네트워크 보안 개요

2018. 03. 13

박종혁 교수
(jhpark1@seoultech.ac.kr)

목 차

컴퓨터 보안

- 컴퓨터 보안 정의
  - 정보시스템 자원의 기밀성, 무결성, 가용성을 보장하는 목표를 갖는 정책
  - 위의 정책이 자동화된 정보 시스템에 제공될 수 있도록 함

- 컴퓨터 보안 목적
  - 기밀성 (Confidentiality) : 허가, 권한이 없는 자에게 정보의 누출방지를 보장하는 성질

    데이터 기밀성 – 실제 데이터에 대한 기밀성

    프라이버시 – 내 권한이 미치는 정보(데이터, 기능)에 대해 통제, 영향을 보장

    소극적 공격에 대한 보장

  - 무결성 (Integrity) : 허가, 권한이 없는 자로부터 정보의 수정(파괴)방지를 보장하는 성질

    데이터 무결성 – 실제 데이터에 대한 무결성

    시스템 무결성 – 시스템의 기능에 대한 무결성

    적극적 공격에 대한 보장

  - 가용성 (Availability)

    시스템이 지체 없고 합법적 사용자에게 적합한 서비스를 제공

컴퓨터 보안

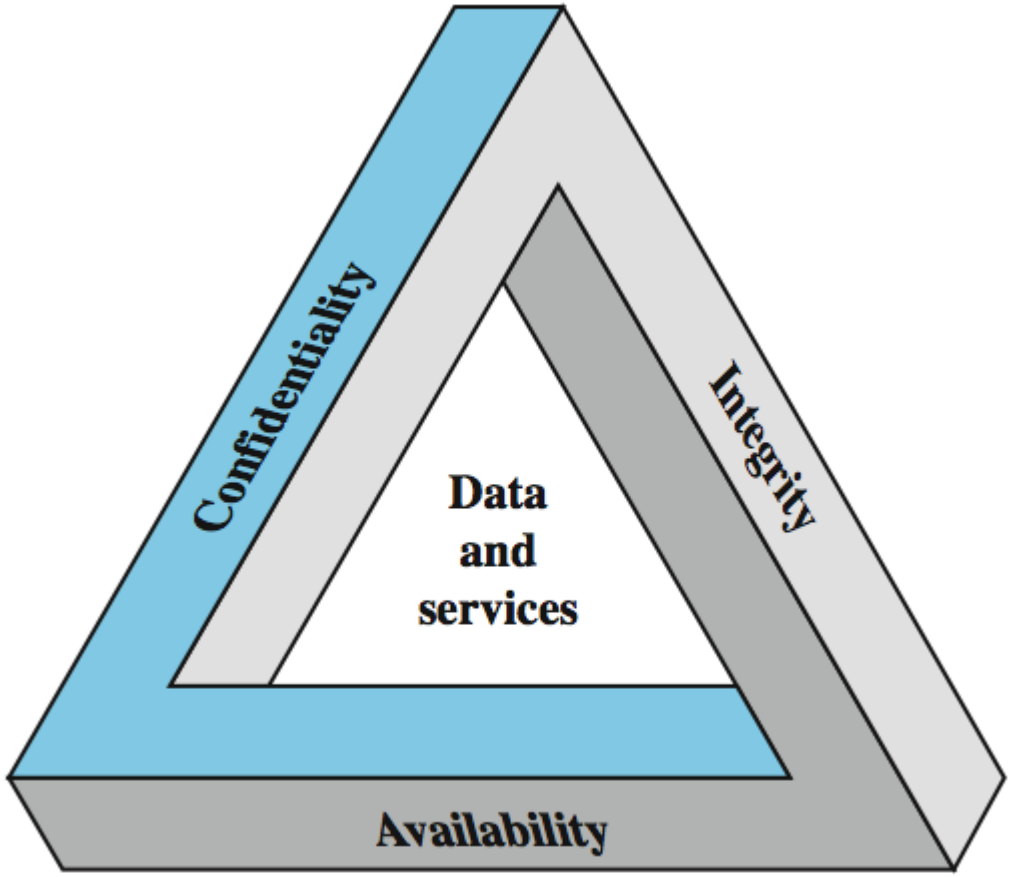
- 컴퓨터 보안 목적
  - 인증 (Authentication)
    - 진짜라는 성질을 확인 할 수 있고 신뢰 할 수 있다는 것
      - 전송, 내용, 출처 유효성에 대한 확신
      - 사용자가 일치하는 사용자임을 인증
      - 자료가 신뢰할 수 있는 출처인지 인증
    - 인증이 완료되면 무결성, 기밀성을 보장함
  - 책임 (Accountability)
    - 보안이 미치는 범위에서는 보안 침해에 대한 정보를 기록, 분석, 추적을 할 수 있어야 함
    - 부인 봉쇄, 억제, 결함 분리, 침입을 탐지 및 예방 함
    - 사후 복구와 법적 조치 등이 포함됨

컴퓨터 보안

- 컴퓨터 보안의 조건과 위협
  - 보안 서비스는 기밀성, 인증, 부인봉쇄(Non-repudiation), 무결성을 필수적으로 보장 해야 함
  - 특정 보안 메커니즘(알고리즘) 개발시 보안구조를 깨려는 모든 공격 가능성을 고려해야 함
  - 특정 보안이 보안의 전체적인 면에서 정말 필요한지 구별이 필요
  - 다양한 보안 메커니즘이 어디에 사용될지 결정 (물리적, 논리적 위치)
  - 비밀정보의 보안을 위한 키의 생성, 분배 문제와 비밀정보의 보호 문제를 지체 없이 처리 할 수 있어야 함
  - 보안이 너무 강하면 효율성을 떨어트림

  - 위와 같이 고려해야 할 사항이 많아 OSI 보안구조의 표준이 존재

Key Security Concepts



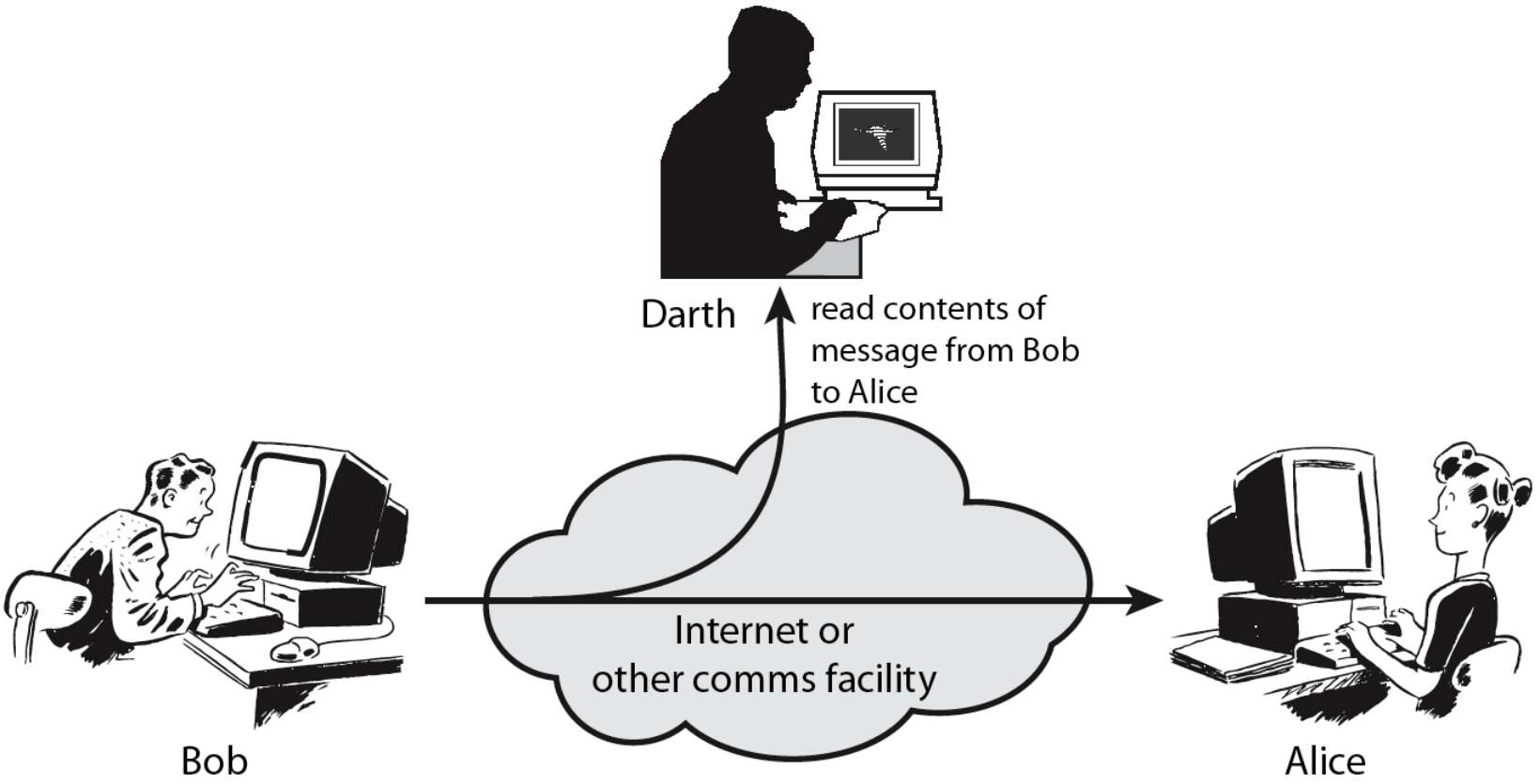
OSI 보안 구조

- **OSI 보안구조 (Security Architecture For OSI)**
  - **OSI (Open System Interconnection)**
    - 컴퓨터 네트워크 프로토콜의 설계, 통신을 계층으로 나누어 설명한 모델
    - 물리, 데이터링크, 네트워크, 전송, 세션, 표현, 응용 의 순으로 7계층
  - **OSI 계층을 바탕으로 보안의 필요성과 가치에 대한 평가, 선택을 위해 보안에 필요한 항목을 체계적으로 정의하고 구체적인 방법들을 제시해주는 국제 표준**
  - **OSI 보안 구조의 핵심은 보안공격, 보안 메커니즘, 보안서비스 을 정의함**

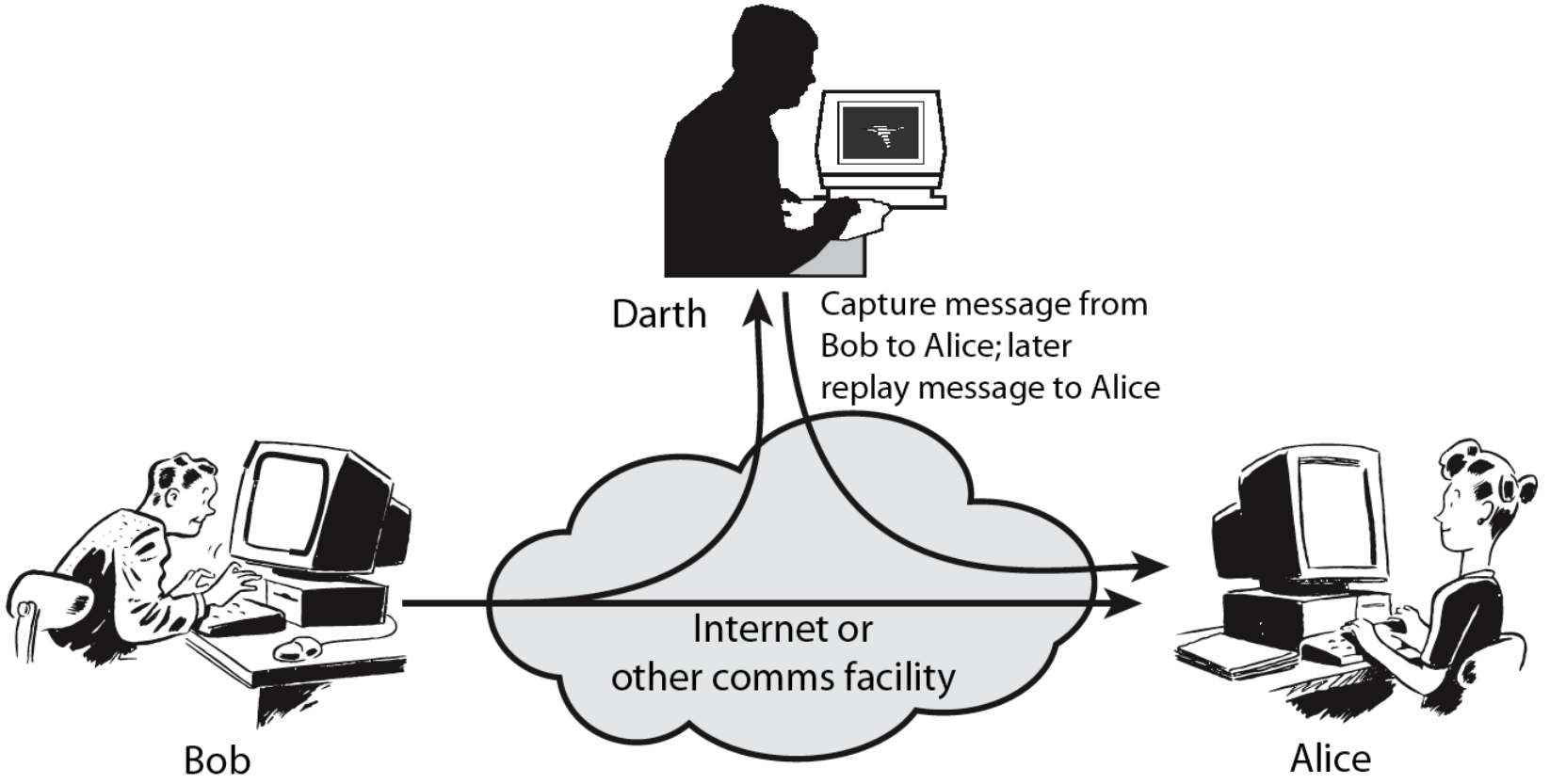
보안 공격

- **보안 공격 (Security Attack)**
  - **기관이 소유한 안전성을 침해하는 행위, 보안 서비스로 대응함**
  - **위협 (Threat) 과 공격 (Attack)**
    - **위협 : 보안에 침해와 위해를 가할 수 있는 환경, 능력, 행동, 사건(event)과 같은 것 보안 취약점을 이용하려는 잠재적인 위험**
    - **공격 : 보안서비스, 시스템 보안 정책을 위반하는 정교한 침입, 시스템 보안에 대한 실제적 침범을 의미**
  - **소극적 공격 (Passive Attack)**
    - **시스템으로부터 정보를 획득, 사용하려는 시도, 시스템 자원에는 영향을 끼치지 않음**
    - **탐지가 어려우므로 예방이 목적**
    - **Ex) 메시지 내용 갈취 (Release Of Message Contents), 트래픽 분석 (Traffic Analysis)**
  - **적극적 공격 (Active Attack)**
    - **데이터 스트림을 수정하거나 가짜를 만드는 행위를 포함하고 하단의 예시**
    - **완벽한 차단 불가능 (물리적 보호가 필요)**
    - **탐지, 피해 복구가 목표**
    - **Ex) 신분 위장(Masquerade), 재전송 (Replay), 메시지 수정 (Modification Of Messages), 서비스 거부 (Denial Of Service)**

Passive Attacks



Active Attacks



보안 메커니즘

- 보안 메커니즘
  - 특정 보안 메커니즘, 일반 보안 메커니즘 으로 분류
- 특정 보안 메커니즘 (Specific Security Mechanisms)
  - 보안 서비스에 적용되어 보안 공격을 탐지, 예방하는 기술
  - 암호화 (Encipherment)
    - 데이터 전송시 데이터를 암호화 기술
    - 복구 가능 암호화 메커니즘
      - » 데이터를 암호화, 복호화할 수 있는 암호 알고리즘
    - 복구불가 암호화 메커니즘
      - » 디지털 서명(해시 알고리즘), 메시지 인증(메시지 인증 코드) 응용에 사용
  - 디지털 서명 (Digital Signature)
    - 데이터 수신자가 데이터의 발신자와 무결성을 입증 하기위한 기술
    - 역으로 위조를 막도록 데이터에 붙이는 데이터 또는 데이터 단위의 암호적 변경
  - 데이터 무결성 (Data Integrity)
    - 데이터단위, 스트림의 무결성을 입증하기 위한 기술

보안 메커니즘

- 특정 보안 메커니즘 (Specific Security Mechanisms)
  - 접근 제어 (Access Control)
    - 자원에 접근할 권한을 제한하는 다양한 메커니즘
  - 인증 교환 (Authentication Exchange)
    - 정보 교환을 통해 개체의 신원을 확인하는 데 사용하는 메커니즘
  - 트래픽 패딩 (Traffic Padding)
    - 트래픽 분석 시도를 방해하기 위해 데이터 스트림 의 빈 곳을 비트로 채워 넣는 것
  - 경로 제어 (Routing Control)
    - 특정 데이터에 대해 물리적으로 안전한 경로를 선택할 수 있게 함
    - 특히, 보안침해가 의심스러운 경우 경로 조정 가능
  - 공증 (Notarization)
    - 데이터 교환의 어떤 성질(기밀성 등)을 확신하기 위해 신뢰 받는 제 3자를 이용

보안 메커니즘

- 일반 보안 메커니즘
  - 특정 OSI보안 서비스나 프로토콜 계층에 구애받지 않는 메커니즘
  - 실제 통신의 대한 처리가 아닌 탐지, 관리, 사후처리 등의 정의

보안 서비스

- 보안 서비스 (Security Service)
  - 처리 시스템, 데이터 전송의 보안을 보장하는 프로토콜 계층에 의해 제공되는 서비스, 실제 보안공격에 대응하기 위한 것
  - 특정 보안 메커니즘이 적용
  - 인증 서비스 (Authentication Service)
    - 인증 서비스는 통신이 검증 되었다는 것을 확인해주는 것
    - 대등 개체 인증 (Peer Entity Authentication)
      - 연결된 통신에서 통신하는 상대방의 신원을 확인시켜줌
      - 초기 연결 설정시에, 데이터 전송 과정 도중에 이 인증 서비스 사용
      - 신분위장, 이전연결에 사용한 메시지를 이용한 재전송 이 아님을 보장
    - 데이터 출처 인증 (Data Origin Authentication)
      - 비연결 통신에서 데이터 단위의 출처에 대한 확인
      - 데이터가 수정, 복제에 대한 방어는 없음
      - 상호 사전 연결협상이 필요 없는 곳에 응용 ex) 전자메일

보안 서비스

- 보안 서비스 (Security Service)
  - 접근제어 서비스 (Access Control Service)
    - 통신 링크를 통한 호스트 시스템과 응용 간의 접근을 제한하고 통제할 수 있는 능력
    - 접근 시도를 하는 각 개체에 대해 신원확인, 인증이 필요하고 그에 적합한 권한을 부여
    - 기밀성을 포함
  - 데이터 기밀성 서비스 (Data Confidentiality Service)
    - 기밀성(트래픽 흐름 보호)에 의해 공격자가 발신지, 목적지, 통신 빈도, 메시지 길이, 특성 등을 볼 수 없어야 함
    - 소극적 공격으로부터 보호를 의미
    - 보호 레벨이 여러 단계, 가장 광범위한 경우 특정 기간 동안 데이터 전송을 모두 보호하는 것
  - 데이터 무결성 서비스 (Data Integrity Service)
    - 메시지가 중간에 복제, 추가, 수정(파괴), 대치, 재전송 없이 그대로 전송됨을 보장
    - 적극적 공격으로부터의 보호를 의미
    - 메시지 스트림, 단일 메시지, 메시지 안의 선별된 필드에 적용
    - 스트림 전체 보호가 가장 유용하고 단순함 예방과 탐지를 의미
    - 복구 가능한 경우 사람, 소프트웨어가 관여 하게 됨, 자동화된 복구 메커니즘이 가장 많이 이용 됨

보안 서비스

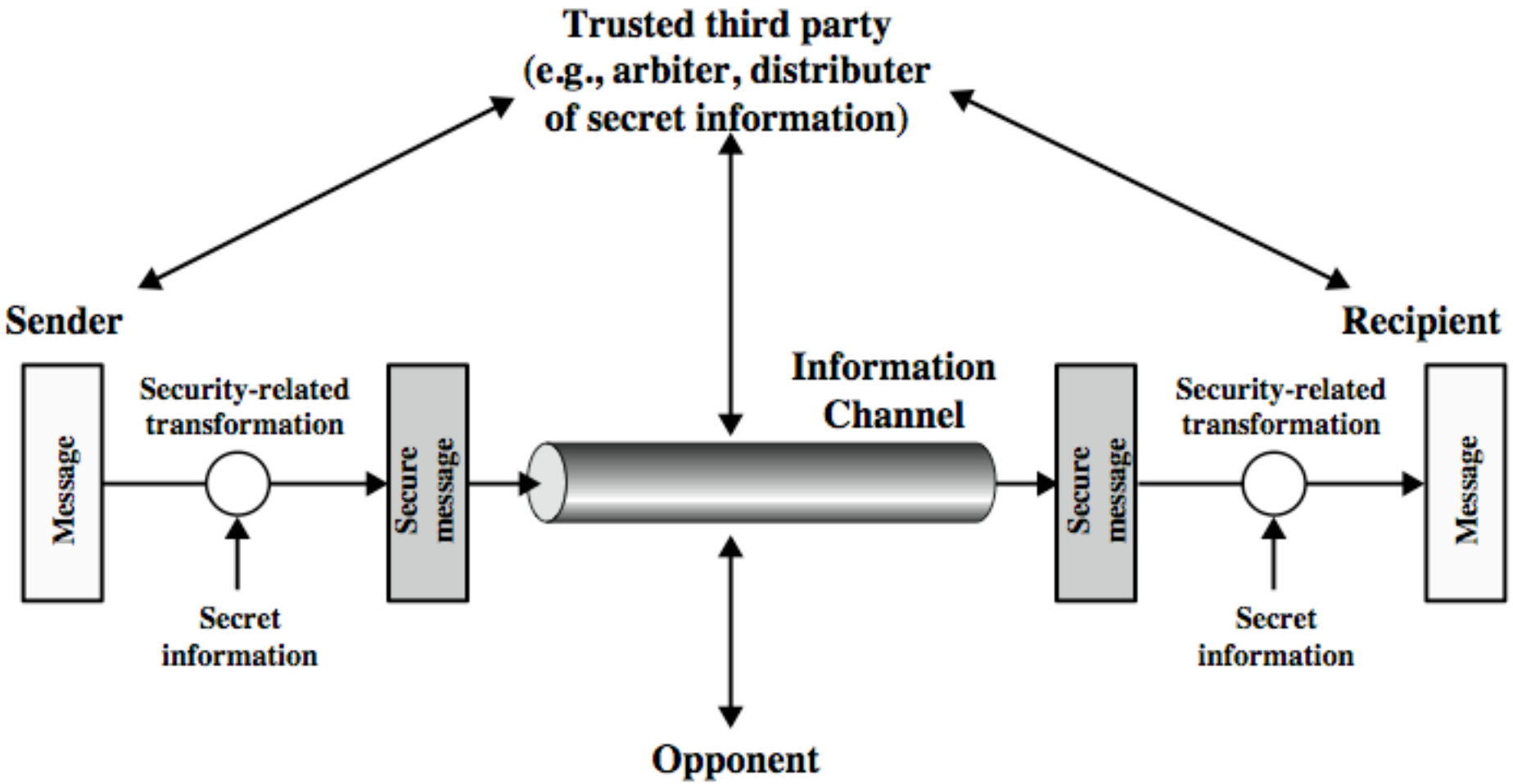
- 보안 서비스 (Security Service)
  - 부인 봉쇄 서비스 (Non-Repudiation Service)
    - 송신자, 수신자 양측이 메시지를 전송한 사실 자체를 부인하지 못하도록 막는 것
    - 메시지가 송신 되었을 때 수신자는 메시지가 실제 송신자 라고 주장하는 주체로부터 송신 되었음을 확신
    - 메시지가 수신 되었을 때 송신자는 메시지가 실제 수신자 라고 주장하는 수신자 에게 수신 되었음을 확신
  - 가용성 서비스 (Availability Service)
    - 시스템이 자원에 접근, 사용 요구를 시스템의 성능에 적합하게 서비스를 처리할 수 있는 것
    - 다양한 형태의 공격에 의해 가용성이 떨어지거나 손실될 수 있음

보안 서비스

- **보안 메커니즘과 서비스**

서비스	메커니즘							
	암호화	디지털 서명	접근제어	데이터 무결성	인증 교환	트래픽 패딩	라우팅 제어	공증
대등 개체인증	Y	Y			Y			
데이터 출처 인증	Y	Y						
접근 제어			Y					
기밀성	Y						Y	
트래픽 흐름 기밀성	Y					Y	Y	
데이터 무결성	Y	Y		Y				
부인 봉쇄		Y		Y				Y
가용성				Y	Y			

Model for Network Security



네트워크 보안 모델

- **네트워크 보안 모델(Network Security Model)**
  - 인터넷에서 메시지 전송시 통신주체(Principals)의 양쪽은 상호 교환을 위한 협조가 필요
  - 송신자에서 수신자까지 통과하는 인터넷의 경로를 정의
  - 각 통신주체는 통신 프로토콜(TCP/IP) 을 사용하기로 협의, 논리적 정보 채널을 구성

  - **모든 보안 기술의 성질**
    - 보안을 위한 전송될 정보 암호화, 신원 확인을 위한 코드를 메시지에 첨부
    - 각 주체는 비밀정보를 공유함
    - 변환, 복구에 사용하는 암호키를 의미

  - **안전한 전송을 위해 신뢰할 수 있는 제 3자가 필요한 경우**
    - 보안을 위한 암호화를 수행하는 알고리즘 설계 (공격자가 깰수 없어야함)
    - 알고리즘에 사용될 비밀 정보를 생성
    - 비밀정보를 안전하게 공유, 배분할 방법 개발
    - 보안 서비스에서 사용할 양쪽 통신주체의 프로토콜을 결정

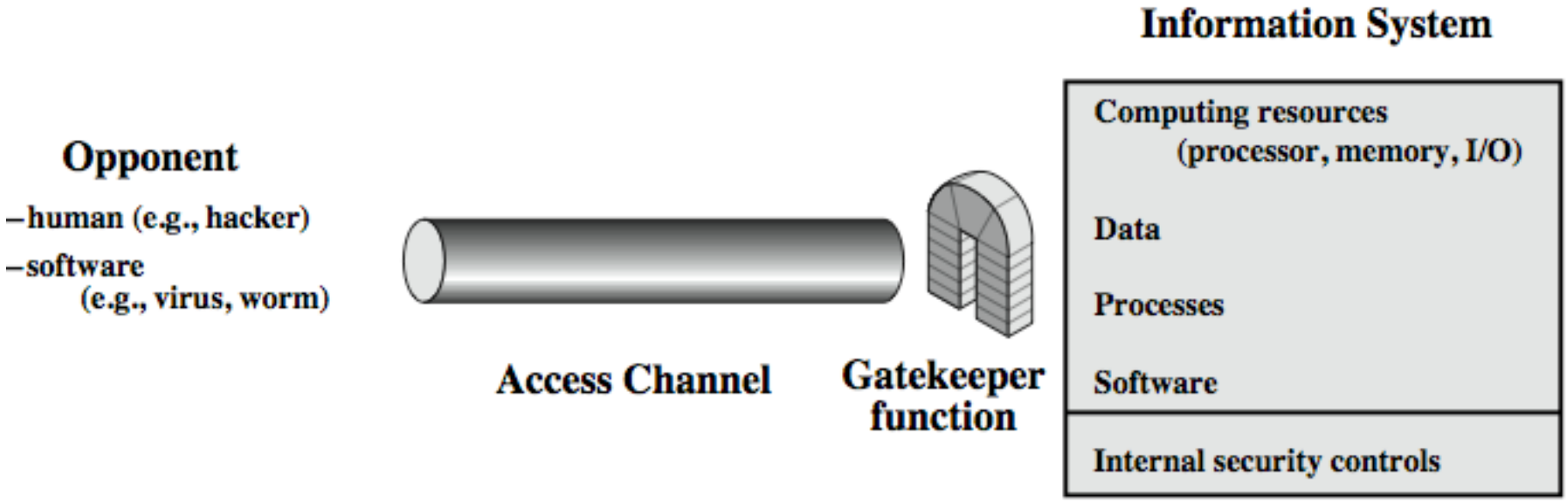
네트워크 보안 모델

- 네트워크 접근 보안 (Network Access Security)
  - 해커 (Hacker)
    - 시스템을 깰 수 있다는 자기만족을 위해 침입하는 공격자
  - 침입자 (Intruder)
    - 손해를 끼칠 의도가 있는 공격자
  - 정보 접근 위협 (Information Access Threats)
    - 특정 사용자에게 접근이 불허된 데이터를 가로채거나 수정해서 그 사용자 자신에게 유리하도록 만드는 위협
  - 서비스 위협 (Service Threats)
    - 합법적인 사용자가 이용하는 것을 방해하기 위해 컴퓨터 서비스의 결함을 악용하는 행위

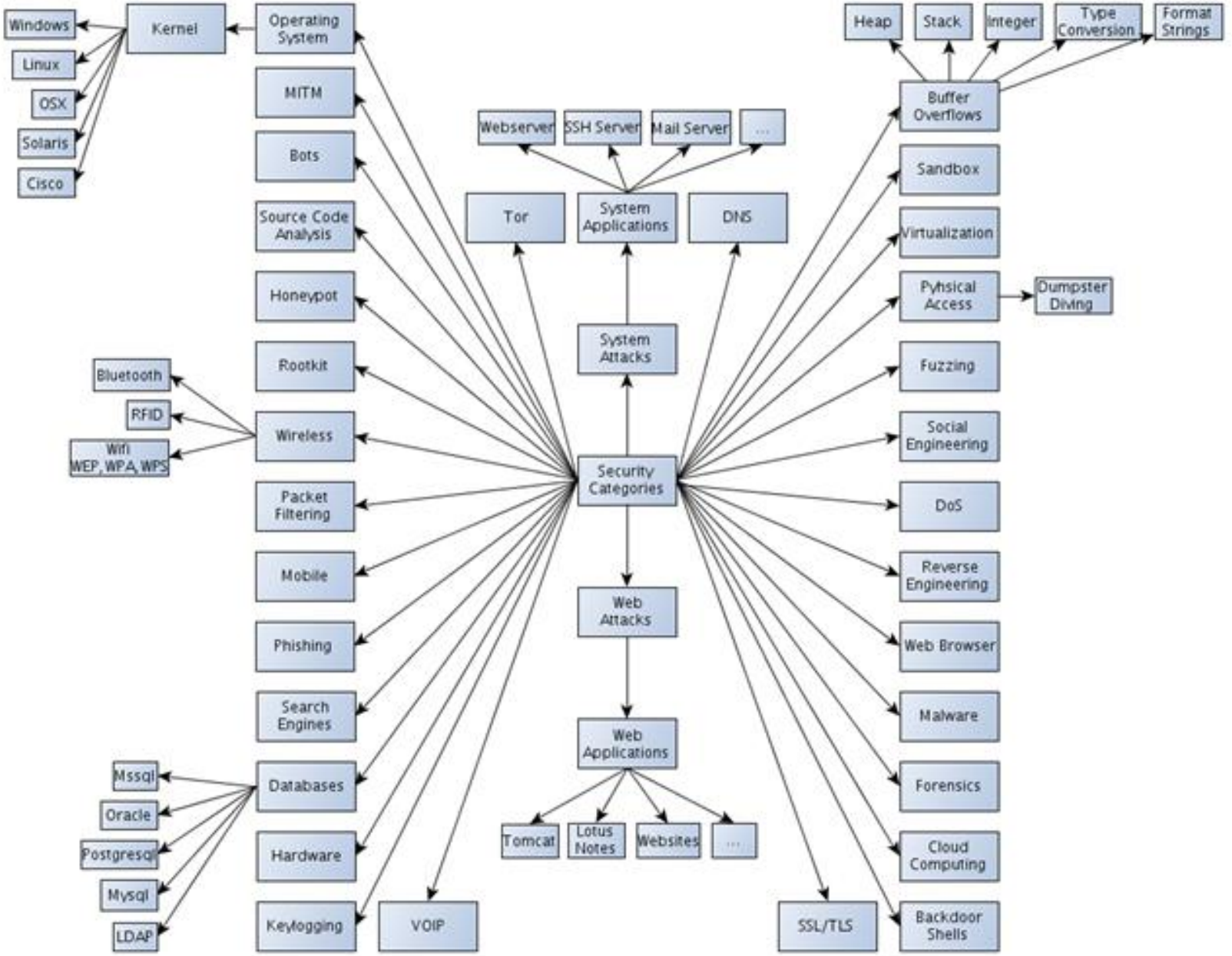
네트워크 보안 모델

- **네트워크 접근 보안 (Network Access Security)**
  - **소프트웨어 공격의 대표적인 사례**
    - 악성 로직이 잠복된 시스템 공격, 네트워크를 통해 전염 될 수 있음
    - 바이러스 (Virus)
      - » 악의적 목적을 가진 스스로를 복제하는 악성 소프트웨어, 프로그램에 기생함
    - 웜 (Worm)
      - » 악의적 목적을 가진 스스로를 복제하는 악성 소프트웨어, 독자적으로 실행 됨, 복사본을 네트워크로 전송
  - **불법 침입 문제의 보안 방법**
    1. 게이트 키퍼 (Gate Keeper)
       - » 패스워드 로그인 과정을 이용해서 인가받지 않은 사용자, 악성 소프트웨어를 탐지하여 제거
    2. 모니터링 (Monitoring)
       - » 1차적으로 인가받지 못한 사용자, 악성 소프트웨어차단
       - » 2차적으로 침입자 탐지를 위해 컴퓨터 동작 모니터링, 저장된 정보분석 등의 내부적 제어 수행

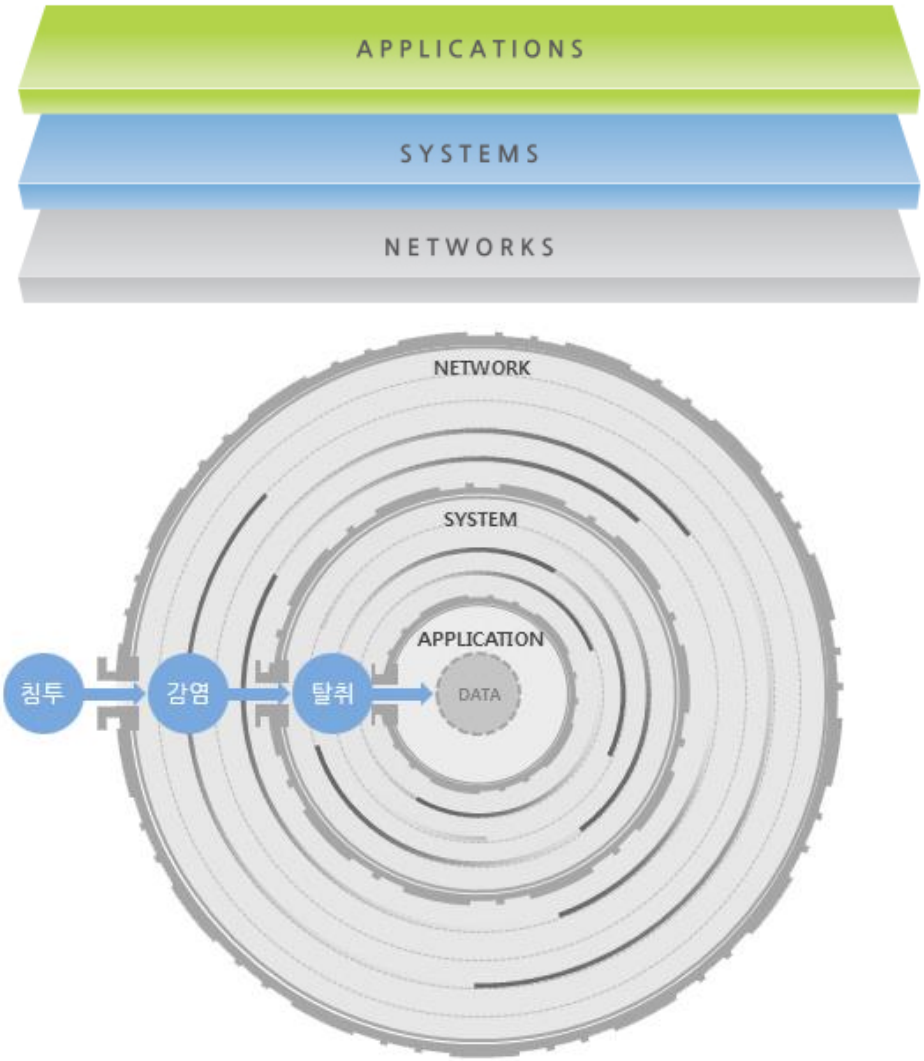
Model for Network Access Security



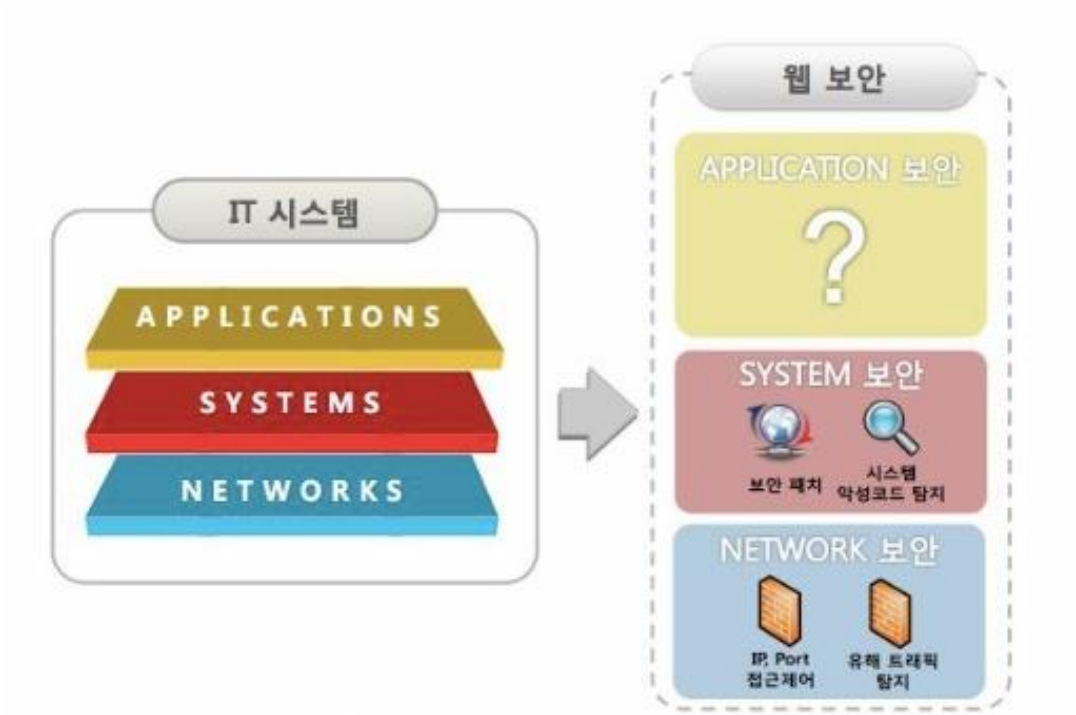
Security 분류


Windows
Linux
OSX
Solaris
Cisco
Kernel
Operating System
MITM
Bots
Source Code Analysis
Honeypot
Rootkit
Bluetooth
RFID
Wifi WEP, WPA, WPS
Wireless
Packet Filtering
Mobile
Phishing
Search Engines
Mssql
Oracle
Postgresql
Mysql
LDAP
Databases
Hardware
Keylogging
VOIP
Webserver
SSH Server
Mail Server
...
Tor
System Applications
DNS
System Attacks
Security Categories
Web Attacks
Web Applications
Tomcat
Lotus Notes
Websites
...
Heap
Stack
Integer
Type Conversion
Format Strings
Buffer Overflows
Sandbox
Virtualization
Pyhsical Access
Dumpster Diving
Fuzzing
Social Engineering
DoS
Reverse Engineering
Web Browser
Malware
Forensics
Cloud Computing
Backdoor Shells
SSL/TLS

IT 시스템 구조


APPLICATIONS
SYSTEMS
NETWORKS
NETWORK
SYSTEM
APPLICATION
DATA
침투
감염
탈취

IT 시스템의 각 계층별 보안



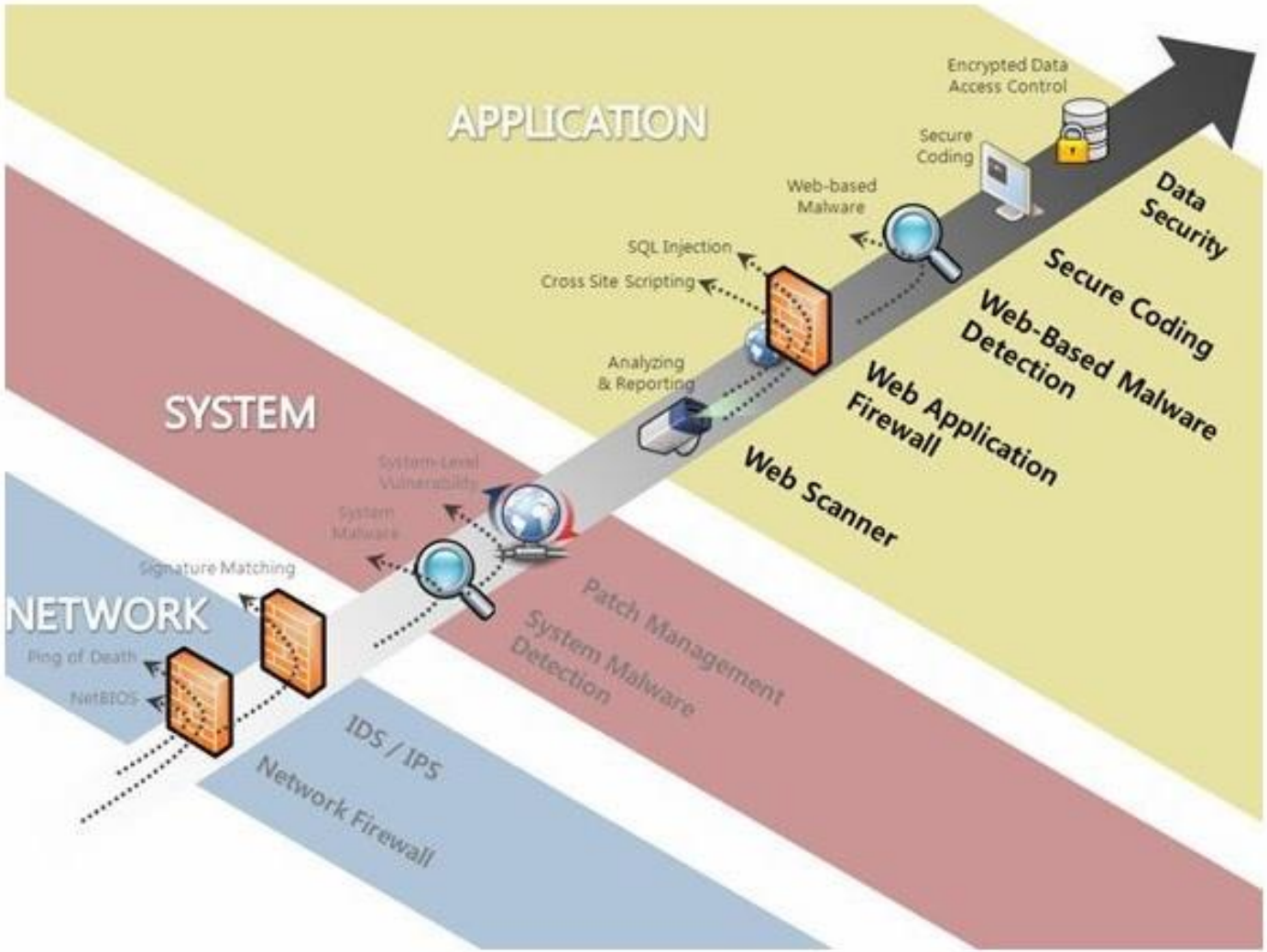
IT 시스템 구조 각 계층별 웹 보안

웹 어플리케이션 보안

웹 애플리케이션 보안 솔루션 모식도

(웹 애플리케이션은 크게 "웹 애플리케이션 서버" 와 "DB"로 구성됩니다)

계층별 보안 솔루션



웹 보안 3계층과 계층 별 보안 솔루션

Q & A

참고문헌

- 네트워크보안 에센셜, William Stallings
- http://resources.infosecinstitute.com/security-categories
- 펜타씨큐리티, https://www.pentasecurity.com
- http://ensxoddl.tistory.com/m/255