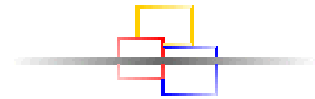




제 9장 e-비즈니스 보안

제 1 절 보안이란 무엇인가?



정보보안정책

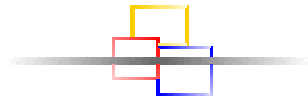
1) 관리적 보안

- (1) 보안정책
- (2) 인력관리
- (3) 절차 관리
- (4) 사고대책 관리

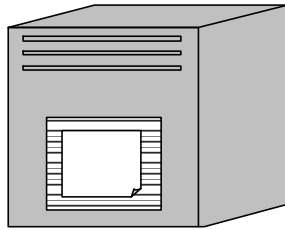
2) 기술적 보안

- (1) 서버(시스템) 보안
- (2) 데이터베이스 보안
- (3) 네트워크 보안
- (4) 응용시스템 보안

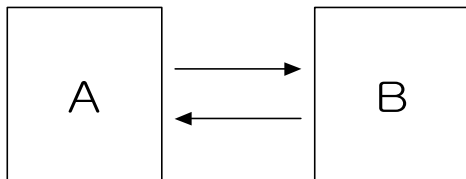
제 1 절 보안이란 무엇인가?



보안서비스



기밀성은 비밀키를 공유하는 사람들만 공유하는 비밀키로, 암호화한 파일을 복호화할 수 있다는 것에 대한 보증이다.



인증은 상대방의 신원에 대한 보증이다. 인증은 제3자가 자신과 교신하는 상대방인 척하는 것을 막는다.



무결성 또는 메시지 인증은 파일이 전송도중에 변경되지 않았다는 것에 대한 보증이다.



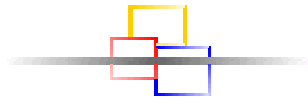
부인 방지는 메시지를 보내는 사람이 파일을 보내지 않고도 파일을 보냈다고 부인할 수 없다는 것에 대한 보증이다. 이것은 비밀키 만으로는 할 수 없다.

[인증에 관한 용어정리]



동익대학교
DONG-EUI UNIVERSITY

제 1 절 보안이란 무엇인가?



보안서비스

1) 신원인증 서비스(Authentication Service)

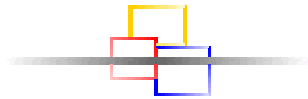
(1) 근접제어(Access Control) 서비스

사용자의 신원인증이 끝나면 인증 받은 그 사용자가 원하는 정보자원 및 전산자원에 접근할 자격이 있는지를 점검하고, 어느 범위 내에서 어떠한 정보 및 전산자원에까지 접근이 가능한지를 허락 받도록 조치하여야 함. 이렇게 함으로써 보안이 필요한 자원에 대해 인가되지 않은 사용자가 접근하는 것을 막을 수 있는데 이를 접근제어 서비스

(2) 데이터 기밀성(Data Confidentiality) 서비스

부당한 데이터의 노출로부터 데이터를 보호하기 위한 것으로 접속 기밀성, 비접속 기밀성, 선별적 필드 기밀성, 전송량 기밀성의 네 가지로 분류할 수 있음

제 1 절 보안이란 무엇인가?



보안서비스

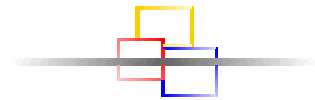
(3) 데이터 무결성(Data Integrity) 서비스

데이터 무결성은 전송 도중 데이터가 변경되거나 위조되지 않았음을 보장하는 서비스

(4) 부인방지(Non-Repudiation) 서비스

데이터 교신 및 전송에 참여한 당사자들이 차후 자신이 행한 행위를 자신이 하지 않았다고 주장할 경우에 대비하기 위하여 만들어진 서비스

제 2 절 암호시스템이란 무엇인가?



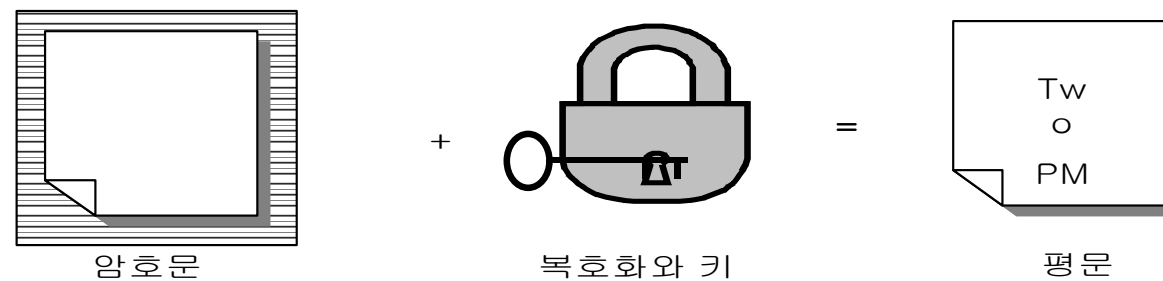
치환법

- 평문에 있는 각각의 문자를 다른 문자로 바꾸는(치환) 방법

암호화

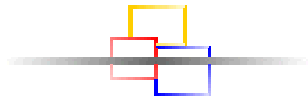


부호화



[암호화와 복호화]

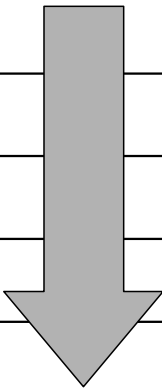
제 2 절 암호시스템이란 무엇인가?



전치법

- 평문에 있는 문자의 위치를 바꾸어 재구성하는 방법

L A S T N I T E W A S H E A V E N P L E A S E M A R R Y M E
L T E L A A E A E R S W V A R T A E S Y N S N E M I H P M E

	L	A	S	T	N	I
	T	E	W	A	S	H
	E	A	V	E	N	P
	L	E	A	S	E	M
	A	R	R	Y	M	E

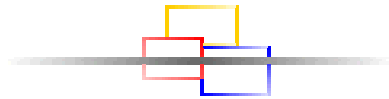
출처: 정재원 외, 보안과 암호화 모든 것, 인포북, 2001

[전치형₉ 암호표]



동의대학교
DONG-EUI UNIVERSITY

제 2 절 암호시스템이란 무엇인가?



DES(Date Encryption Standard)

- 두 가지 방법을 이론적으로 혼합하여 만든 암호화 기법이 바로 DES



암호화 방법

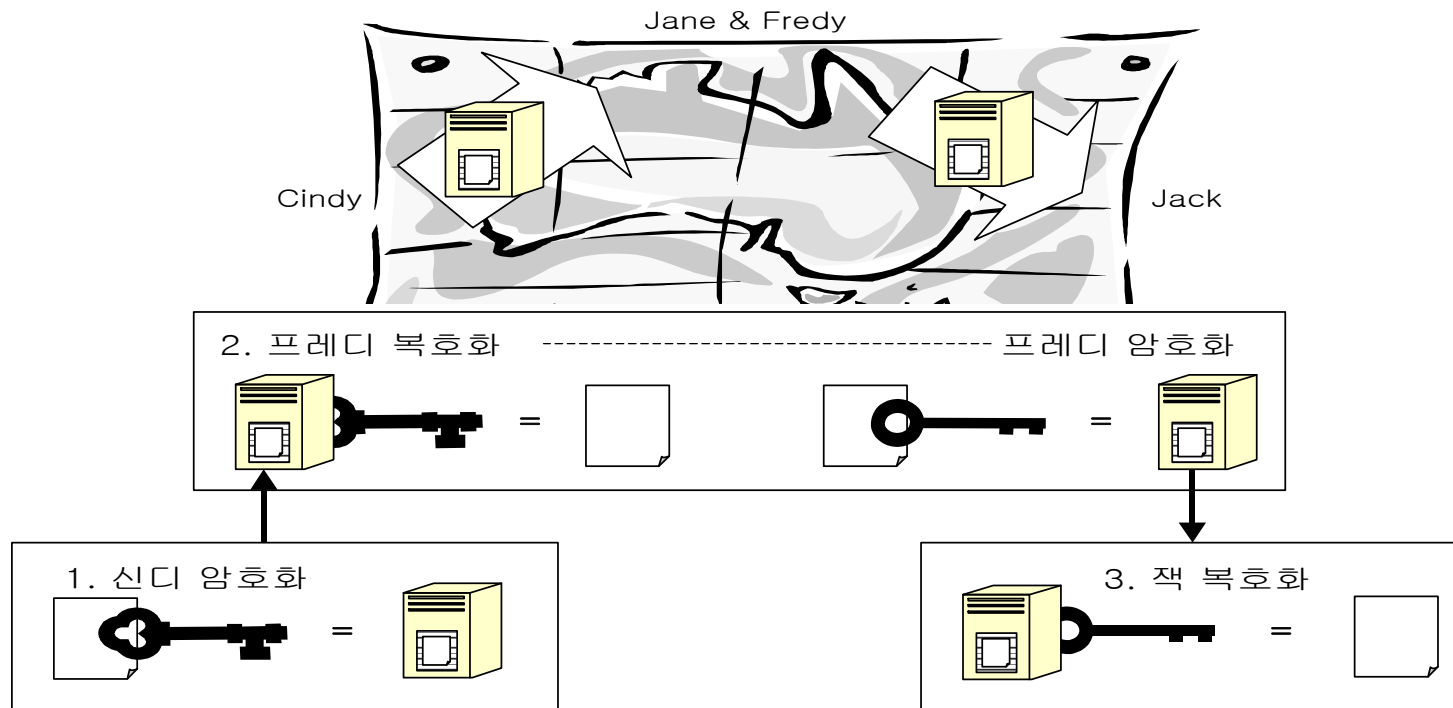
1) 대칭키 방식

암호화 키와 복호화 키가 같거나 하나의 키로부터 다른 하나의 키를 산출해 낼 수 있는 암호화 방식을 대칭키 방식 또는 비밀키 방식

제 2 절 암호시스템이란 무엇인가?



암호화 방법



프레디는 신디와 잭을 위해서 믿을 수 있는 써드파티(Trusted Third Party)이 된다.

[Trusted Third Party의 예]

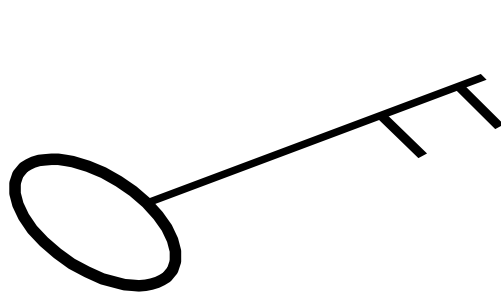
제 2 절 암호시스템이란 무엇인가?



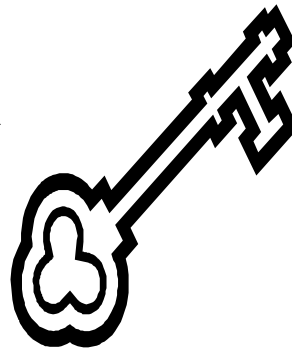
암호화 방법

2) 공개키 암호화 방식

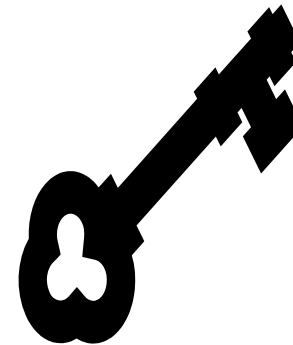
암호화키와 복호화키가 전혀 다르며, 어느 하나로 다른 하나를 추론해내거나 산출해 낼 수 없는 방법



비밀키



공개키

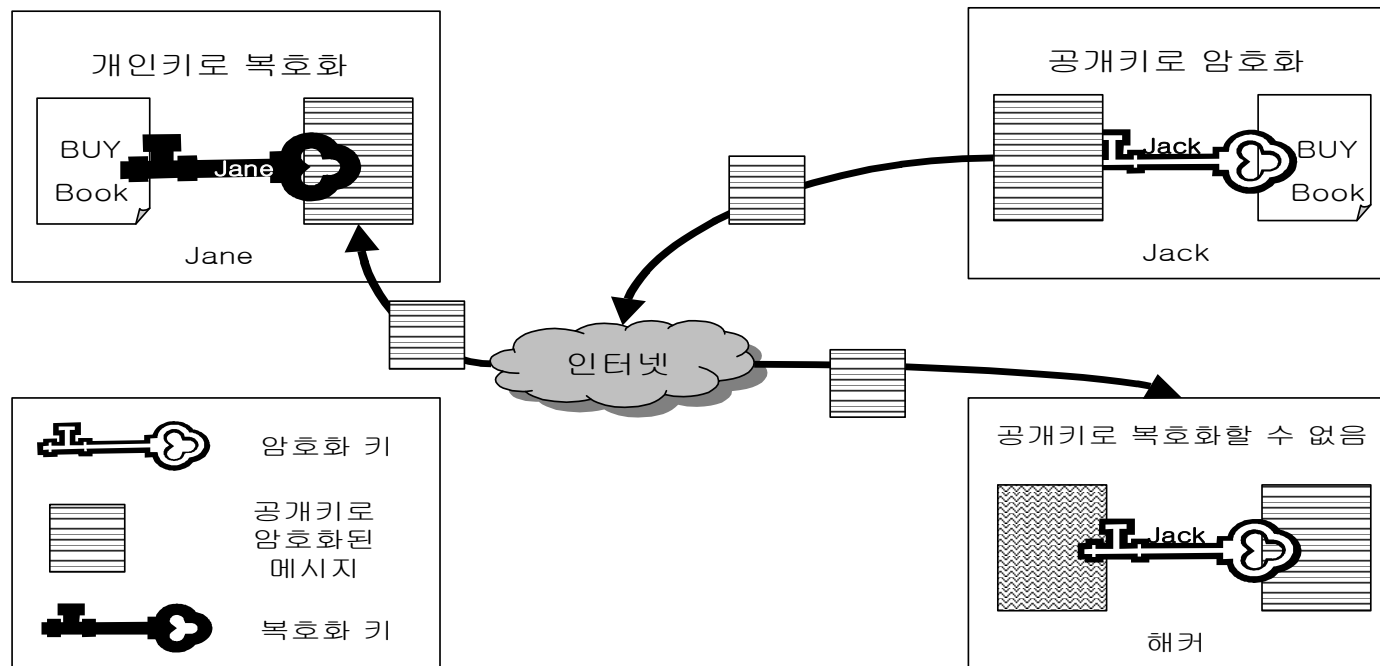


개인키

제 2 절 암호시스템이란 무엇인가?



암호화 방법



잭은 공개키로 암호화한 메시지를 제인에게 보내고, 해커가 이 메시지를 얻어내더라도 원래 메시지를 복수할 수 없다.

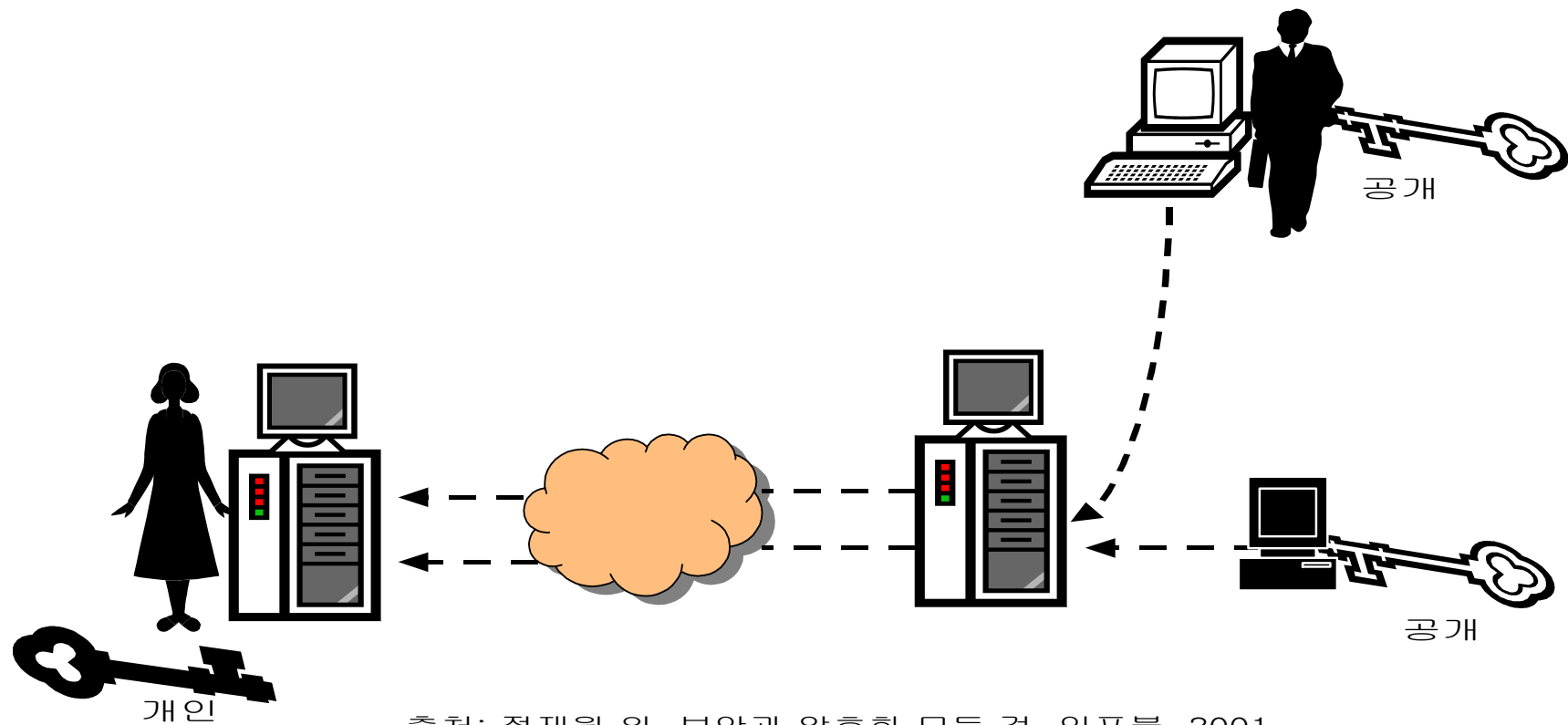
출처: 정재원 외, 보안과 암호화 모든 것, 인포북, 2001

[개인키와 공개키의 활용]

제 2 절 암호시스템이란 무엇인가?



암호화 방법



출처: 정재원 외, 보안과 암호화 모든 것, 인포북, 2001

[공개키 방식을 이용한 암호화와 복호화]



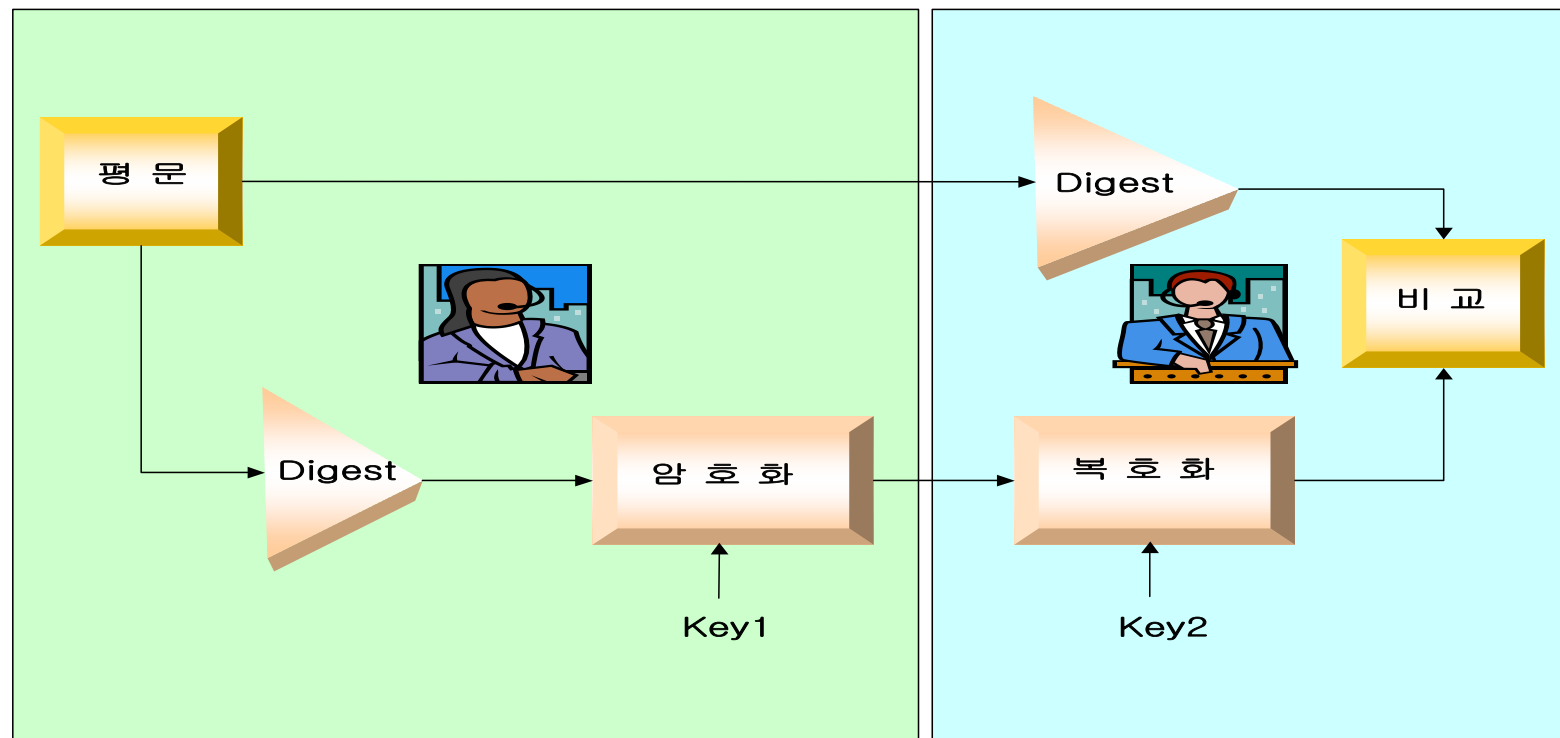
동의대학교
DONG-EUI UNIVERSITY

제 2 절 암호시스템이란 무엇인가?



암호화 방법

3) 메시지 다이제스트



[메시지 다이제스트의 절차]

9-13



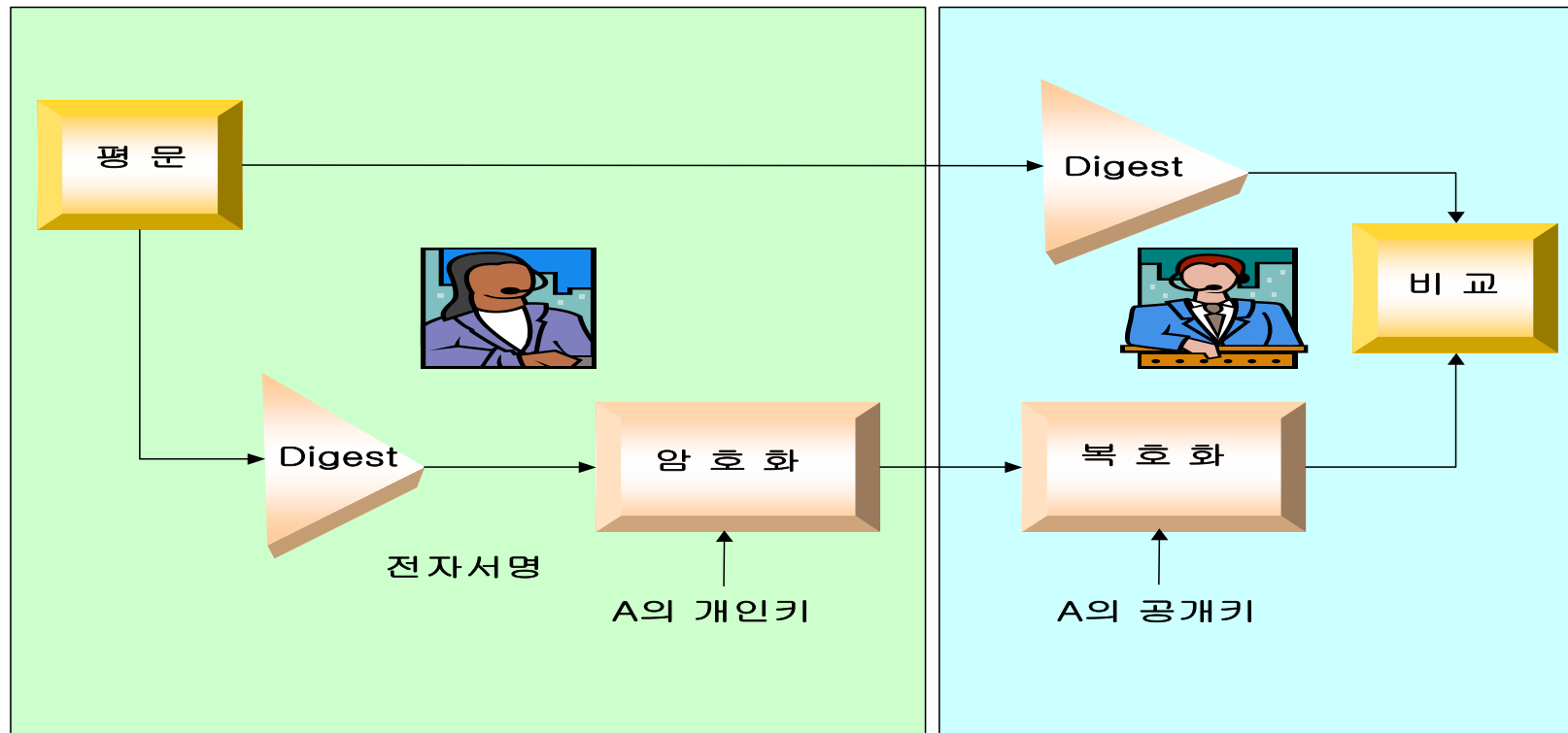
동의대학교
DONG-EUI UNIVERSITY

제 2 절 암호시스템이란 무엇인가?



암호화 방법

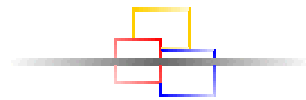
4) 전자서명(Digital Signature)



[전자서명의 내용화 절차]

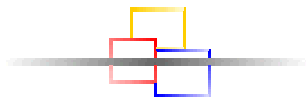


제 3 절 방화벽이란 무엇인가?



방화벽의 개요

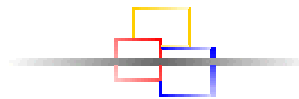
신뢰성 있는 비공개 인트라넷과 신뢰성이 적은 외부에 공개되는 인터넷 사이를 구분할 목적으로 방어의 경계선에 위치한 소프트웨어와 하드웨어로 구성된 시스템



방화벽의 구성요소

스크린 라우터, 베스천 호스트, 프락시 서버

제 3 절 방화벽이란 무엇인가?



방화벽의 구성요소

The screenshot shows the ZoneAlarm Pro interface. The top bar includes 'ZONE LABS', 'INTERNET', 'IN OUT' status, a 'STOP' button, 'INTERNET TRUSTED' status, a lock icon, and 'PROGRAMS'. A green status bar indicates 'All Systems Active'. The left sidebar has navigation links: Overview, Firewall, Program Control, Alerts & Logs (selected), Privacy, and E-mail Protection. The main area is titled 'Alerts & Logs' and contains a table of recent alerts. Below the table is an 'Entry Detail' section for the selected alert.

Alerts & Logs

This is a record of your security activity.

Click an alert in the list, then read details about it in the Entry Detail window.

To get an analysis from AlertAdvisor, click More Info.

To add the traffic source to a Zone, click Add to Zone.

View only the last 50 alerts.

Rating	Date / Time	Type	Protocol
Medium	2004/02/22 22:40:42+9:00 GMT	Firewall	TCP (flags:S)
Medium	2004/02/22 22:40:18+9:00 GMT	Firewall	TCP (flags:S)
Medium	2004/02/22 18:09:00+9:00 GMT	Firewall	TCP (flags:S)
Medium	2004/02/22 18:08:38+9:00 GMT	Firewall	TCP (flags:S)
Medium	2004/02/22 17:39:28+9:00 GMT	Firewall	TCP (flags:S)
Medium	2004/02/22 17:05:18+9:00 GMT	Firewall	TCP (flags:S)
Medium	2004/02/22 17:05:14+9:00 GMT	Firewall	TCP (flags:S)
Medium	2004/02/22 16:24:50+9:00 GMT	Firewall	TCP (flags:S)

Entry Detail

Description	Packet sent from 220.82.42.136 (TCP Port 4...)
Direction	Incoming
Type	Firewall
Source DNS	

Buttons: Add to Zone >>, More Info

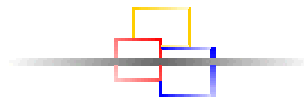
Buttons: Hide Text, Clear List

[개인 방화벽 프로그램의 사례]



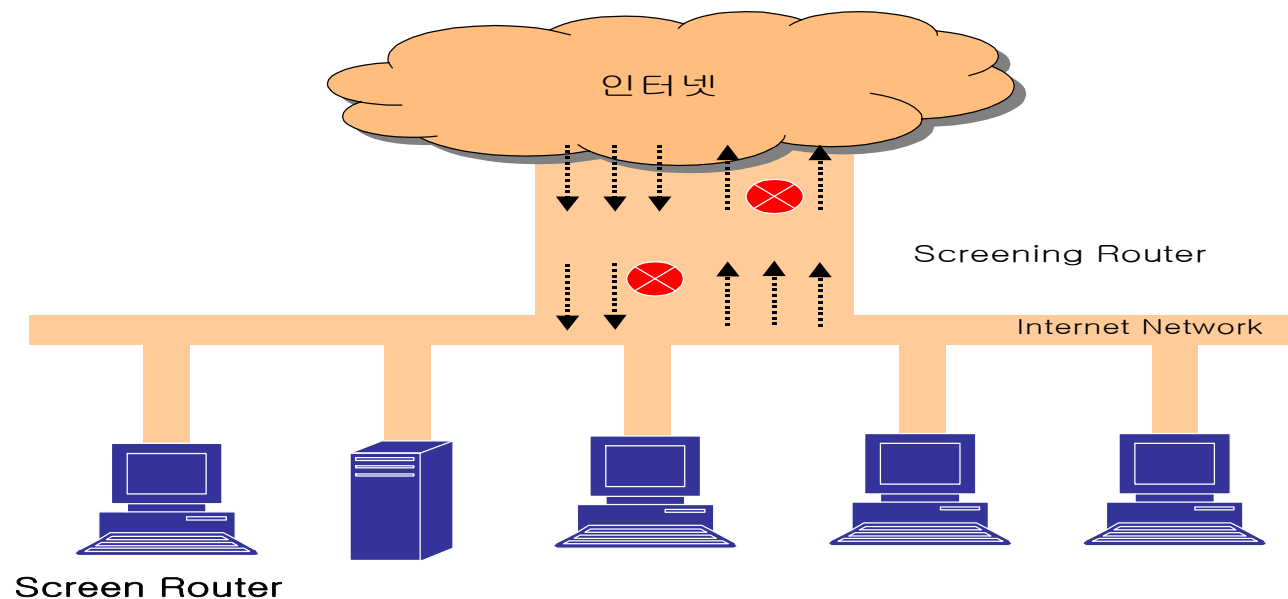
동익대학교
DONG-EUI UNIVERSITY

제 3 절 방화벽이란 무엇인가? ㄸ



방화벽의 구성요소

1) 스크린 라우터(Screen Router)



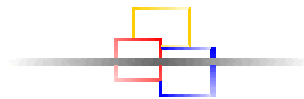
출처: 홍승필 외, e-Business Security, 파워북, 2000

[스크린 라우터의 기능]

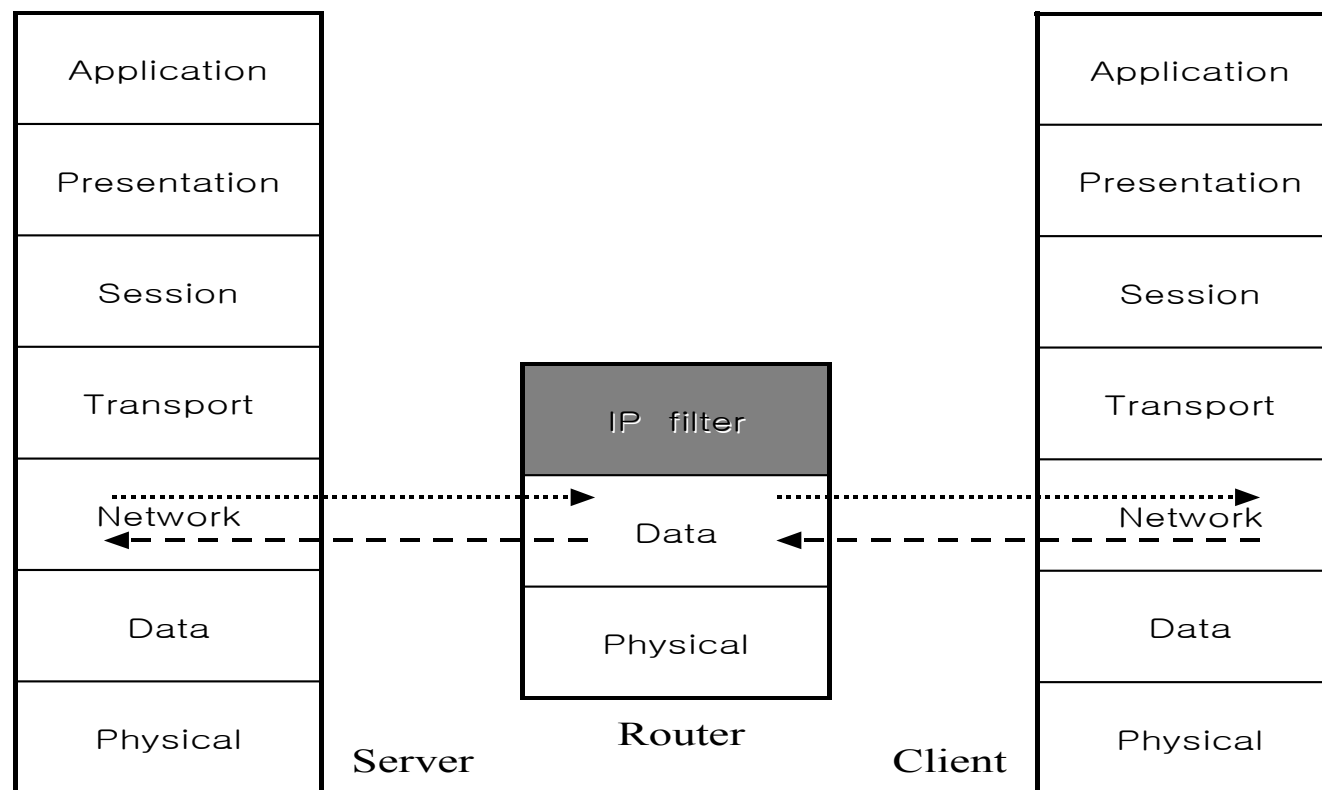


동익대학교
DONG-EUI UNIVERSITY

제 3 절 방화벽이란 무엇인가? ㅍ



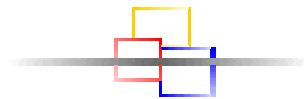
방화벽의 구성요소



[네트워크 수준의 패킷 필터링]

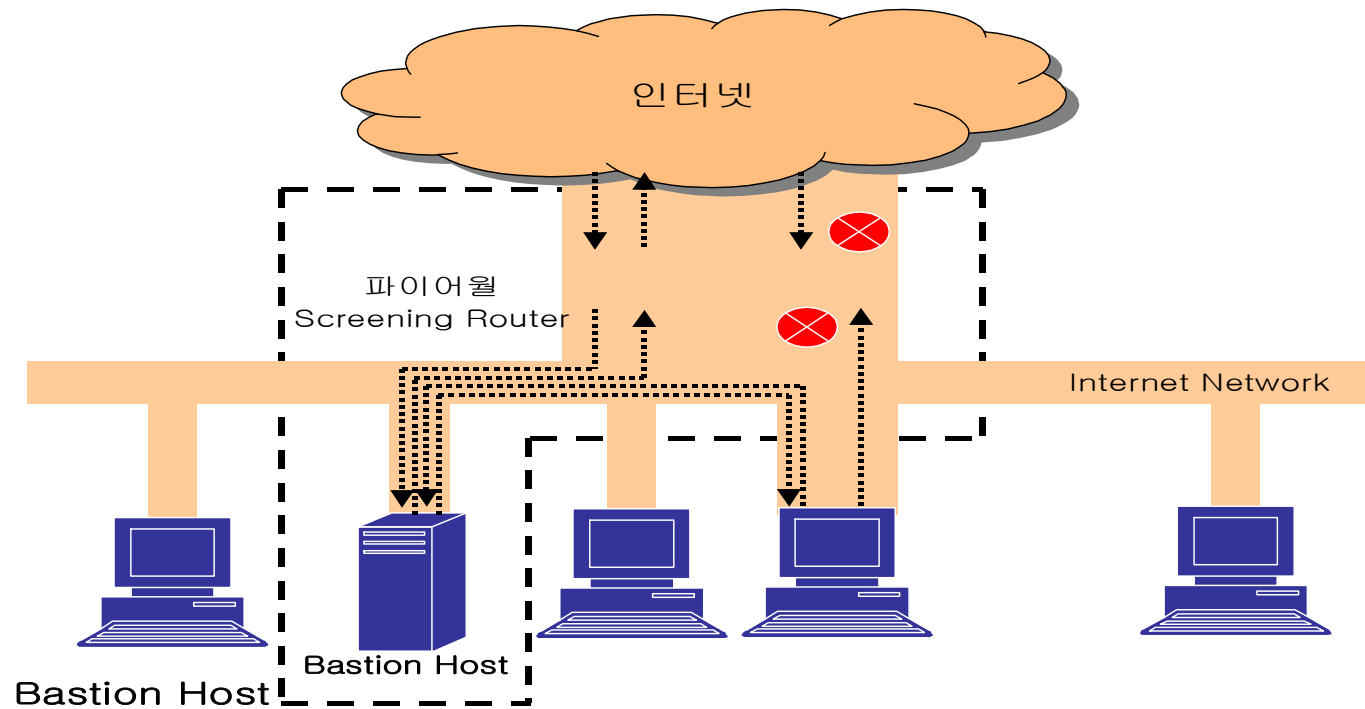


제 3 절 방화벽이란 무엇인가?



방화벽의 구성요소

2) 배스천 호스트(Bastion Host)



출처: 홍승필 외, e-Business Security, 파워북, 2000

[배스천 호스트의 기능]



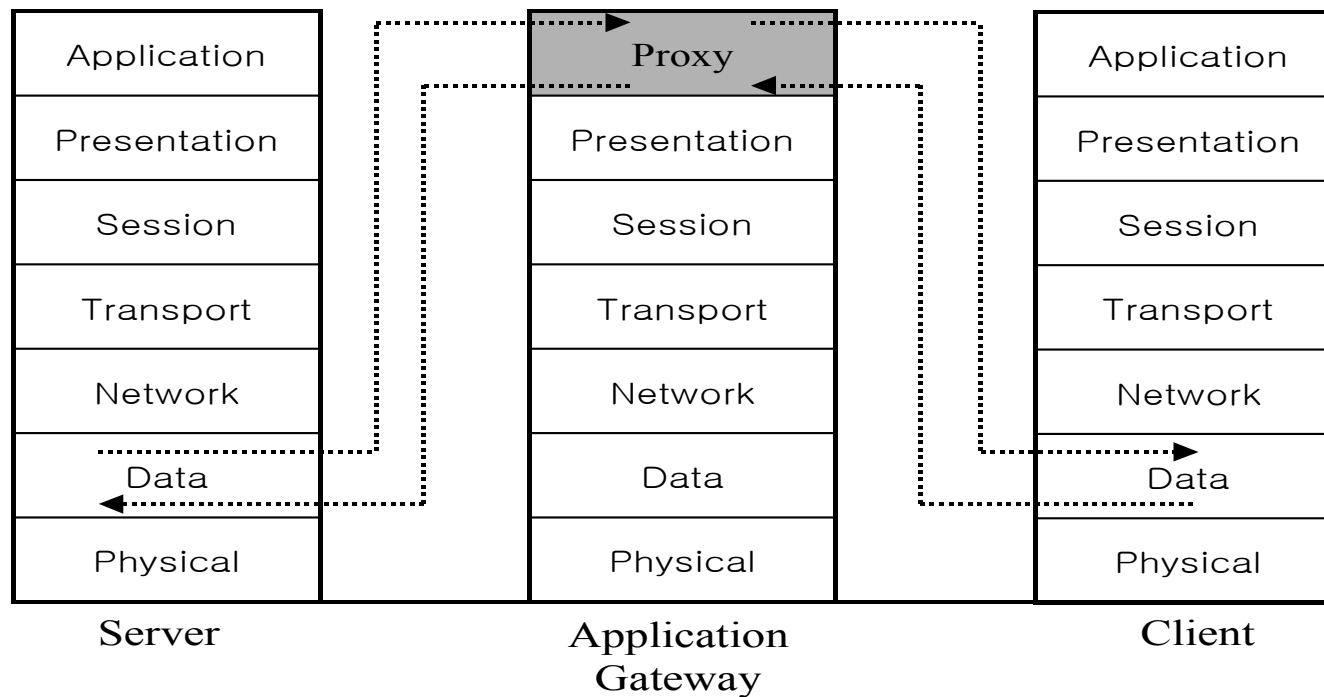
동익대학교
DONG-EUI UNIVERSITY

제 3 절 방화벽이란 무엇인가?



방화벽의 구성요소

3) 프락시 서버(Proxy Server)



[프락시 서버를 통한 애플리케이션 수준의 보안]



제 3 절 방화벽이란 무엇인가?



방화벽의 기능

1) 내 · 외부 접근 제어(Access Control)

2) 인증(Authentication)

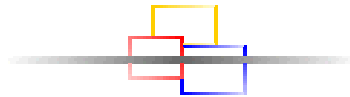
사용자가 인가된 사용자인지를 확인해주는 서비스

3) 가상사설망(Virtual Private Network)을 위한 데이터 암호화

가장 대중적인 네트워크인 인터넷을 사용하여 멀리 떨어져 있는 협력업체나

지점들과 연결하면서도 개인 사설망을 사용하는 것만큼 보안상 안전한 네트워크

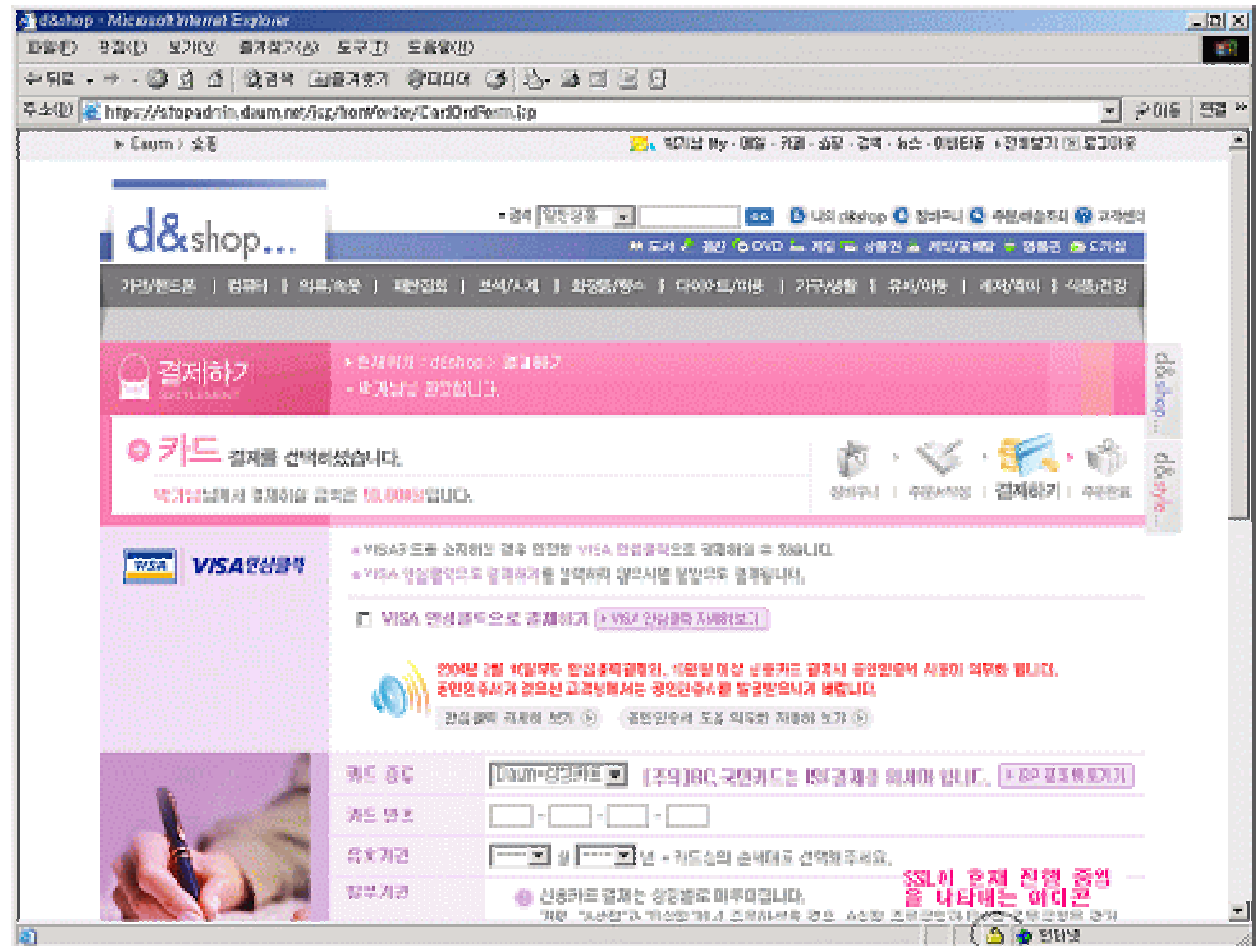
제 4 절 인터넷 보안



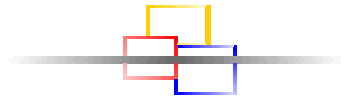
SSL(Secure Socket Layer)

1) SSL의 개념

인터넷에서 신용카드를
사용하게 되면 여러분이 반드시
접하게 되는 서비스가 바로
SSL서비스



제 4 절 인터넷 보안



SSL(Secure Socket Layer)

- 2) SSL의 역사
- 3) SSL 세션의 개요

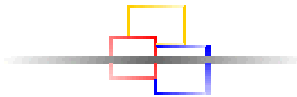


출처: 정재원 외, 보안과 암호화 모든 것, 인포북, 2001

[SSL의 인증 및 비밀키 교환절차]



학교
DONG-EUI UNIVERSITY



웹 브라우저의 보안

1) 웹 브라우저의 보안상 문제점

- (1) 웹 브라우저 설계 및 개발상의 문제점
- (2) 웹상의 자원과 연결되는 프로그램의 보안문제
 - 웹 기반의 언어의 버그를 이용한 공격
 - 사회 공학적 공격(Social Engineering Attack)

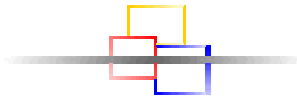
2) 자바 스크립트상의 문제점

- (1) 자바 스크립트의 보안문제
 - 자바 스크립트를 통한 개인정보의 누출
 - 서비스 거부 공격(Denial of Service Attack)



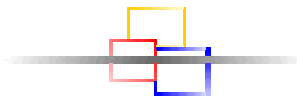
침입탐지 시스템(Intrusion Detection System)

각종 침입 행위들을 자동적으로 탐지하고, 대응조치를 취하며, 사후적으로 보고하는 보안시스템으로 정의할 수 있다. 이러한 침입탐지시스템은 크게 네트워크 기반의 침입탐지 시스템과 호스트 기반의 침입탐지 시스템



서버 보안의 개요

- 첫째는 웹 서버의 보안
- 두 번째는 운영체제의 보안임



웹 서버 보안의 문제점

- 1) 정책(Policy)
- 2) 보안 관련 도구
 - (1) 스냅샷 도구(Snapshot tool)
 - (2) 시스템 변경검사 도구
 - (3) 네트워크 스캐닝(scanning) 도구
 - (4) 침입탐지 프로그램
 - (5) 프로그램상의 오류
 - (6) 로깅(Logging)
 - (7) 백업