정보보안개론

2009. 10

박 종 혁
(jhpark1@snut.ac.kr)
www.parkjonghyuk.net

발표 내용

- 정보보안이란 무엇인가?
- 보안공격이란?
- 정보보안의 목표
- 정보보안의 간략한 역사
- 암호시스템
- 암호분석이란?
- 정보보안의 중요 개념들
- 정보보안의 영역
- 계층적 방어 전략
- 네트워크 보안 개요
- 시스템 보안 개요
- 해킹
- 최근 보안 관련 이슈들
- 질의응답

정보보안이란 무엇인가?

❒ 정보화 사회에서 정보의 의미

- ❍ 정보는 물질이나 에너지 자원보다 더 중요한 가치를 가지게 됨
- ❍ 정보가 중요한 자산으로서 인식되며 사회 및 생활 전반에 있어서 중요한 위치를 차지하게 됨 (정보 = 자산 or 권력)

❒ 정보보안 (Information Security)

- ❍ 정보 및 정보 시스템을 허가되지 않은 접근, 사용, 공개, 손상, 변경, 파괴 등으로부터 보호함으로써 무결성, 기밀성, 가용성을 제공하는 것
  - USC Title 44, Chapter 35, §3542
    The term “information security” means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide integrity, confidentiality, and availability.

보안 공격이란?

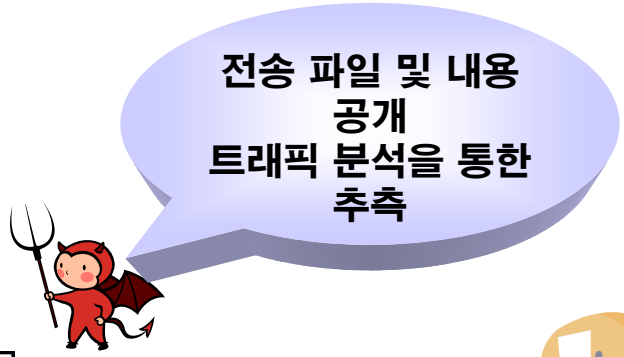
- **보안 공격** (Security Attack)
  - **조직의 정보보호를 저해하는 제반행위**

- **보안 공격의 유형**
  - **소극적 공격** (passive attack)
  - **적극적 공격** (active attack)

보안 공격의 유형

보안 공격

소극적 공격



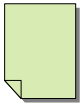
철 수

영희

가로채기

재전송, 메시지 수정

적극적 공격



철수로 위장

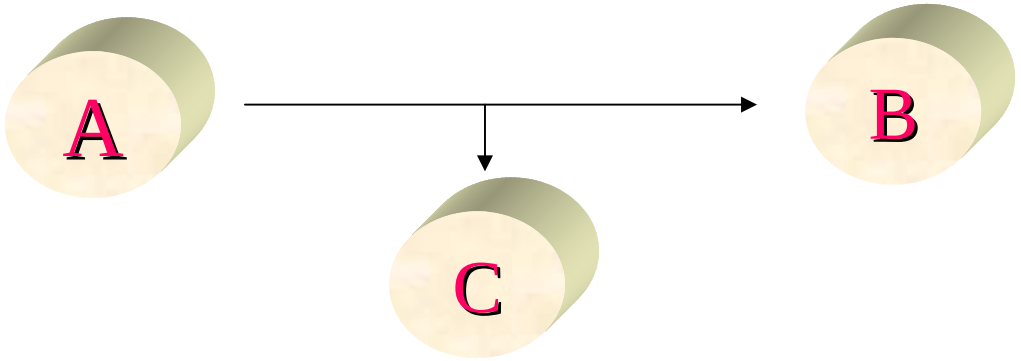
소극적 공격: passive attack

- 소극적 공격이란?
  - 가로채기
  - 도청
  - 트래픽 분석: 송수신자 신분, 통신시간 , 주기관찰
  - 변화가 없으므로 검출 곤란
  - 검출보다 예방 필요

가로채기: Interception

❍ 가로채기

- 비인가자들의 불법적인 접근에 의한 신뢰성에 대한 공격

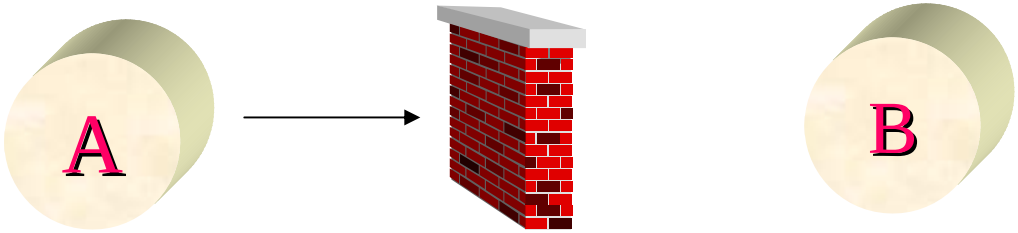


적극적 공격: active attack

- 적극적 공격이란?
  - 방해: 가용성 침해
  - 불법적 수정: 무결성 침해
  - 재전송 : 데이터 단위 수동적 획득 -> 다시 전송
  - 서비스 부인 (서비스 거부 공격) : 특정 목표물을 대상으로 무력화, 성능저하 유발
  - 예방하기가 대단히 어려움: 모든 자원과 시간 보호불가능
  - 예방, 탐지, 복구 필요

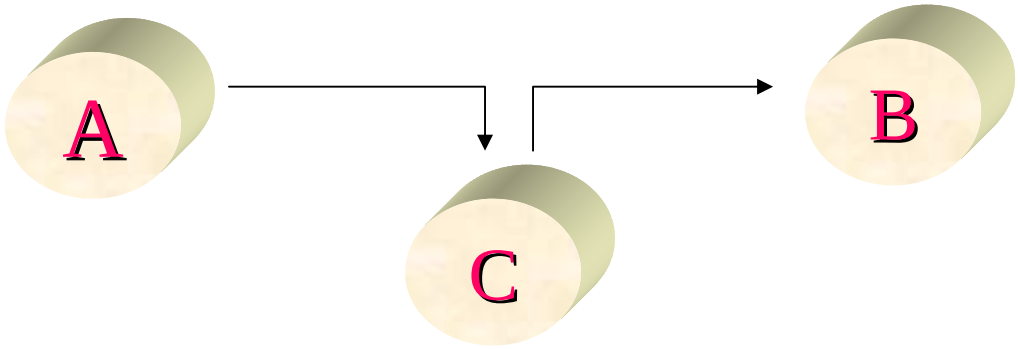
방해: Interruption

- 방해
  - 시스템의 일부가 파괴되거나 사용할 수 없는 경우로 가용성에 대한 공격



불법수정: Modification

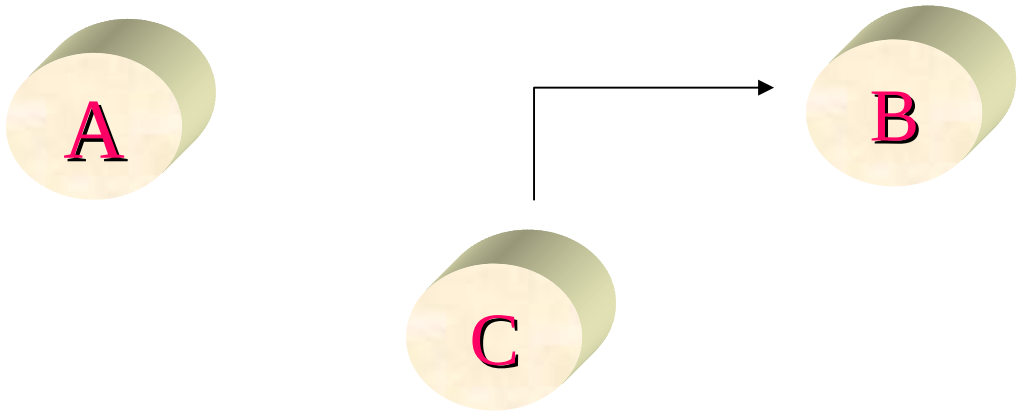
- 불법수정
  - 비인가자들의 불법적인 접근 뿐만 아니라 불법적인 변경에 의한 무결성에 대한 공격



위조: Fabrication

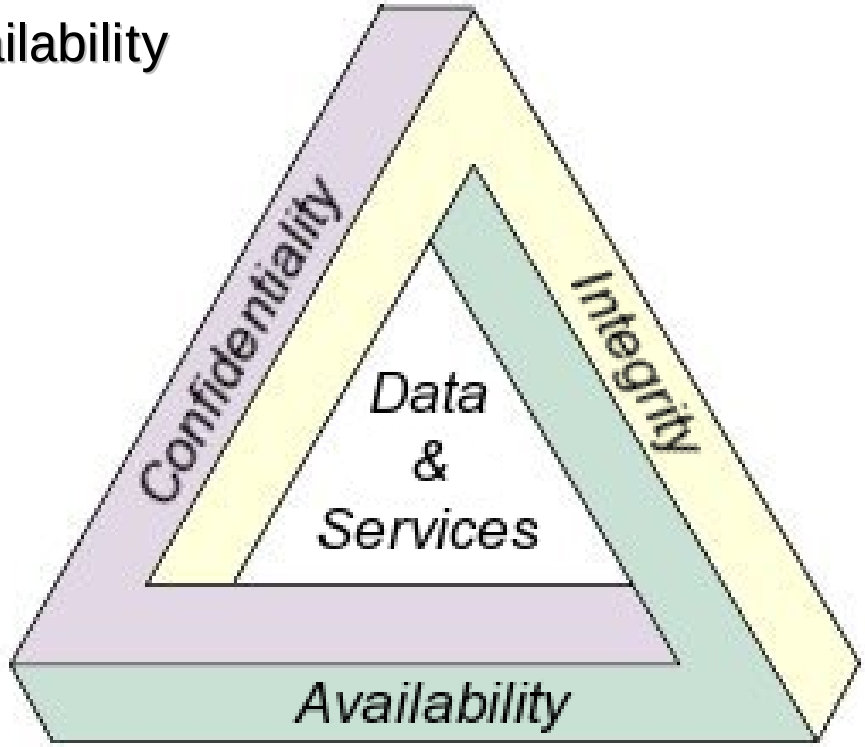
❒ 위조

❍ 비인가자들의 시스템에 대한 위조물 삽입에 의한 인증에 대한 공격



정보보안의 목표

- **보안의 3원칙** (CIA Triad)
  - **정보보안이 목표로 하는 세가지 핵심적인 원칙**
  - **기밀성**: confidentiality
  - **무결성**: integrity
  - **가용성**: availability



기밀성: confidentiality

- 기밀성이란?
  - 합법적인 실체만 읽을 수 있도록 보호하는 서비스
  - 메시지 내용 공개, 트래픽 흐름 분석, 도청으로부터 전송 메시지 보호
  - 접속 구간 기밀성, 내용 기밀성, 메시지 흐름 기밀성
  - 암호 알고리즘 이용

무결성: integrity

❒ 무결성이란?

- ❍ **합법적인 실체만 수정할 수 있도록 보호하는 서비스**
- ❍ **연결형 무결성 서비스, 비연결형 무결성 서비스**
  - 연결형 : 메시지 스트림을 대상, 불법변경 보호와 서비스 부인 방지
  - 비연결형 : 개인 메시지들만을 대상, 불법변경 보호
- ❍ **무결성이 깨지는 경우의 예**
  - 사고에 의한 또는 의도적인 변경 또는 삭제
  - 중복 보관 중인 정보 중의 일부가 변경 또는 삭제
  - 컴퓨터 바이러스 등에 의한 손상
- ❍ **해쉬 함수, 디지털 서명, 암호 알고리즘 이용**

가용성: availability

- 가용성이란?
  - 정보에 대한 접근과 사용이 적시에 확실하게 보장되는 상태를 의미함
  - 다시 말해서, 정보 또는 정보 시스템 또는 정보보안 시스템이 원하는 때에 제대로 제공(작동)되는 것을 의미함

인증 서비스: authentication

- 인증이란?
  - 정보 및 시스템의 자원을 사용하는 정당한 사용자임을 확인할 수 있도록 보호하는 서비스
  - 연결된 송수신자 확인, 제 3자의 위장 확인
  - 발신처 인증, 메시지 인증, 실체 인증

부인봉쇄 서비스: non-repudiation

- 부인봉쇄란?
  - 송수신자가 송수신 사실에 대한 부인을 하지 못하게 하는 것
  - 송신자 부인 봉쇄, 수신자 부인봉쇄, 배달증명, 의뢰증명

접근 제어: access control

- 접근 제어란?
  - 사용자가 시스템 혹은 특정 자원에 접근 하고자 할 때 인가 받은 사용자만 접근을 허락하도록 제어하는 서비스

정보보안의 간략한 역사

- 고대 – 중세
  - 문서를 봉인하여서 전달함으로써 기밀성과 무결성을 보장하려 함
  - Caesar 암호 등을 비롯한 간단한 방식의 암호기법이 사용됨
- 2차 세계 대전 시기
  - 정보보안의 많은 진보가 있었고, 전문적인 영역으로 인정받게 됨
  - 각종 환자 및 전치 암호 방식이 개발되고 사용됨
- 현대
  - 컴퓨팅 환경과 네트워킹 환경이 급속도로 발전함에 따라서 정보의 가치가 높아지게 되고, 이에 따라서 정보보안에 인식이 높아지고 다양한 기술 개발이 이뤄지게 됨
  - 시스템과 네트워크 등을 총괄하는 기술적인 개념 위주의 정보보안의 영역이 정보보증이라는 상위 개념으로 확대되고 있음

STEGANOGRAPHY

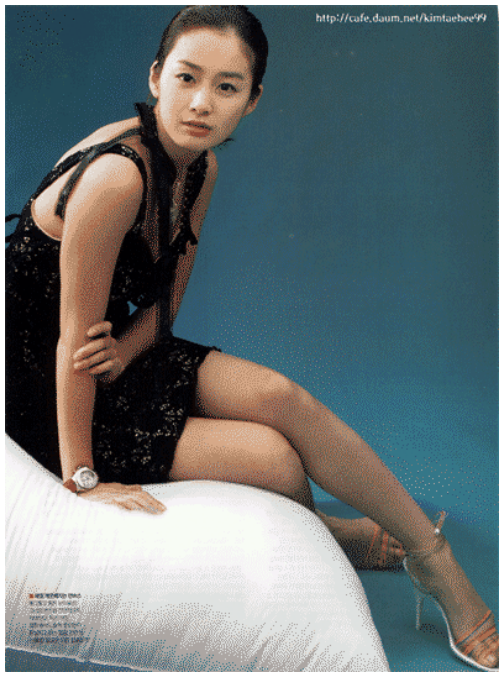
- **메시지의 존재 자체를 은폐하는 방식**
  - **그림 파일에 일정한 그림이나 문자 혹은 문서를 변환 삽입**
  - **문자 마킹**
    - 인쇄 또는 타자된 원문의 문자들을 선택하여 연필로 그 위에 덧쓰는 방법, 밝은 빛을 적당한 각도로 비춰야만 보임
  - **보이지 않는 잉크**
    - 종이에 열 또는 화학 처리를 해야만 보이는 다양한 종류의 잉크 사용
  - **핀 구멍**
    - 빛을 비춰야만 보이는 작은 구멍을 원문의 특정 문자에 넣는 방법
  - **타자 수정 리본**
    - 흑색 리본으로 타자된 줄 사이에 강한 빛에서만 보이는 수정 리본을 이용

- **미국의 테러사건의 빈라덴과 알카에다의 조직원들이 웹의 이미지 사진에 정보를 숨겨서 이용함**

STEGANOGRAPHY

❒ STEGANOGRAPHY

- ❍ **실습** : www.stegoarchive.com **개발사 및 프리 소프트웨어 제공**
- ❍ **실습 프로그램** : S-tools3**를 다운받아 실행**
  - ▪ 하나의 이미지 안에 다른 이미지를 숨김
    - • 아래 김태희 사진에 프로그램 순서도 이미지를 숨길 예정



김태희 사진

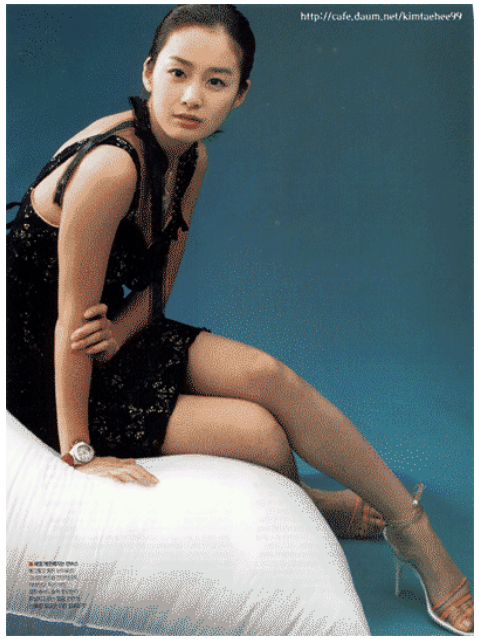
기호	기호의 설명	보기
	순서도의 시작이나 끝을 나타내는 기호	시작(끝)
	값을 계산하거나 대입 등을 나타내는 처리 기호	A=B+C
	조건이 참이면 '예', 거짓이면 '아니오'로 가는 판단 기호	A>B 아니오 예
	서류로 인쇄할 것을 나타내는 인쇄 기호	인쇄 A
	일반적인 입·출력을 나타내는 입·출력 기호	입력(출력)
	기호를 연결하여 처리의 흐름을 나타내는 흐름선	시작 A,B 입력

프로그램 순서도

STEGANOGRAPHY

- **그러나 실제로는 앞 사진에 이미 S-tool3를 이용하여 다른 이미지 하나를 미리 숨겨 두었음.**
  - **1번은 인터넷 상 실제 이미지 즉 원본**
  - **2번은 다른 이미지를 숨긴 앞 피티에서 본 이미지**
    - 의식하지 않고 보면 그냥 해상도가 낮은 사진처럼 보임

1번 김태희 사진

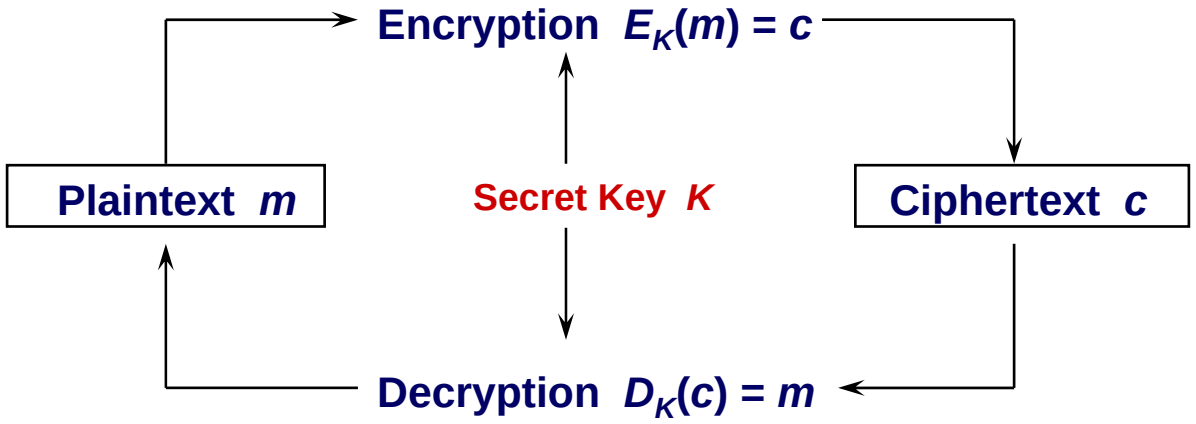


2번 김태희 사진

암호시스템 : Cryptosystem

❒ 구성요소

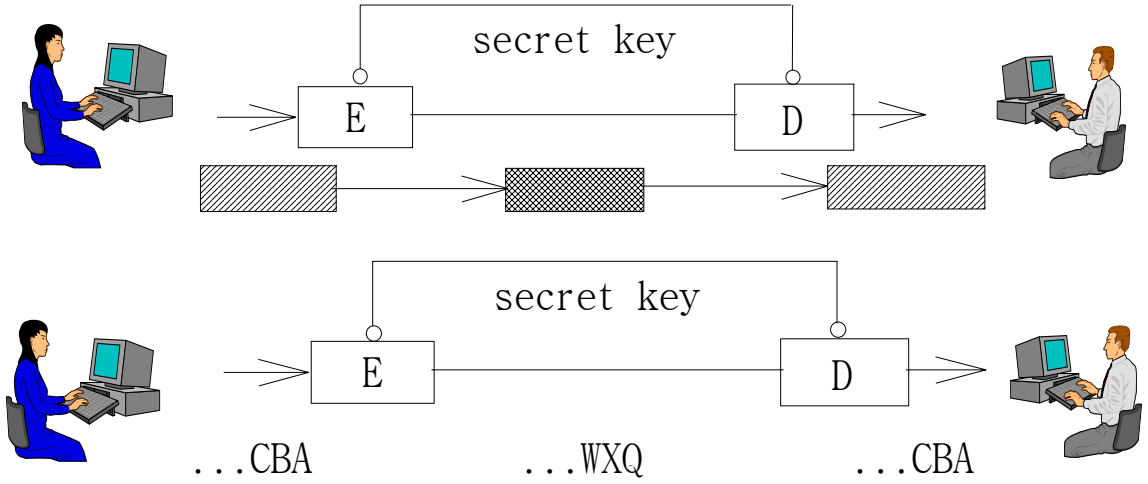
- ❍ M : Plaintext Message Space
- ❍ C : Ciphertext Message Space
- ❍ K : Key Space
- ❍ E_k : M C, a set of Encryption Transformations
- ❍ D_k : C M, a set of Decryption Transformations



암호시스템의 분류

- Symmetric Cryptosystem (Private-Key Cryptosystem)
- Asymmetric Cryptosystem (Public-Key Cryptosystem)

- Block Cipher
- Stream Cipher



평문 길이에 의한 분류

- 암호화가 적용되는 평문 길이의 최소단위에 의한 분류
  - 스트림 암호 – 평문 길이의 최소단위가 한 개의 비트나 문자
  - 블록 암호 – 평문 길이의 최소단위가 한 개 이상의 비트나 문자

키의 동일 여부에 따른 분류

❒ 암호화에 사용되는 키와 복호화에 사용되는 키의 동일여부

- ❍ 대칭형 암호시스템 – 동일 예> DES
- ❍ 공개키 암호시스템 – 공개키 (암호화에 사용)
  개인키 (복호화에 사용)
  – 예) RSA

암호분석이란?

- **암호분석** (Cryptanalysis)
  - 암호문으로부터 평문이나 비밀키를 도출
  - 특정암호문과 그에 해당하는 평문으로부터 적용된 비밀키를 도출
    - ※ 암호 시스템의 설계나, 안전성의 검증에 사용

- **암호공격 방법**
  - **암호문 공격** (Ciphertext – only attack)
  - **알려진 평문 공격** (Known-plaintext attack)
  - **선택된 평문 공격** (Chosen-plaintext attack)
  - **선택된 암호문 공격** (Chosen-ciphertext attack)

암호문 공격: Ciphertext – only attack

- 암호문 공격
  - 도청된 암호문만 주어진다
  - 가능한 모든 키 적용 : 가장 간단; 키가 길면 유효하지 못함
  - 공개된 암호화 및 복호화 알고리즘에 대한 취약점 분석이 주된 공격 대상

알려진 평문 공격: Known-plaintext attack

- 알려진 평문 공격
  - 몇 쌍의 평문과 대응하는 암호문이 주어진다
  - 도청된 암호를 해독하거나 적용된 비밀키 분석

선택된 평문 공격: Chosen-plaintext attack

- **선택된 평문 공격**
  - **암호분석가가 선택한 평문에 해당하는 암호문 선택**
  - **비밀키 구조 파악이 예상되는 평문 선택**
  - **목적**
    - 비밀키 분석
    - 보내고 싶은 평문에 대응하는 암호문을 만드는 것
  - **가장 선호되는 분석환경**
  - **이 공격에서 안전하면 가장 이상적**

선택된 암호문 공격: Chosen-ciphertext attack

- 선택된 암호문 공격
  - 암호분석가가 선택한 암호문에 해당하는 평문을 얻을 수 있다
  - 암호분석가가 복호화 장치에 접근 가능한 상황
  - 목적 : 다른 관측된 암호문에 해당되는 평문 도출

정보보안의 중요 개념들

- 위험 관리
  - 변화하는 환경에 맞게 1)과 2)를 지속적으로 수행하는 프로세스
    1) 위험 식별: 정보 자원의 취약점과 위협요소를 파악하는 것
    2) 대책 마련: 정보 자원의 가치에 합당한 수준으로 위험을 감소시키는 대책을 마련하는 것
- 취약점 (vulnerability)
  - 정보자원에 위험이나 손상을 입힐 수 있는 약점들
- 위협요소 (threat)
  - 장애나 손상을 유발할 수 있는 잠재적인 대상들
- 대책 (countermeasure)
  - 위험 관리를 위해 사용될 수 있는 방법들
  - 정보보안의 영역으로 설명될 수 있음

위협 요소

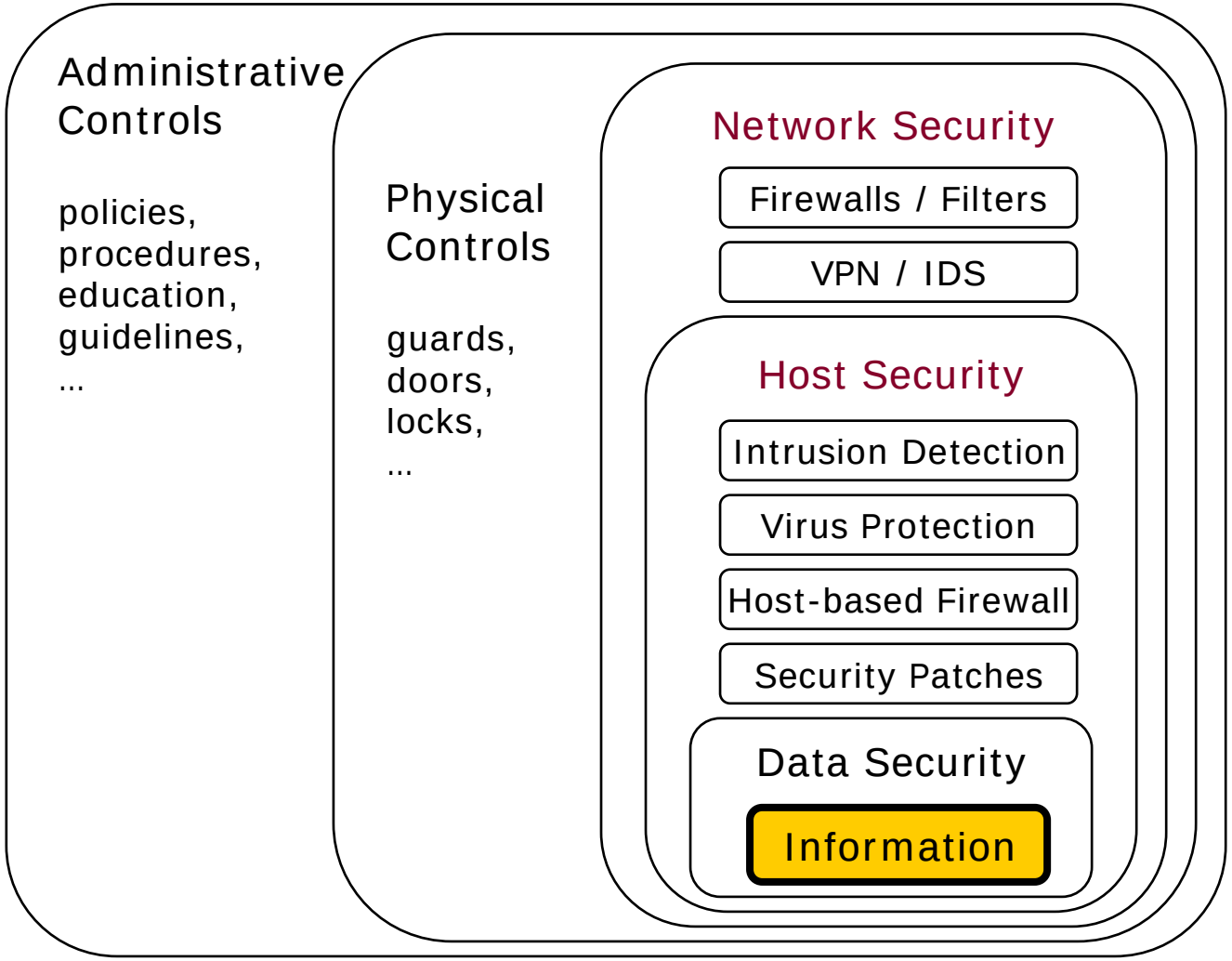
- 자연적 위협 요소
  - 자연적 재앙, 에러 및 손실, 정보관리 부실
  - 네트워크 장애, 시스템 장애

- 고의적 위협 요소
  - 내부의 적, 컴퓨터 해킹, 위장(Masquerade)
  - 메시지 순서 변조 (Modification of Message Sequence)
  - 정보 변조 (Modification of Information)
  - 서비스 거부 (Denial of Service), 부인 (Repudiation)
  - 정보노출 (Leakage of Information)
  - 신분 레이블 변조 (Modification of Identification Label)

정보보안의 영역

- 관리적 통제 (administrative controls)
  - 정책적인 통제
  - 문서화된 정책, 정형화된 절차, 표준, 가이드 라인 등
- 물리적 통제 (physical controls)
  - 작업장 또는 컴퓨팅 장치 등에 대한 감시와 통제를 의미한다
  - 예) 출입문, 잠금 장치, 감시 카메라, 경비원, 네트워크 분리, …
- 논리적 통제 (logical controls)
  - 기술적인 통제, 가장 일반적으로 생각하는 정보보안의 영역
  - 정보 시스템을 감시하고 통제하기 위해서 소프트웨어와 특정 데이터를 이용하는 것
  - 예) 패스워드, 방화벽, 침입탐지시스템, 접근제어, 데이터 암호화, …
- 환경적 통제 (environmental controls)
  - 환경적 재해(자연재해, 화재, 정전)에 대한 대비 및 복구 방안

계층적 방어 전략 (defense in depth)



네트워크 보안 개요

❒ 방화벽

❍ 신뢰하지 않는 외부 네트워크와 신뢰하는 내부 네트워크 사이를 지나는 패킷을 차단하거나 보내주는 기능을 하는 HW 또는 SW

- 접근제어 (access control)
  - 관리자가 방화벽에게 통과시킬 접근과 그렇지 않은 접근을 명시
  - 패킷 필터링(packet filtering) 방식, 프록시(proxy) 방식
- 로깅(logging)과 감사추적(auditing)
  - 허가, 또는 거부된 접근에 대한 기록을 유지
- 인증(authentication)
  - 메시지 인증, 사용자 인증, 클라이언트 인증
- 데이터의 암호화(encryption)
  - 방화벽에서 다른 방화벽까지 전송되는 데이터를 암호화

❒ 네트워크 기반의 침입 탐지 시스템(NIDS)

❍ 침입에 대한 빠른 탐지를 위한 목적으로 사용된다

❍ 자료의 수집, 필터링과 축약, 분석 및 탐지, 추적과 대응을 용이하게 한다

시스템 보안 개요

- 대표적인 시스템 보안 관리 업무
  - 적절한 보안설정
  - 정기적인 보안 패치 적용
  - 바이러스 방역
  - 호스트 기반의 침입 탐지 시스템 (HIDS)
  - 호스트기반 방화벽
  - 운영체제 취약점 분석 및 대응 방법 마련

해킹

❒ 해킹

- ❍ **관리자가 구축해놓은 보안망을 무력화 시키고 네트워크/시스템에 불법적으로 접근하는 모든 행위**

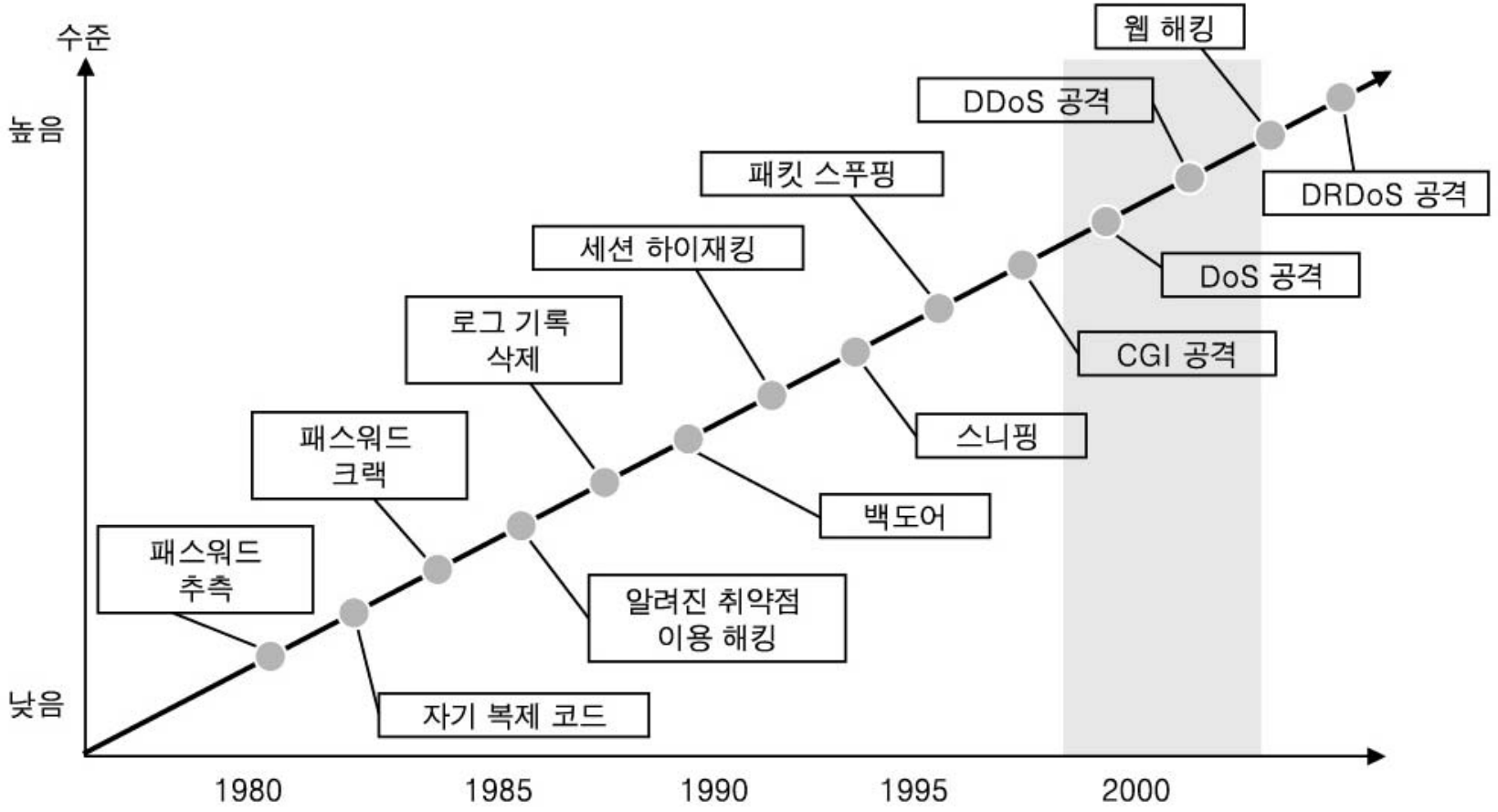
❒ 대표적인 해킹의 유형

- ❍ **침입** (intrusion)
  - 불법적으로 시스템 자원을 사용하거나 또 다른 해킹을 위한 경로로 사용하는 행위
- ❍ **서비스 거부** (DoS, denial of service)
  - 특정 호스트나 네트워크가 제 기능을 수행하지 못하도록 각종 서비스를 정지시키는 행위
- ❍ **정보 유출**
  - 경쟁 기업의 정보를 훔치거나 훔쳐낸 기밀을 외부에 유포/판매하는 행위

공격의 종류

- 시스템과 서비스의 설정 취약점을 이용한 공격
  - 파일 시스템의 쓰기 권한 취약점을 이용
  - SUID 프로그램의 문제를 이용, ...
- 프로그램의 취약점을 이용한 공격
  - CGI/자바스크립트의 취약점을 이용한 공격
  - ASP, PHP 스크립트의 취약점을 이용한 공격
  - 버퍼 오버플로우(Buffer Overflow) 공격
  - 힙 오버플로우(Heap Overflow) 공격
  - 레이스 컨디셔닝(Race Conditioning) 공격
  - 포맷 스트링(Format String) 공격
  - 프레임 포인터 오버플로우(Frame Pointer Overflow) 공격
- 프로토콜의 취약점을 이용한 공격
  - DoS, 스니핑(Sniffing), 세션 하이재킹(Session Hijacking), 스푸핑(Spoofing)
- 악성 코드
  - 바이러스, 트로이안, 백도어, 웜

해킹의 기법의 변화


수준
높음
낮음
웹 해킹
DDoS 공격
패킷 스푸핑
DRDoS 공격
세션 하이재킹
DoS 공격
로그 기록
삭제
CGI 공격
패스워드
크랙
스니핑
백도어
패스워드
추측
알려진 취약점
이용 해킹
자기 복제 코드
1980
1985
1990
1995
2000

최근 보안 관련 이슈들

❒ 유비쿼터스 환경에서의 보안

❍ 유비쿼터스 환경

= Internet of things + pervasive computing
+ context awareness + intelligent services
+ multimedia + embedded + ...

❍ 전파식별 (RFID)

- 사용자 프라이버시 보호, 위치추적 방지

❍ 센서네트워크 (sensor networks)

- 정보 유출 방지, 잘못된 정보의 필터링 → 키관리

❍ 임베디드 시스템 (embedded systems)

- 정보 유출 방지, 위변조 방지

참고문헌

- 양대일, "정보보안 개론과 실습 시스템 해킹과 보안", 한빛 미디어, 2006.7
- 양대일, "정보보안 개론과 실습 네트워크 해킹과 보안", 한빛 미디어, 2005.8
- 최용락 외 3명, "컴퓨터 통신보안", 그린, 2006.1
- 홍승필, "유비쿼터스 컴퓨팅 보안", 한티미디어, 2006,9
- 박창섭, "암호이론과 보안", 대영사, 2006,2

질의응답

감사합니다