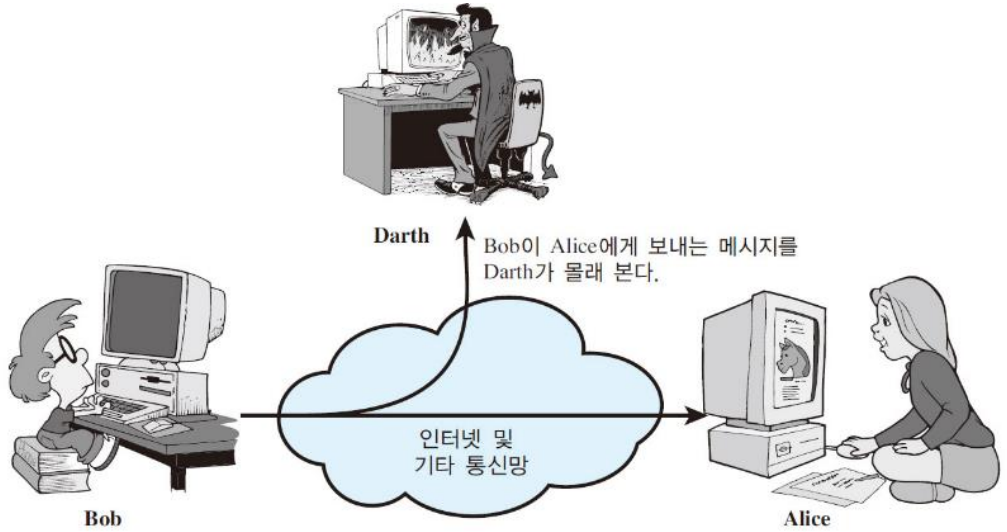
컴퓨터 네트워크

[15주차] 네트워크 보안

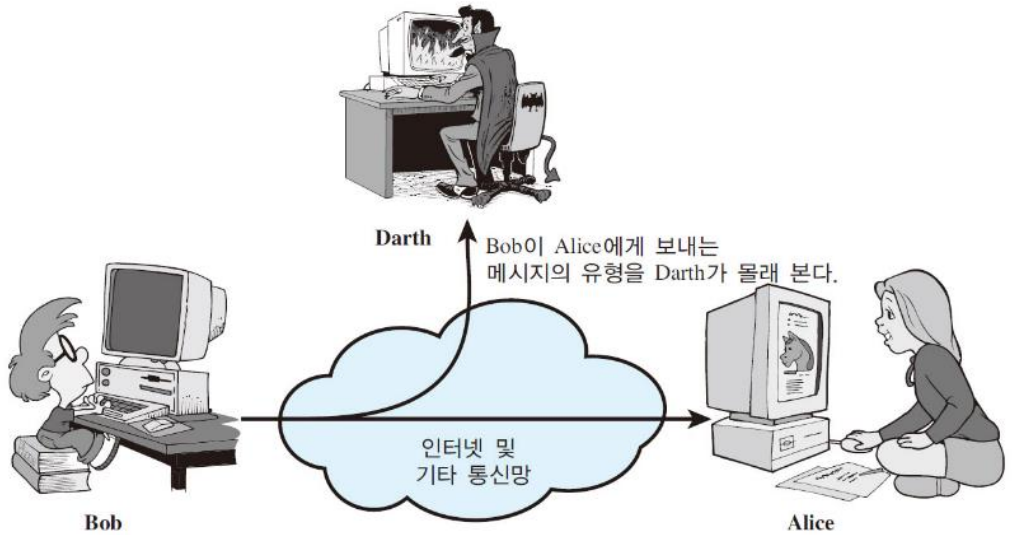
2018. 12. 11. 화요일

1. 보안 공격

- 보안 공격의 종류
  - 소극적 공격
    - 시스템으로부터 정보를 획득하거나 사용하려는 시도로, 시스템 자원에 영향을 끼지지 않는 공격 형태
    - 전송 정보에 대한 도청이나 감시를 의미하며, 전송 중인 정보를 취득하는 것이 목적



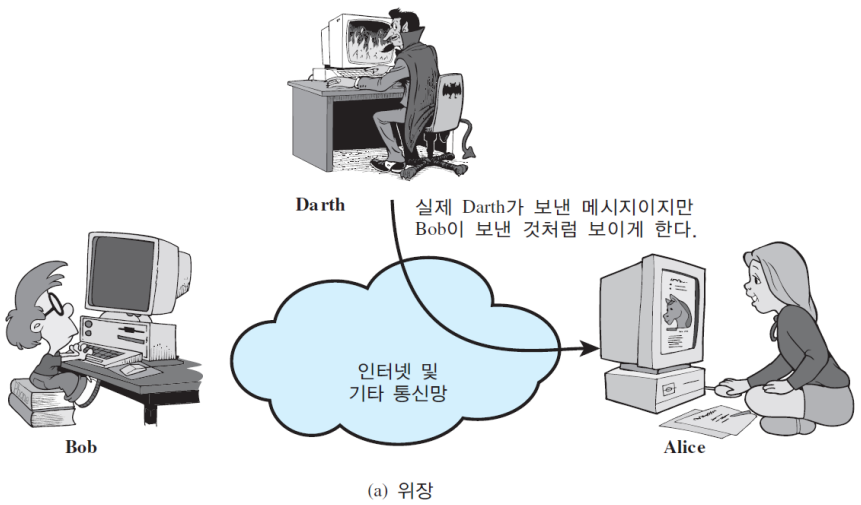
(a) 메시지내용 갈취



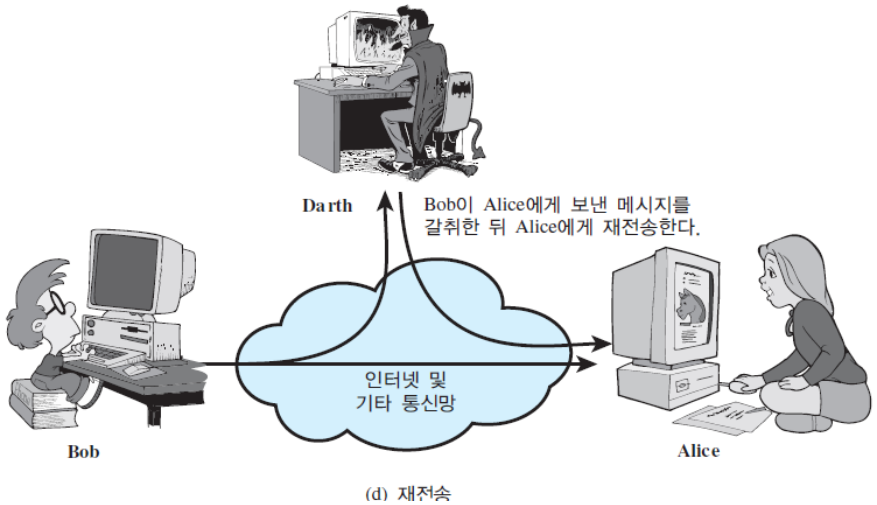
(b) 트래픽 분석

  - 적극적 공격
    - 시스템 자원을 변경하거나 시스템의 작동에 영향을 끼치는 공격 형태
    - 데이터 스트림을 수정하거나 가짜 데이터 스트림을 만드는 행위

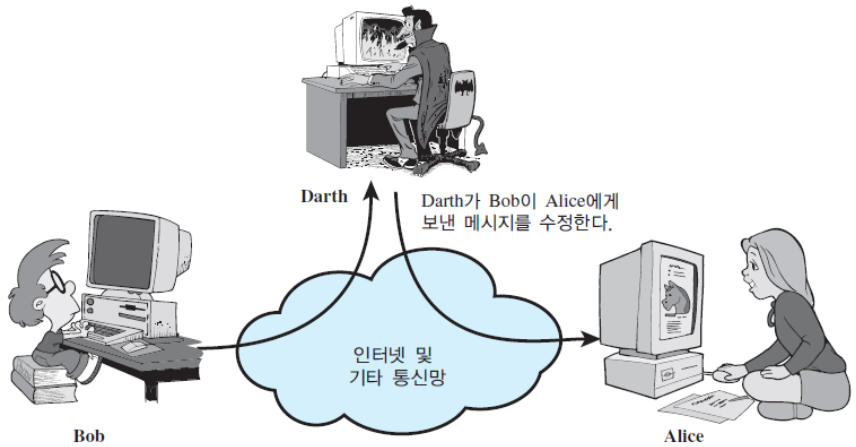
1. 보안 공격



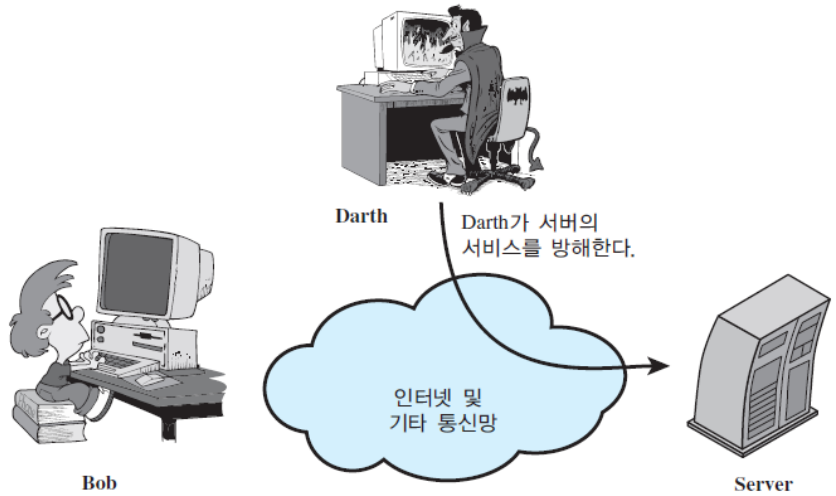
(a) 위장



(d) 재전송



(C) 메시지 수정



(d) 서비스의 거부

1. 보안 서비스

- 시스템의 적절한 보안이나 데이터 전송의 보안을 보장하는 통신 개방 시스템의 프로토콜 계층에서 제공되는 서비스
- 시스템 자원 보호를 위해 시스템이 제공하는 처리 서비스나 통신 서비스
- 보안 정책을 구현하고, 보안 메커니즘에 의해 구현

- 인증(Authentication)
  - 통신 개체가 주장하는 것처럼 정말 그 당사자인지를 확인
  - 대등 개체 인증(Peer Entity Authentication)
    - 연결하고 있는 개체의 신분에 대한 확신을 주기 위해서 논리적 연결에서 사용하는 인증
  - 데이터 출처 인증(Data Origin Authentication)
    - 비연결 전송에서 수신된 데이터의 출처가 정말 주장하고 있는 곳에서 온 것인지 확인시켜주는 인증

- 접근제어(Access Control)
  - 자원을 불법적으로 사용하지 못하도록 방지하는 것
  - 누가, 어떤 조건하에, 어떤 자원을 사용하도록 하는지 등 자원에 대한 접근을 제한

2. 보안 서비스

- 데이터 기밀성(Data Confidentiality)
  - 연결 기밀성(Connection Confidentiality)
    - 연결시 모든 사용자 데이터에 대한 보호
  - 비연결 기밀성(Connectionless Confidentiality)
    - 단일 데이터 블록 안의 모든 사용자 데이터에 대한 보호
  - 선별된 필드 기밀성(Selective field Confidentiality)
    - 연결이나 단일 데이터 블록의 사용자 데이터 안의 선별된 필드에 대한 보호
  - 트래픽 플로우 기밀성(Traffic Flow Confidentiality)
    - 트래픽 플로우를 관찰하여 정보를 가로채려는 경우에 대한 보호

- 데이터 무결성(Data Integrity)
  - 수신된 데이터가 인증된 개체가 보낸 것과 정확히 일치하는지에 대한 확신
  - 수정, 추가, 제거, 혹은 재전송이 없음을 확인
  - 복구 가능 연결 무결성(Connection Integrity with Recovery)
    - 연결시 사용자 데이터의 무결성을 제공
    - 데이터를 복구할 때 전체적인 데이터 열 안의 모든 데이터에 대한 수정, 추가, 제거, 혹은 재전송이 있었는지를 감지

2. 보안 서비스

- 복구 없는 연결 무결성(connection Integrity without Recovery)
  - 위와 동일하나 복구하지 않고 탐지
- 선별된 필드 연결 무결성(Selective Field Connection Integrity)
  - 연결시 전송되는 데이터 블록의 사용자 데이터 안의 선별된 필드들의 무결성을 제공
  - 선별된 필드의 수정, 추가, 제거, 재전송이 있었는지를 판단할 수 있는 형태를 취함
- 비연결 무결성(Connectionless Integrity)
  - 단일 비연결 데이터 블록의 무결성을 제공, 데이터의 수정을 탐재할 수 있는 형태를 취할 수 있음
  - 재전송 탐지를 위한 제한적 형태를 취할 수 있음
- 선별된 필드 비연결 무결성(Selective Field Connectionless Integrity)
  - 단일 비연결 데이터 블록안의 선별된 필드들에 대한 무결성을 제공
  - 선별된 필드의 수정이 있었는지를 판단할 수 있는 형태를 취함

- 부인봉쇄(Nonrepudiation)
  - 통신의 한 주체가 통신에 참여했던 사실을 일부 혹은 전부를 부인하는 것을 방지
  - 부인봉쇄, 출처(Nonrepudiation, Origin)
    - 메시지가 특정 출처에서 보내졌음을 증명
  - 부인봉쇄, 목적지(Nonrepudiation, Destination)
    - 특정 개체가 메시지를 수신했음을 증명

2. 보안 서비스

- 가용성 서비스
  - 인가된 시스템이 자원에 접근할 필요가 있거나 사용하고자 할 때 시스템의 성능에 따라 시스템 자원에 접근할 수 있도록 하는 것
  - 다양한 형태의 공격에 의해서 가용성이 줄어들거나 가용성에 손실이 발생
  - 다양한 보안 서비스와 연관된 자원으로 간주
  - 시스템의 가용성을 보장하기 위해 시스템을 보호하는 서비스로, 서비스거부 공격 때문에 제기 되는 보안 문제에 역점을 두고 있음

3. 보안 메커니즘

- 특정 보안 메커니즘(Specific Security Mechanisms)
  - 통신 개체가 주장하는 것처럼 정말로 그 당사자인지를 확인
  - 암호화(Encipherment)
    - 데이터를 읽을 수 없는 형태로 변환하는 데 수학적 알고리즘을 사용
    - 데이터를 변환하고 다시 복구하는 것은 알고리즘과 사용되는 키들에 따라 달라짐
  - 디지털 서명(Digital Signature)
    - 데이터 수신자가 데이터의 발신자와 무결성을 입증하고 위조를 막도록 데이터에 붙이는 데이터나 데이터 단위의 암호적 변경을 말함
  - 접근제어
    - 자원에 접근할 권한을 제한하는 다양한 메커니즘
  - 데이터 무결성
    - 데이터 단위나 데이터 단위들의 스트림의 무결성을 확신하는데 사용
  - 인증 교환(Authentication Exchange)
    - 정보교환을 통해 개체의 신원을 확인하는데 사용하는 메커니즘
  - 트래픽 패딩(Traffic Padding)
    - 트래픽 분석 시도를 방해하기 위해서 데이터 스트림 안의 빈 곳에 비트를 채워넣는 것

3. 보안 메커니즘

- 경로 제어(Routing Control)
  - 특정 데이터에 대해 물리적으로 안전한 경로를 선택하고 보안 침해가 의심스러운 경우 경로를 변경
- 공증(Notarization)
  - 데이터 교환의 어떤 성질을 확신하기 위해 신뢰받는 제 3자를 이용

- 일반 보안 메커니즘(Pervasive Security Mechanisms)
  - 임의의 특정 OSI 보안 서비스나 프로토콜 계층에 구애받지 않는 메커니즘
  - 신뢰받는 기능(Trusted Funcionality)
    - 어떤 기준(보안정책에 의해 형성되는)으로 볼때 올바른 것으로 여겨지는 것
  - 보안 레이블(Security Label)
    - 자원(데이터 단위)의 보안 속성에 이름을 붙이거나 자원의 보안속성을 지정하는 그 자원에 대한 표시
  - 사건 탐지(Event Detection)
    - 보안 관련 사건에 대한 탐지
  - 보안 감사 추적(Security Audit Trail)
    - 보안 감사를 하기 위해 수집하거나 이용되는 데이터로서 시스템 기록과 동작을 독립적으로 조사하고 검토하는 것
  - 보안 복구(Security Recovery)
    - 사건 처리와 관리 기능 같은 메커니즘의 요구사항을 다루고 복구 동작을 수행

3. 보안 메커니즘

- 보안 서비스와 메커니즘과의 관계

서비스	메커니즘							
	암호화	디지털서명	접근제어	데이터 무결성	인증 교환	트래픽 패딩	라우팅 제어	공증
대등 개체인증	Y	Y			Y			
데이터 출처인증	Y	Y						
접근제어			Y					
기밀성	Y						Y	
트래픽 흐름 기밀성	Y					Y	Y	
데이터 무결성	Y	Y		Y				
부인봉쇄		Y		Y				Y
가용성				Y	Y			

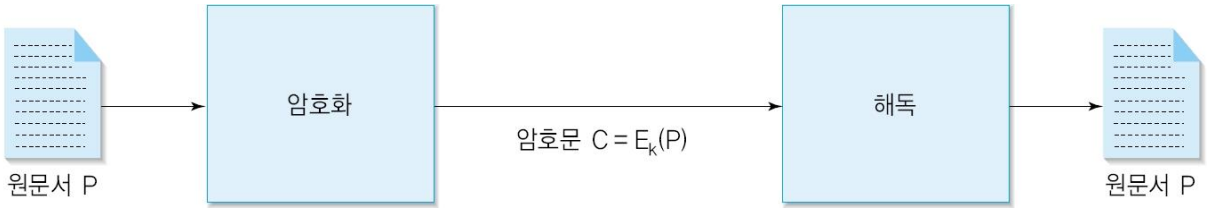
4. 암호화의 이해

- 암호화
  - 문서의 내용을 암호화(Encryption)하여 전송함으로써, 외부 침입자로부터 문서를 보하는 방법은 컴퓨터 네트워크가 보급되기 전부터 사용하던 방식
  - 문서의 송수신자는 암호문을 작성하고 해석하는 과정에서 자신들만 아는 비밀키를 사용
  - 컴퓨터 보안은 일반인도 중요성을 인식하는 분야지만, 네트워크에서는 이론적으로 간단하지 않은 분야에 속함

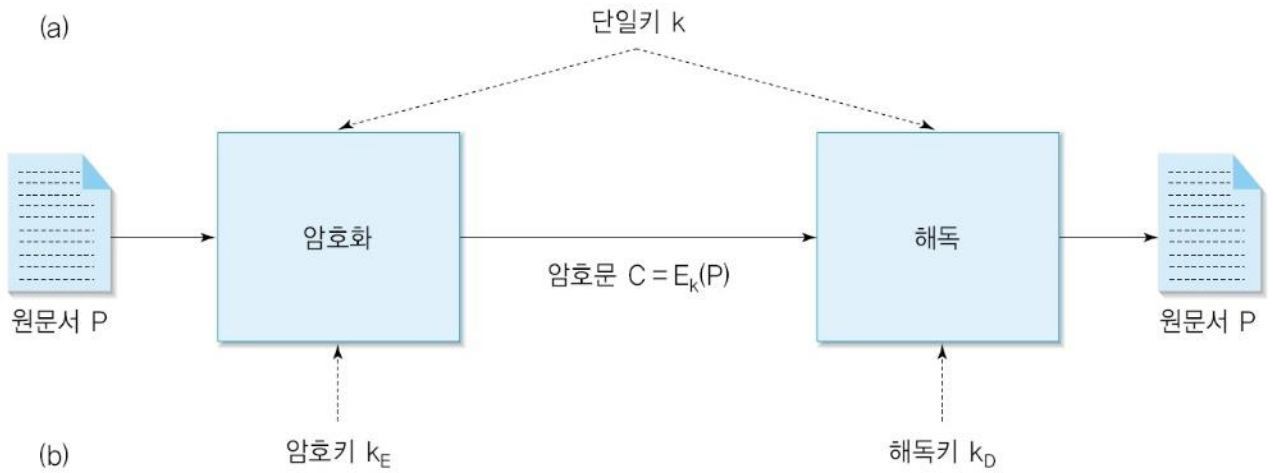
- 외부침입자가 전송 메시지에 가하는 위해(危害) 행동
  - 메시지 읽기
    - 전송선로를 흐르는 신호를 도청하여 메시지의 내용을 읽음
    - 인터넷에서는 신호 도청을 차단하기 쉽지 않아 암호화 기법으로 해결
  - 전송 방해
    - 전송 메시지가 수신자에게 도착하지 못하게 함으로써, 송수신자 간의 통신을 방해
    - 인터넷에서 방화벽 기능을 통해 불법 사이트에 접속하지 못하도록 차단하는 것 등
  - 메시지 수정
    - 전송되는 메시지의 내용을 수정하는 것
    - 송수신자가 교환하는 메시지의 의미를 왜곡

4. 암호화의 이해

- 암호화 용어
  - 원문서(Plaintext): 암호화 전의 원본 문서
  - 암호문(Ciphertext): 원문서를 임의의 형태로 암호화 한 문서
  - 암호화(Encryption)
    - 메시지의 내용을 변형, 원래의 의미를 알아볼 수 없도록 변형하는 작업
    - 송수신자만 해독할 수 있는 표현방식을 사용해 침입자가 메시지 내용을 알아볼 수 없도록 전송하는 것
  - 해독(Decryption): 암호화된 문서를 원래 언어로 변형



- 암호화 알고리즘
  - 암호화와 해독 과정에서는 키(Key)를 사용



4. 암호화의 이해

- 대체 암호화
  - 특정 문자를 다른 문자로 1:1 대응하는 방식
  - 시저 암호화
    - 알파벳 문자를 순차적으로 세 문자씩 오른쪽으로 이동
    - 암호키

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

    - 예

N	E	T	W	O	R	K		T	E	C	H	N	O	L	O	G	Y
q	h	w	z	r	u	n		w	h	f	k	q	r	o	r	j	b

  - 키워드 암호화
    - 지정된 키워드 문자를 먼저 적고, 나머지 문자를 알파벳 순으로 기술
    - 암호키: seoul

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	s	e	o	u	l	a	b	c	d	f	g	h	i	j	k	m	n	p	q	r	t	v	w	x	y	z

키워드 — s, e, o, u, l을 제외한 문자를 알파벳 순서로 배치

4. 암호화의 이해

- 복수 개의 문자표
  - 둘 이상의 문자표를 사용

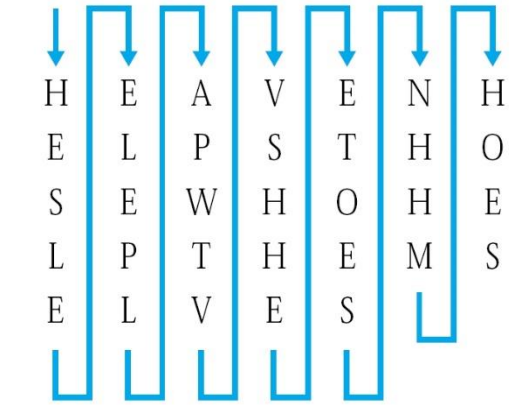
홀수 위치에 있는 문자

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c

짝수 위치에 있는 문자

원문	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
암호문	s	e	o	u	l	a	b	c	d	f	g	h	i	j	k	m	n	p	q	r	t	v	w	x	y	z

- 위치 암호화
  - 컬럼 암호화(Colum Cipher)
    - 원문: HEAVEN HELPS THOSE WHO HELP THEMSELVES
    - 암호문1: HESLE ELEPL APHTV VSHHE ETOES NHHM HOES
    - 암호문2: HESLE ELEPL APHTV VSHHE ETOES NHHMZ HOESZ
  - 키워드 암호화
    - 임의의 단어를 이용하여 컬럼의 순서를 결정
    - 원문: HEAVEN HELPS THOSE WHO HELP THEMSELVES
    - 키워드: NETWORK
    - 암호문: ELEPL HOESZ HESLE ETOES NHHMZ APWTV VSHHE



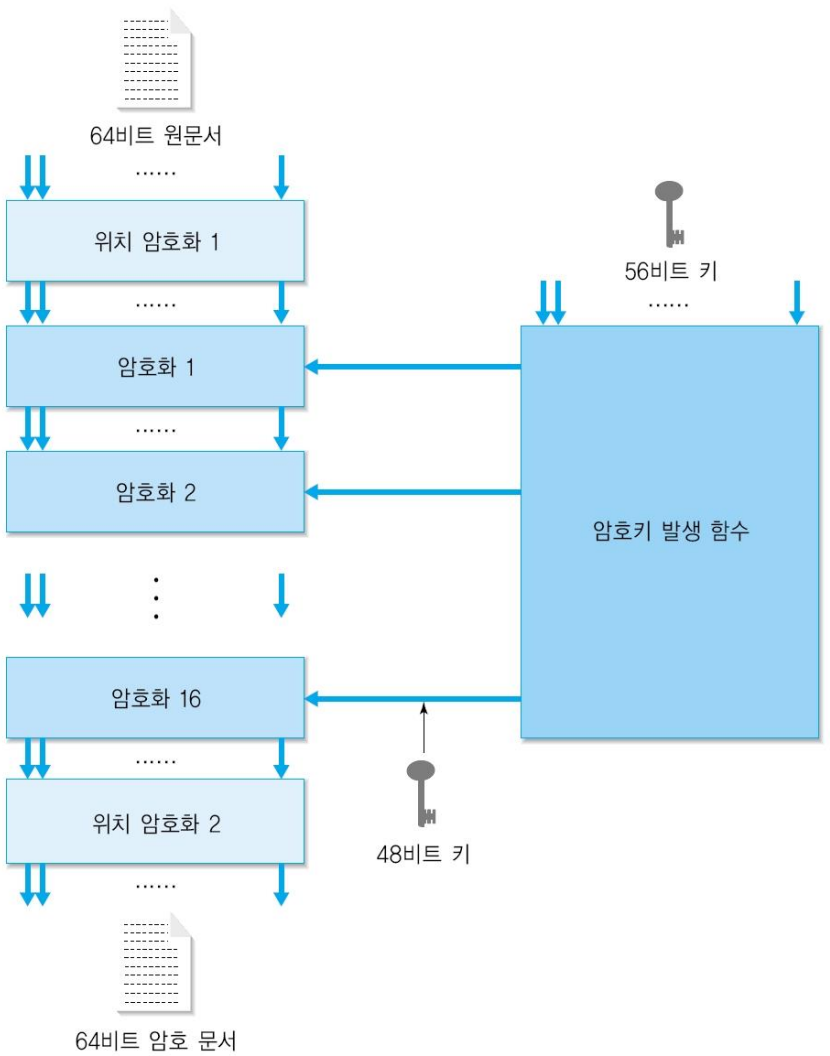
키워드	N	E	T	W	O	R	K
순서	3	1	6	7	4	5	2
	H	E	A	V	E	N	H
	E	L	P	S	T	H	O
	S	E	W	H	O	H	E
	L	P	T	H	E	M	S
	E	L	V	E	S	Z	Z

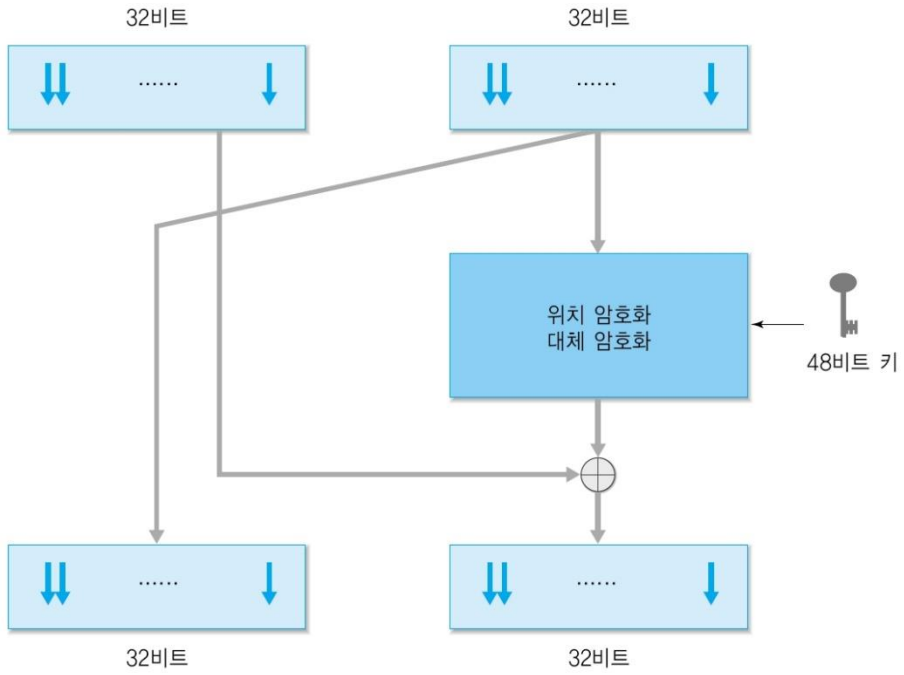
5. 암호화 시스템

- DES 알고리즘(Data Encryption Standard)
  - 암호문을 작성할 때와 해독할 때 사용하는 암호키가 같음
  - 절대로 외부에 유출되지 않도록 관리해야 하기 때문에 비밀키(Secret Key)라고도 부름
  - 양쪽이 동일 키를 사용해 대칭키(Symmetric Key)로도 부름
  - 외부 사용자에게 노출되지 않아야 하는 암호키로 암호화 하는 알고리즘을 비공개키 알고리즘이라 함
  - 미국 정부가 개발하여 여러 하드웨어와 소프트웨어에 사용
  - 암호화를 64비트 단위로 수행, 암호키의 크기는 56비트
  - 동작방식
    - 64비트인 데이터 블록을 32비트씩 나누어 독립적으로 처리
    - 16단계의 암호화 과정과 2단계의 위치 암호화 과정을 수행

5. 암호화 시스템

- DES 알고리즘 동작과정과 16단계 암호화



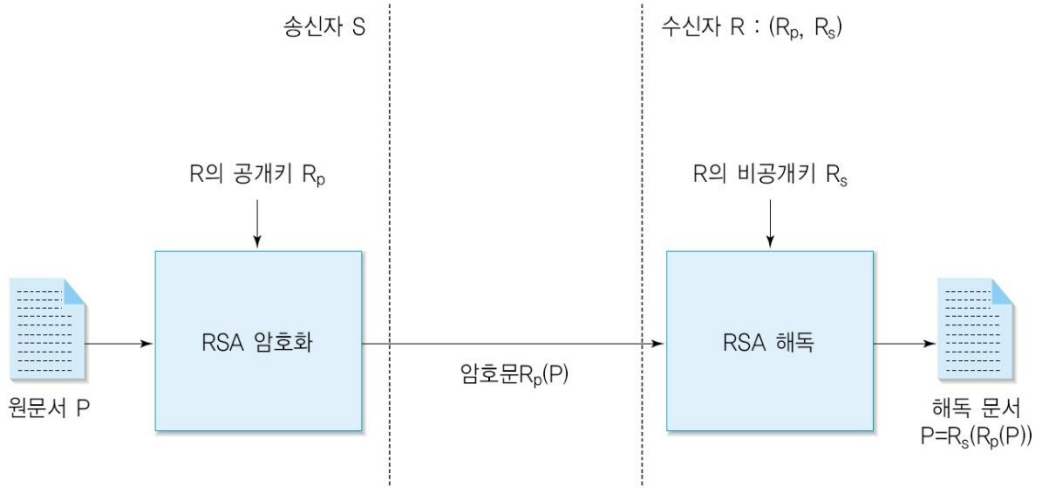


[그림 13-4] [그림 13-3]의 16단계 암호화 알고리즘

5. 암호화 시스템

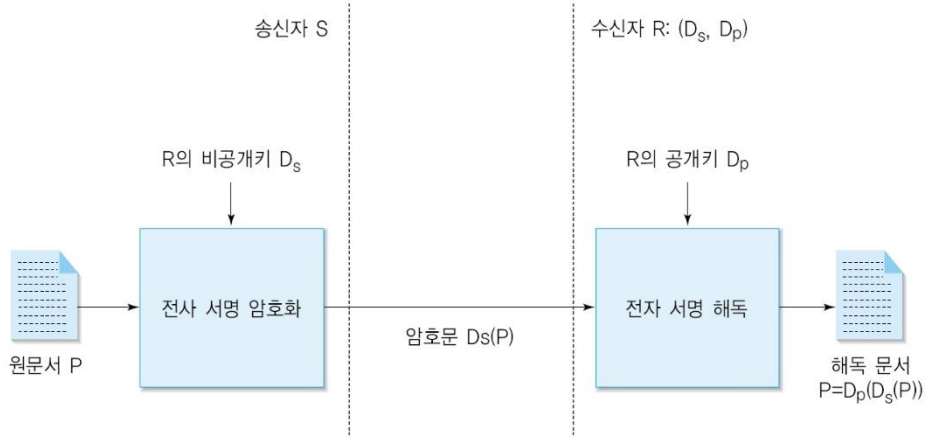
- 공개키 알고리즘
  - 암호화하는 키와 해독하는 키가 동일하지 않도록 고안된 방식
  - 암호문을 작성할 때 사용하는 암호키가 외부에 공개되어도 해독키를 모르면 암호문 해독이 불가능
  - 공개키(Public Key)
    - 원문서를 암호화하는데 사용하므로 원칙적으로 누구에게나 공개
    - 따라서 송신자는 공개키로 원문서를 암호화 하여 전송
  - 비공개키(Private Key)
    - 수신자가 암호문을 해독하기 위해 사용, 공개키와 다른 값을 갖음

  - RSA 알고리즘
    - 알고리즘 발명자인 Rivest, Shamir, Adelman의 첫 글자
    - 공개키와 비공개키 조합을 발생시키는 방법을 제시

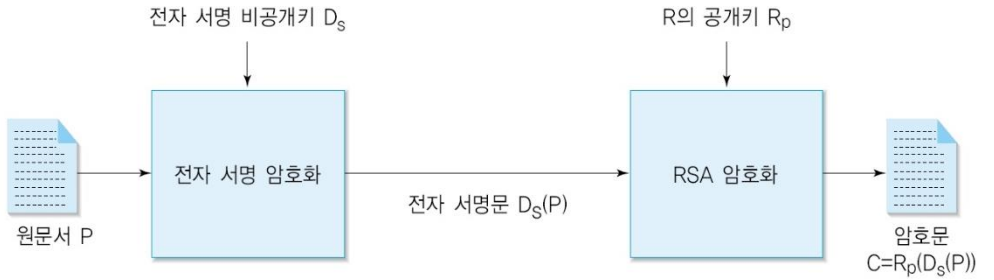


5. 암호화 시스템

- 전자서명
  - 인터넷 환경에서 특정 사용자를 인증하는 목적으로 사용
  - 특정인이 진짜 그 사람인지를 확인하는 절차
  - RSA 알고리즘과 반대 원리로 동작
    - 비공개키: 원문서의 암호화 용도(특정인만 암호화 과정 수행)
    - 공개키: 암호문 해독 용도(모든 사람이 해독 과정 수행)



  - 암호화 과정
    - 1단계: 전자서명 알고리즘으로 인증 정보를 암호화 (사용자 인증)
    - 2단계: RSA 알고리즘으로 전자 서명 정보를 암호화 (전송 보안)



  - 해독 과정
    - 1단계: RSA 알고리즘으로 전자 서명 정보를 해독
    - 2단계: 전자 서명 알고리즘을 인증 정보 해독

6. 보안 프로토콜

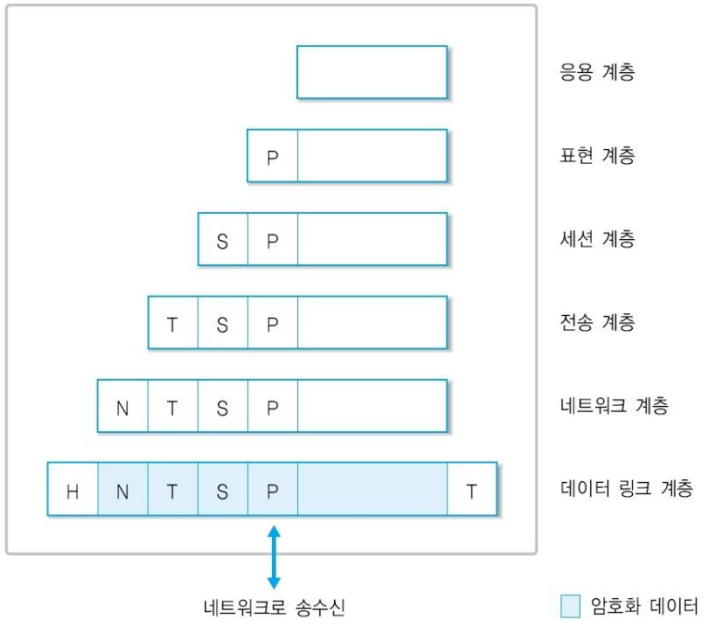
- 보안 프로토콜의 개요
  - 인터넷은 전세계적으로 연결된 거대한 통신망으로, 송신자가 전송한 데이터가 수신자에게 전달되는 과정에서 여러 호스트와 매체를 통함
  - 중간에 위치한 호스트의 보안 등급이 낮게 설정된 경우 위험에 노출될 가능성이 높아짐
  - 위협요소의 종류
    - 전송 데이터를 중간에서 감청하거나 임의로 변경하는 경우
    - 호스트 데이터에 위해를 가하는 등 직접적으로 호스트 내부에 침입하는 경우
    - 과도한 트래픽을 발생시켜 특정 호스트의 통신을 방해하는 경우

* 감청이란?

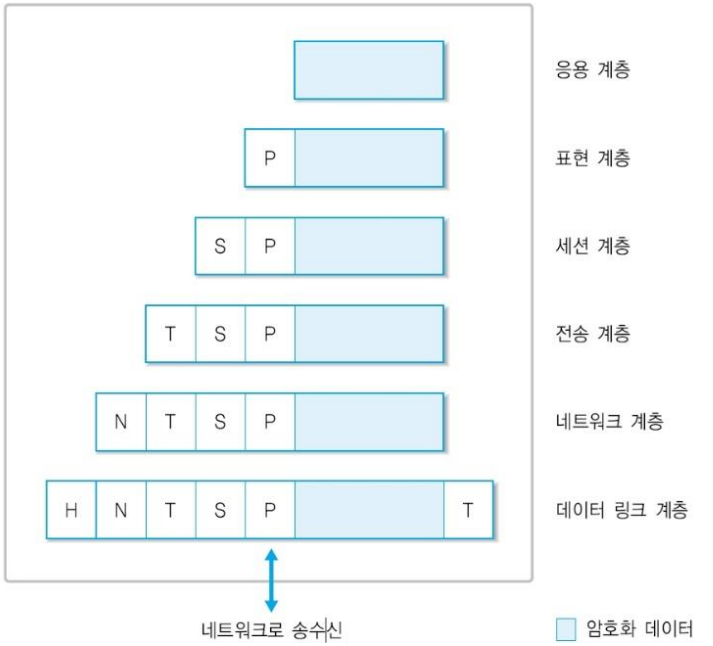
- 허가받지 않은 자가 직간접적인 방법으로 전송중인 데이터를 얻어내는 것
- 얻어낸 정보를 변경한 후 이를 통신 과정에 입력함으로써 송수신 호스트의 통신 내용을 왜곡하는 것도 넓은 의미에서 감청에 포함
- 전통적으로 감청의 가장 일반적인 형태는 유선의 통신 선로에서 이루어짐
- 휴대폰의 무선 데이터는 무선 신호가 넓은 범위로 전파되므로 물리적 감청이 훨씬 용이한 편

6. 보안 프로토콜

- 암호화
  - 데이터 링크 계층 암호화
    - 전송 미디어에서의 감청 위협으로부터 데이터를 안전하게 보호하는 방법에는 물리 계층에서 데이터를 송신하기 전에 암호화



  - 응용 계층 암호화
    - 데이터 링크 계층 암호화는 네트워크 계층에서 암호화가 되지 않기 때문에 라우터에서 보안이 되지 않음
    - 라우터를 포함한 전송 호스트 내부에서는 보안을 지원하지 않고, 호스트와 호스트 사이의 전송 과정에서만 보안이 유지



6. 보안 프로토콜

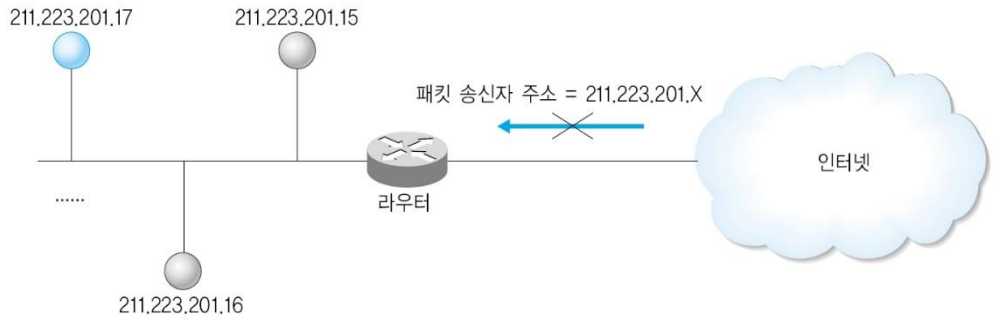
- 트래픽 제어
  - 특정 호스트가 누구와 통신을 많이 하는지에 대한 정보도 네트워크 보안에 포함
  - 무의미한 가공 데이터를 여러 호스트에서 주기적으로 발생시켜 통계자료에 혼선을 주는 방법으로 통신량 분석을 방해

- 방화벽(Firewall)
  - 개방적인 공중 인터넷망과 제한된 사용자 그룹에게 허가된 사설망 사이에 보안 기능을 제공

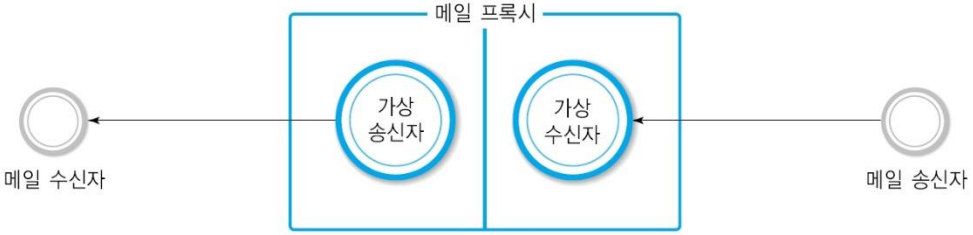
  - 패킷 필터링 방식
    - 방화벽이 패킷의 헤더를 검색하거나 필요에 따라서 내용까지 검색하여 적절하지 못한 패킷을 배제
    - 보통은 라우터에서 이루어짐
  - 의심스러운 행위를 하는 사용자를 감시
  - 사설 망을 외부로부터 보호하는 가장 간단한 방법은 외부 망을 완전히 끊어버리는 것

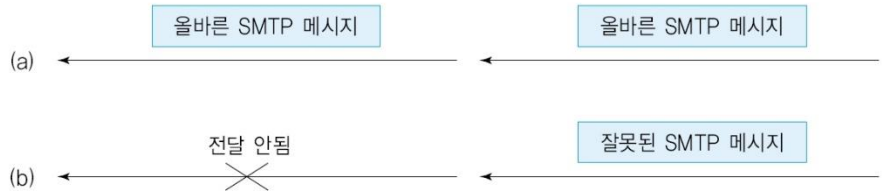
6. 보안 프로토콜

- 라우터를 이용한 방화벽 구현
  - 인터넷에 연결된 모든 호스트는 외부 통신망과 연결하기 위해 반드시 라우터의 중개 과정을 거쳐야 함
  - 네트워크 계층과 전송 계층의 헤더 정보에 기초하여 보안 제공
  - 간단하면서도 매우 효과적인 방법
  - 라우터 방화벽의 사용
    - 외부의 특정 호스트가 스팸 메일을 보낼 때
    - 내부 사용자가 불법 사이트에 접근한 것 차단
  - IP 주소 뿐만 아니라 포트 번호를 이용한 응용 프로그램에 대한 접근도 차단이 가능



- 프록시(Proxy)를 이용한 방화벽 구현
  - 프록시는 응용 환경에서 적절하게 처리할 수 있는 정보만 수신하도록 가상의 응용프로그램을 시뮬레이션 하는 방화벽
  - 내부 네트워크의 호스트에는 외부 네트워크의 응용 연결처럼 보이고, 외부 네트워크에서는 내부 네트워크의 응용 연결처럼 보임





한 학기 동안 고생 많으셨습니다!