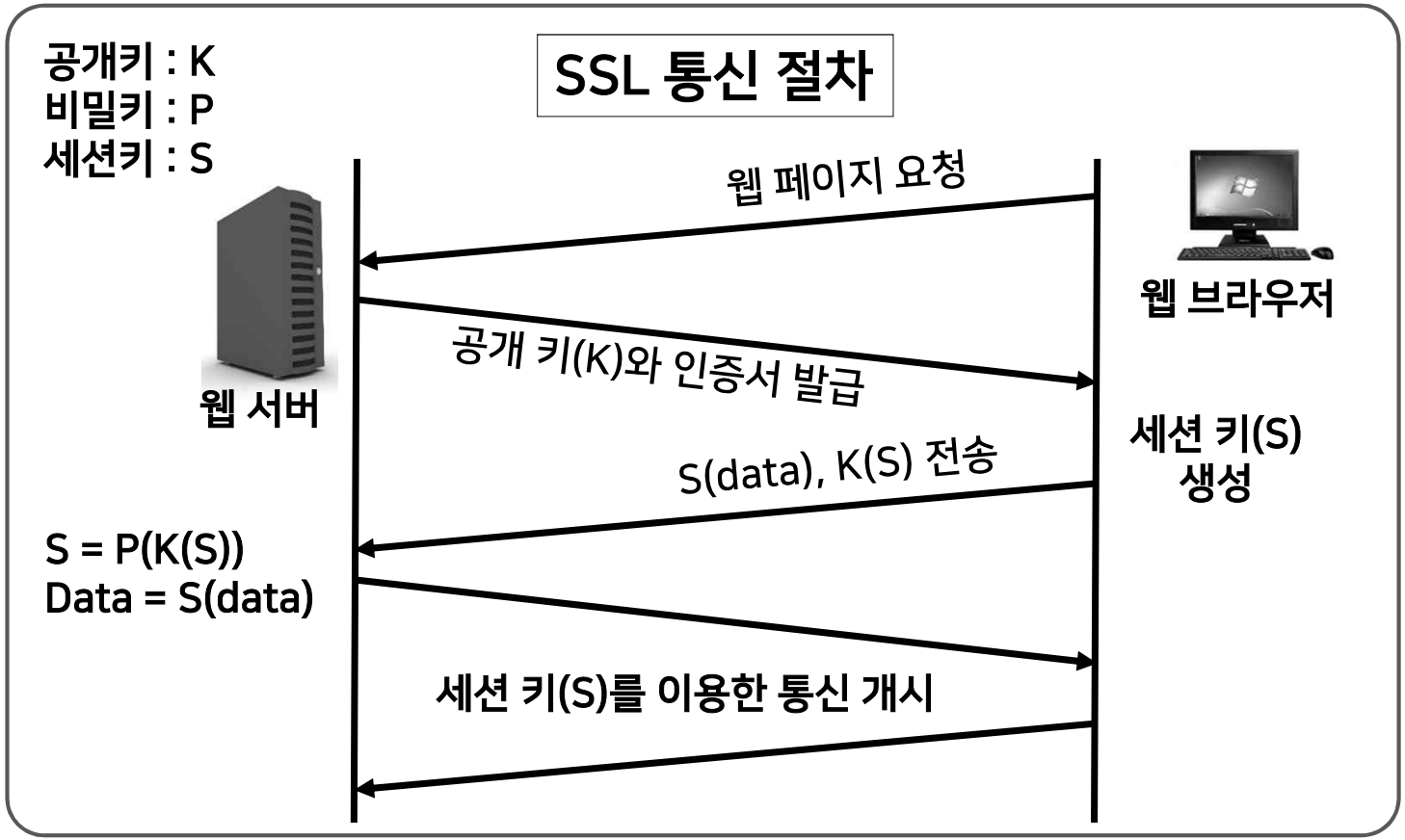
3 웹 보안 프로토콜

전송계층 웹 보안 프로토콜 - SSL

- SSL (Secure Sockets Layer)
- 웹 페이지 보안 프로그램으로 대부분의 웹 브라우저가 지원해 줌
- Netscape Communications사에서 개발한 de facto standard
- http 외에도 ftp, SMTP, Telnet 등의 응용에도 적용 가능
- SSL이 적용된 웹 페이지의 URL은 **https**로 시작되며
  보안 포트 (보통 443번 port)를 사용
  (참고: http는 80번 port)

3 웹 보안 프로토콜

SSL (Secure Sockets Layer)



3 웹 보안 프로토콜

전송계층 웹 보안 프로토콜 - TLS

- TLS (Transport Layer Security)
- SSL을 계승한 전송 계층의 보안 프로토콜
- TLS의 상위계층의 응용 프로토콜과는 독립적이기 때문에
  어떤 응용 프로그램도 TLS를 이용하여
  안전한 통신을 할 수 있음

3 웹 보안 프로토콜

네트워크계층 웹 보안 프로토콜 - IPSec

- IPSec (Internet Protocol Security)
- IP 계층 (네트워크 계층)에서 동작하는 보안 프로토콜
  - Authentication Header(AH) :
    - ✓ 송신자의 인증
  - Encapsulation Security Payload(ESP) :
    - ✓ 송신자의 인증과 데이터 암호화
- IP 계층에서의 데이터 기밀성, 데이터 무결성,
  데이터 인증 등의 보안 서비스를 제공

4. 방화벽과 프락시 서비

(1) 방화벽의 개요
(2) 방화벽의 종류
(3) 프락시 서버의 개요
(4) 프락시 서버의 기능

4 방화벽과 프락시 서버

(1) 방화벽의 개요

- 방화벽(firewall)은 네트워크와 네트워크 사이에서 패킷을 검사하여 조건에 맞는 패킷만을 통과시키는 (packet filtering) 소프트웨어나 하드웨어를 총칭함

4 방화벽과 프락시 서버

(2) 방화벽의 종류

- 배스천 호스트(bastion host)
- 스크리닝 라우터(screening router)
- 이중 홈 게이트웨이(dual-homed gateway)
- 스크린 호스트 게이트웨이(screened host gateway)
- 스크린 서브넷(screened subnet)

4 방화벽과 프락시 서버

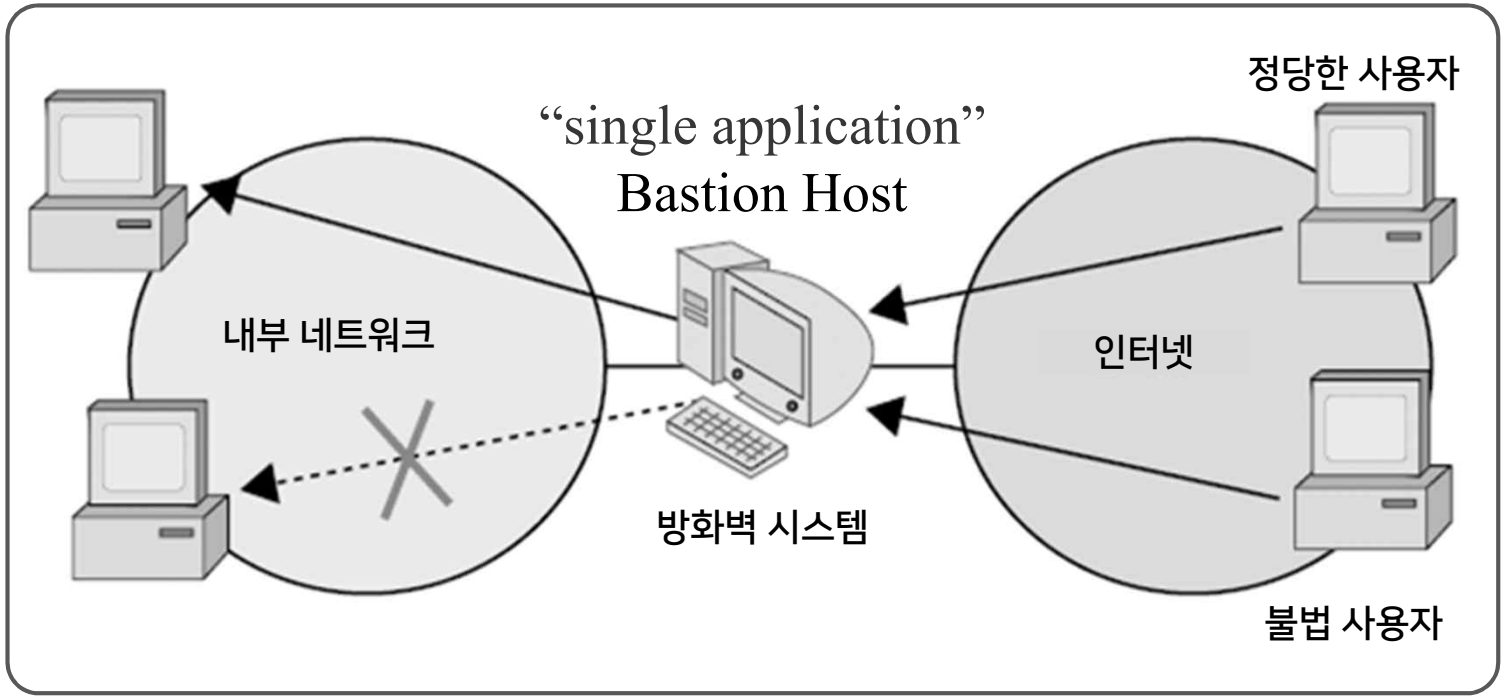
방화벽의 종류

- 배스천 호스트(bastion host)

4 방화벽과 프락시 서버

방화벽의 종류

- 배스천 호스트(bastion host)

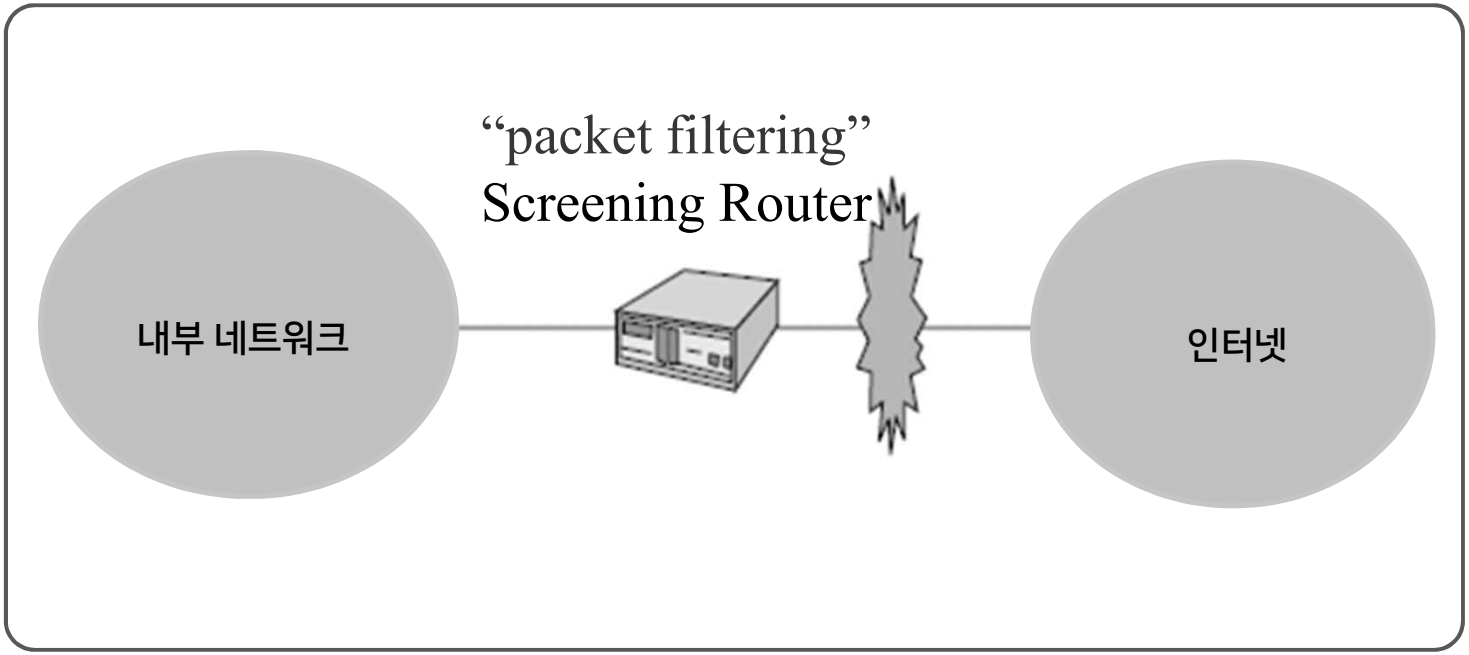


[그림] 방화벽 시스템

4 방화벽과 프락시 서버

방화벽의 종류

- 스크리닝 라우터(screening router)

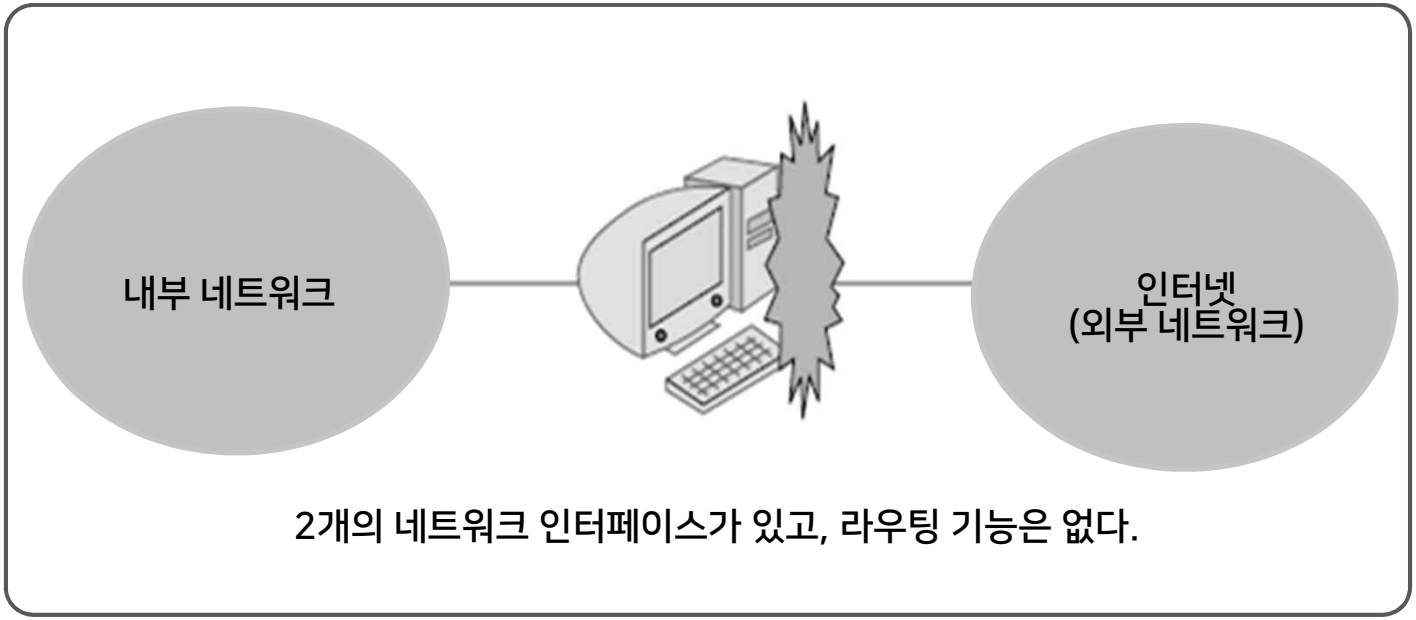


[그림] 스크리닝 라우터

4 방화벽과 프락시 서버

방화벽의 종류

- 이중 홈 게이트웨이(dual-homed gateway)
  - 2개 이상의 네트워크에 동시에 접속된 Bastion host

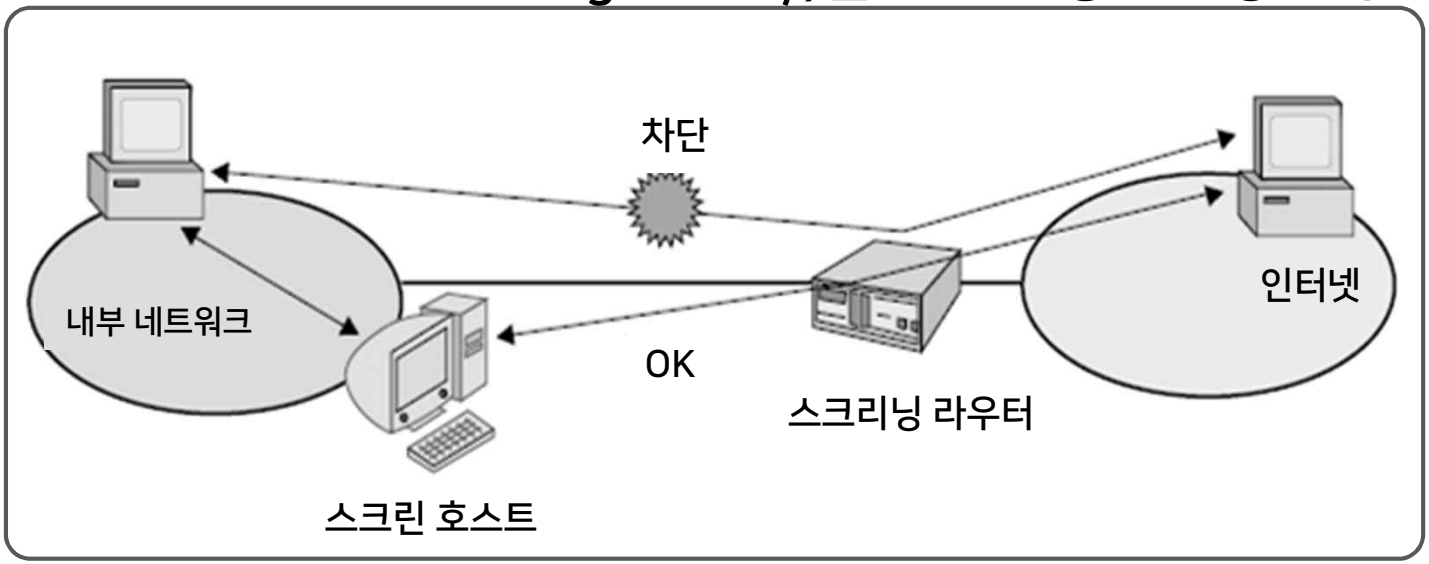


[그림] 이중 홈 게이트웨이

4 방화벽과 프락시 서버

방화벽의 종류

- 스크린 호스트 게이트웨이(screened host gateway)
  - 스크리닝 라우터와 스크린 호스트(Bastion host 또는 Dual-homed gateway)를 혼합한 형태의 방화벽

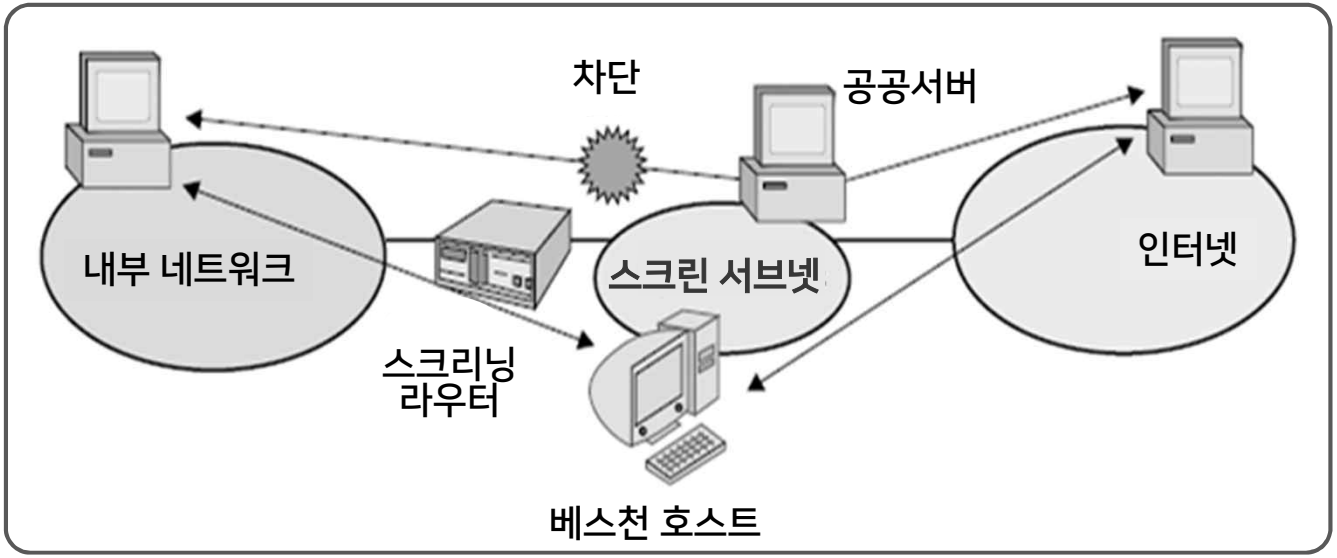


[그림 8.11] 스크린 호스트 게이트웨이

4 방화벽과 프락시 서버

방화벽의 종류

- 스크린 서브넷(screened subnet)
  - 외부 네트워크와 내부 네트워크 사이에 DMZ의 역할을 하는 완충 지역 개념의 서브 네트

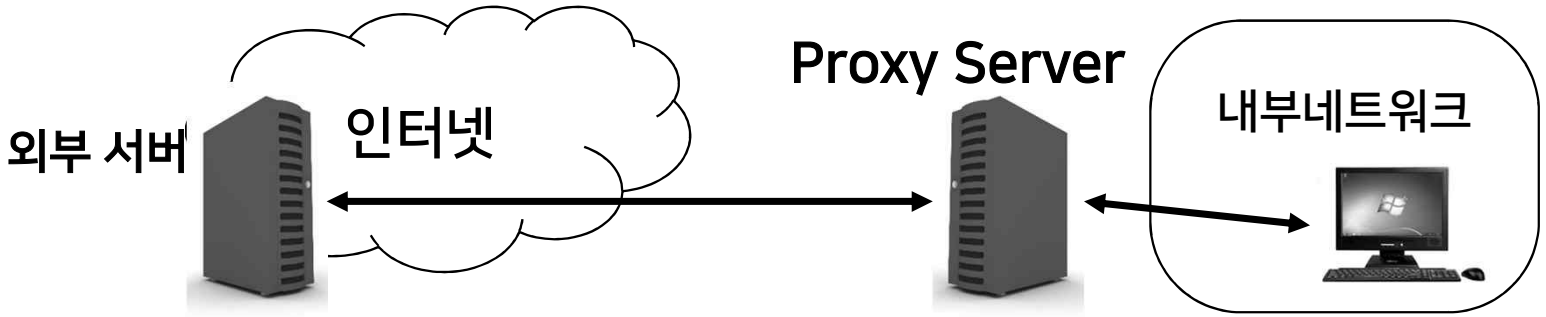


[그림] 스크린 서브넷

4 방화벽과 프락시 서버

(3) 프락시 서버(proxy server)의 개요

- 내부 네트워크에 있는 Client를 대신하여 인터넷에 접속하고 Client가 요청한 통신 서비스를 Client에게 제공해주는 서버
- 동작 절차
  - ① Proxy server는 client 요청에 따라 외부 서버에게 서비스 요청
  - ② 외부 서버는 proxy server에게 요청한 서비스를 전달
  - ③ Proxy Server는 전달받은 서비스를 client에게 전달



4 방화벽과 프락시 서버

(4) 프락시 서버의 기능

- 안정성 : 사용자 인증 기능, 서비스 이용 제한 등의 기능을
  proxy server에 두면 client는 일괄적 보호를 받음
- 익명성 : 외부 서버에 접근하는 것은 proxy server이므로,
  client의 고유정보가 노출될 가능성이 감소함
- 신속성 : 사용자가 열람한 웹 사이트의 정보를 캐시에
  임시적으로 보관해놓는데, 이를 이용하면
  client가 동일한 웹 사이트에 접속하는 경우
  서비스를 신속하게 할 수 있음

학습 내용 정리

제 15 강 네트워크 보안(II)

(1)암호 기법

- 암호화 기술의 분류
  - 동작 형태 : 대치 / 전치 / 혼합 암호, 대수화 암호
  - 평문의 처리 방법 : 스트림 암호화, 블록 암호화
  - 암호화 키 : 대칭 키 암호화, 공개 키 암호화

(2)디지털 서명

학습 내용 정리

제 15 강 네트워크 보안(II)

(3)웹 보안 프로토콜

- PGP, PEM, S/MIME (응용계층)
- SSL, TLS (전송계층)
- IPSec (네트워크계층)

학습 내용 정리

제 15 강 네트워크 보안(II)

(4) 방화벽과 프락시 서버

- Firewall: 조건에 맞는 패킷만을 통과시키는 소프트웨어나 하드웨어를 총칭
- 종류 : Bastion host, Screening router, Dual-homed gateway, Screened host gateway, Screen subnet
- Proxy Server: 내부 네트워크에 있는 client를 대신하여 인터넷에 접속해주는 서버

정보통신망 복습

장	제목	학습 내용
1	컴퓨터통신망 소개	컴퓨터통신망의 정의,역사, 활용 목적 데이터 통신 시스템 통신 프로토콜
2	데이터 통신의 기초	변조 및 복조 전송 코드 전송 방식 및 전송 효율
3	데이터 통신의 요소	통신 선로, 전송 매체 네트워크 형태 네트워크 장치 및 네트워크 소프트웨어
4	데이터 통신의 기능	데이터 교환 방식 오류제어 흐름제어, 경로선택

정보통신망 복습

장	제목	학습 내용
5	OSI 참조 모델	OSI 참조 모델 개관 계층의 분리원칙과 캡슐화 계층별 서비스
6	TCP/IP	개요(역사 및 기본 구조) IP, UDP, TCP ARP, RASP, ICMP, IGMP, DHCP
7	근거리 통신망	개요(정의, 역사, 특성, 효과 등) 분류(위상, 전송매체, 전송방식, MAC방식) LAN의 참조모델 및 표준화 무선 LAN 및 고속 LAN
8	네트워크 보안	개요(보안 요구사항 및 보안 위협 유형) 암호 기법, 디지털 서명, 웹 보안 프로토콜 방화벽과 프락시 서버

좋은 글, 좋은 생각

사회적 경력 · 학력을 제외하고 자신을 설명할 수 있는 사람은 참 행복한 사람이다.
명함을 내보이지 않고 자신을 얼마나 자세하게, 그리고 흥미롭게 서술할 수 있는가가 진정한 성공의 기준이다.

(김정운, "에디톨로지" 중에서)