TOPCIT 학습법 특강: 정보보안 이해와 활용

Sep 25, 2024

Myoungsung You (famous77@kaist.ac.kr)

Network and System Security (NS^2) Lab

School of Electrical Engineering at KAIST

NS2 Network and System Security Laboratory KAIST

Index

강사 소개

유명성, Myoungsung You

famous77@kaist.ac.kr

- KAIST 전기및전자공학부 박사과정
- KAIST 전산학부 석사과정 졸업
- **Awards and honors**: 과기부/행안부/교육부 장관상 등 수상 경력 다수 보유
- **Research interests**: Cloud Computing, Programmable Data Plane, and Network Security
- **Recent publications**:
- (ICDCS 24) HardWhale: A Hardware-isolated Network Security Enforcement System for Cloud Environments
- (SoCC 23) HELIOS: Hardware-assisted High-performance Security Extension for Cloud Networking
- (SoCC 23) Cryonics: Trustworthy Function-as-a-Service using Snapshot-based Enclaves
- (ICNP 22) MECaNIC: SmartNIC to Assist URLLC Processing in Multi-Access Edge Computing Platforms

1. TOPCIT 이란?

2. 정보보안 이해와 활용 영역 학습 방법

정보보안 이해와 활용 영역 학습 방법

영역의 평가 목적 및 특징

- **평가 목적**: 안전한 소프트웨어의 개발에 필요한 정보보안 지식을 이해하고 활용할 수 있는 능력
- **특징**: 시스템 영역보다 더 어려운 개념이 가장 많이 등장
- **문항 수**: 8, **배점**: 85점
- **평가 문항**
  - 정보보안의 개념
  - 애플리케이션 보안
  - 데이터 보안
  - 시스템 아키텍처 보안
  - 보안 위협 및 대응 기술

정보보안 이해와 활용 영역 학습 방법

빈출 개념

- 정보보안 개요
  - 정보보안의 기본 개념과 목표
  - 정보보안 3요소 (CIA)
- 암호 기술
  - 대칭키 암호와 비대칭키 암호
  - 해시 함수와 전자서명
  - PKI (공개키 기반구조) 시스템
- 시스템 보안
  - 운영체제 보안
  - 접근제어 메커니즘

정보보안 이해와 활용 영역 학습 방법

빈출 개념

- 네트워크 보안
  - 방화벽, IDS/IPS의 이해와 구성
  - VPN (가상사설망)의 개념과 구현
  - 무선 네트워크 보안
- 애플리케이션 보안
  - 웹 애플리케이션 보안 취약점과 대응책
- 정보보호관리체계와 표준
  - 정보보호관리체계 (ISMS) 이해
- 사이버 공격과 대응
  - 주요 사이버 공격 유형 (DDoS, APT, 랜섬웨어)

정보보안 이해와 활용 영역 학습 방법

- 영역의 평가 목적 및 특징

Computer 및 software 공학에 대한 이해도를 기본으로 하는 영역

정보보안 이해와 활용 영역 학습 방법

실무에서의 정보보안 이해와 활용 영역

합류하면 함께 할 업무예요

- 토스의 인프라에 대한 모의 해킹 및 APT 공격을 수행하고, 인프라 시스템 진단을 수행해요.
- 전자금융기반시설 기반의 기
- 새로운 해킹 공격 기법 및 방

이런 분과 함께하고 싶어요

- 다양한 IT 인프라 아키텍쳐
- 정보보안 솔루션/인프라에
- 웹/네트워크 취약점에 대한
- 기술적 취약점 진단 절차를

담당업무

- (개인)정보보안 관리체계 수립 및 운영
- (개인)정보보안 관련 사내 컴플라이언스 검토 및 임직원 보안 가이드
- 내 · 외부 IT 및 위탁사 정보보안 감사 대응
- 글로벌 핀테크 및 (개인)정보보호 법 체계 분석
- 정보보안 솔루션 정책 관리 및 보안 교육

자격요건

- 5년 이상의 (개인)정보보안 정책 및 체계 수립/운영 실무 경력이 있는 분
- 정보보안 관련 인증 혹은 감사 대응 경험이 있는 분 (ISMS, ISO27001 등)
- 해외 출장 및 근무에 결격사유가 없는 분

합류하면 함께 할 업무예요

- 토스의 고객 서비스와 임직원의 업무환경을 보호하기 위한 정보보안솔루션을 구축하고 운영하는 업무를 수행해요.
- 토스커뮤니티의 정보시스템(DB, Server, Network 등)을 보호하기 위한 접근 통제 방안을 마련하여, 보안솔루션의 구축 및 운영, 관리 업무를 수행해요.
- 금융 컴플라이언스에 따른 망분리환경 및 정보 유출 대응 체계 구축에 필요한 보안 시스템(망연계, 데이터 유출 방지 등)의 구축 및 운영 관리 업무를 수행해요.
- 안전한 토스팀의 업무 환경 구성을 위한 보안 가시성 확보 및 보안 관리 및 접근 체계를 개선하고 연구하는 업무를 수행해요.

이런 분과 함께하고 싶어요

- FW, NAC, Proxy 과 같은 네트워크 보안 시스템 구축, 운영 및 인프라 아키텍처 설계 경험을 가진 분이 필요해요.
- SAC, DAC 을 통한 서버 및 데이터 베이스 접근 제어 모델 설계 및 통제 솔루션 구축 및 운영 경험을 가진 분이 필요해요.
- Cloud (IasS - AWS, Azure, Openstack 등 / SaaS - Google Workspace, M365 등) 기반의 인프라 및 서비스 구축과 운영, 보안 관리 경험을 가진 분이 필요해요.
- IAM 및 SSO 관련 시스템 (OKTA, KeyCloak 등) 구축, 운영 및 권한 관리 체계를 설계하고 적용해 보신 경험을 가진 분이 필요해요.
- MS Intune, Workspace One, Jamf 등의 사용자 클라이언트에 대한 식별과 관리를 위한 UEM 시스템을 운영해 보거나 구축해 보신 분들이면 더욱 좋아요.

3. 정보보안 이해와 활용 영역 주요 개념

정보보안 기본 개념

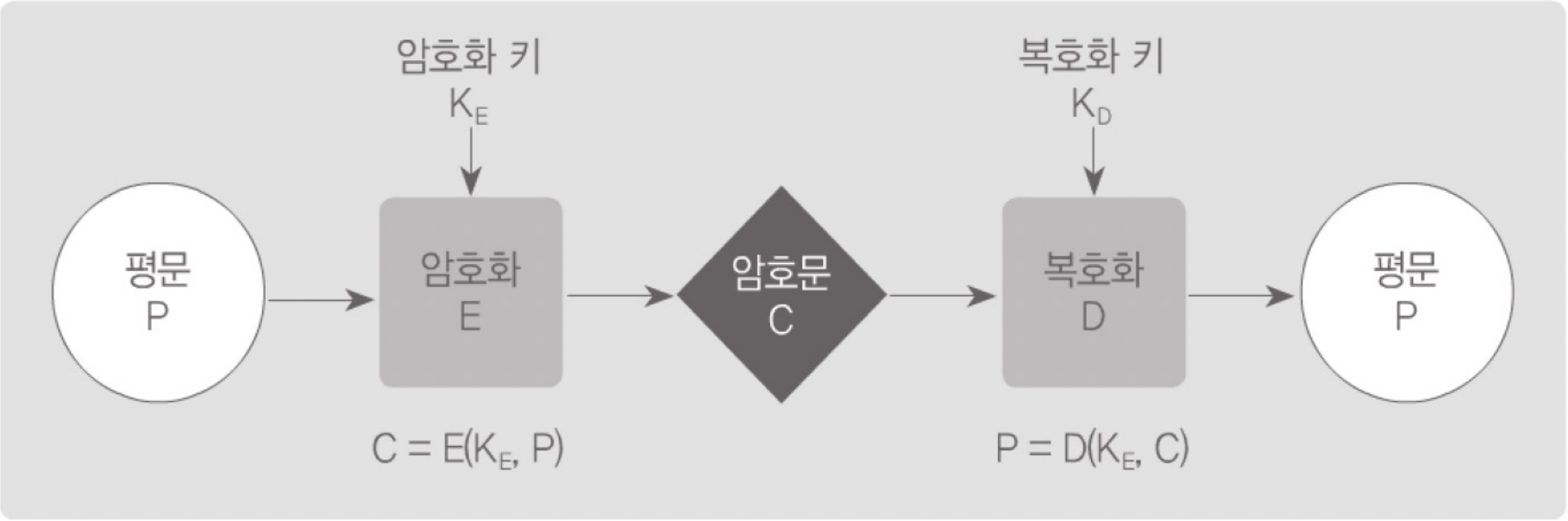
정보보안의 3요소 (CIA)

- Confidentiality (기밀성): 허가되지 않은 자가 정보에 접근할 수 없게 하는 것
- Integrity (무결성): 인가된 사용자가 인가된 방법으로만 정보를 변경할 수 있게 하는 것
- Availability (가용성): 허가된 자가 정보에 접근하려 할 때 방해가 없도록 하는 것

정보보안 기본 개념

암호 알고리즘

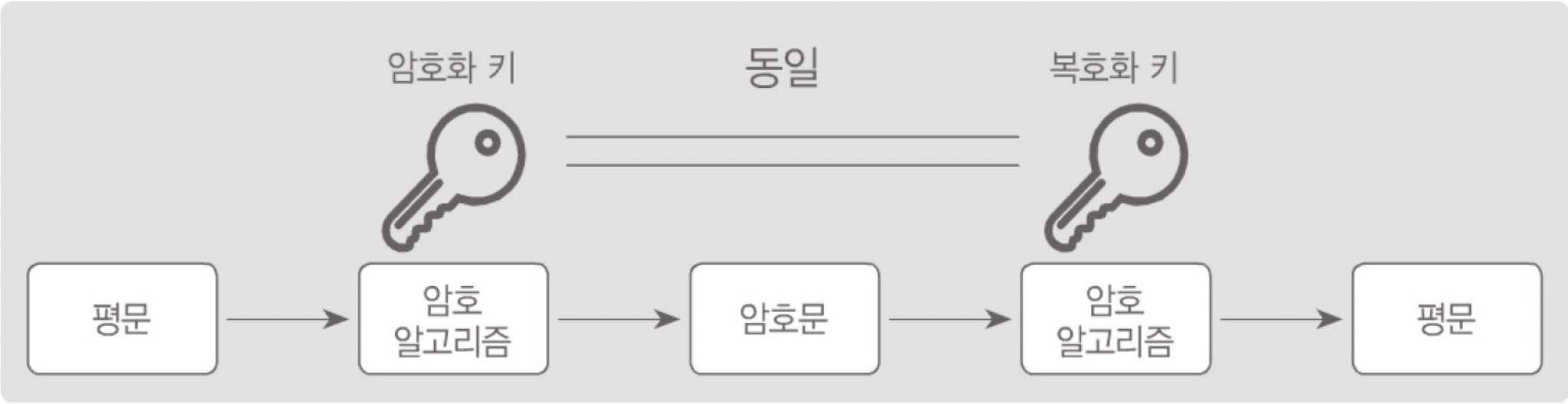
- 암호 키를 사용해 데이터를 제 3자가 볼 수 없도록 암호화 하는 알고리즘
- 평문을 *암호화 키*로 암호화하여 암호문을 생성, 암호문을 *복호화 키*로 복호화해 평문 복원 가능



정보보안 기본 개념

대칭키(비밀키) 암호화

- 암호화와 복호화에 사용하는 키가 동일한 알고리즘
- 키 길이가 짧아도 되며 연산속도가 빠름



정보보안 기본 개념

대칭키(비밀키) 암호화

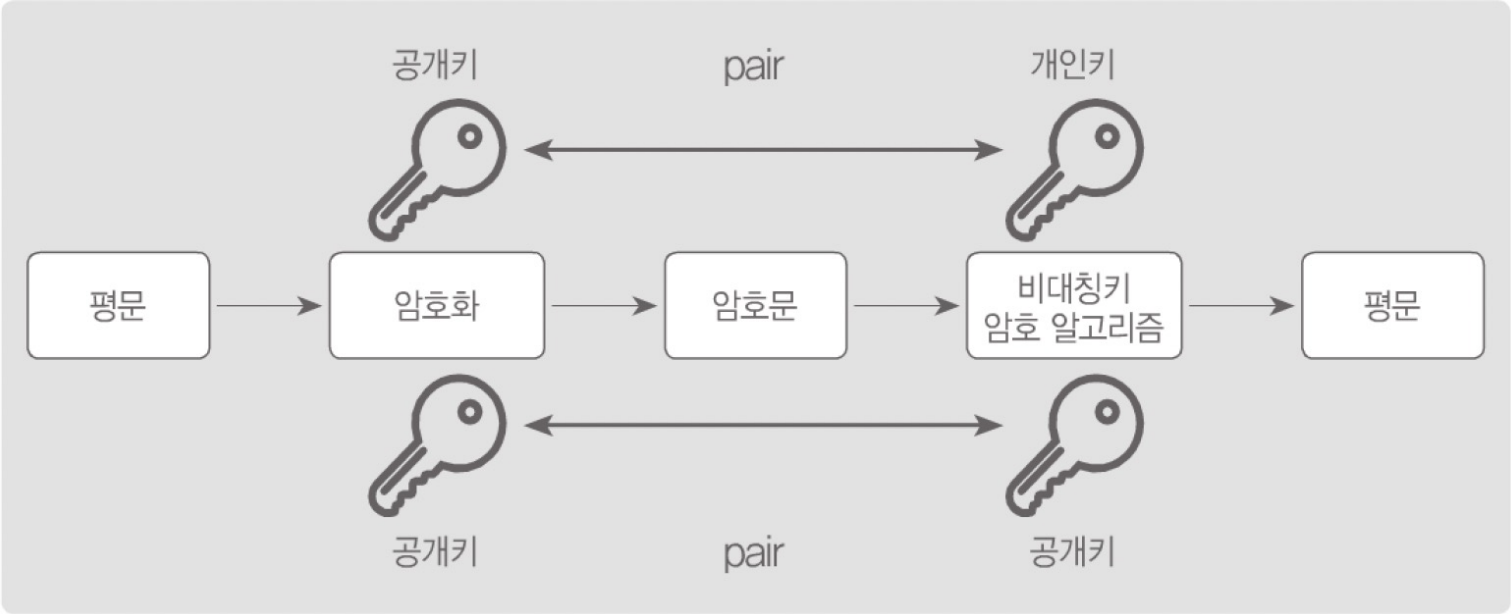
- 평문 데이터 처리 방식에 따라 ‘스트림 암호’와 ‘블록 암호’로 구분됨

구분	블록 암호	스트림 암호
동작방식	평문을 블록이라는 고정된 길이로 나누고 블록 단위로 암호화 진행	평문을 비트 단위로 암호화 수행
장점	구현이 용이	오류 확산 위험이 낮음, 이동통신 환경에서 구현 용이
단점	오류 확산 위험이 높음, 초기값 설정 필요	느린 수행 시간, 공격자의 공격에 취약
알고리즘	DES, AES, SEED, ARIA	RC4

정보보안 기본 개념

비대칭키(공개키) 암호화

- 암호화와 복호화에 사용하는 키가 다른 암호 알고리즘 (RSA, ElGamal, ECC)
- 송신자는 수신자의 공개키로 평문을 암호화하여 전송하고 수신자는 자신의 개인키로 평문을 복호화



정보보안 기본 개념

비대칭키(공개키) 암호화

- 공개키 암호화는 다른 사람들과 키를 공유하지 않아도 됨
  - 개인키는 안전하게 보관하고 공개키는 모두에게 공개하여 사용
  - 특정 유저의 공개키로 암호화된 내용은 해당 유저의 개인키로만 복호화 가능
- 암호화뿐 아니라 전자서명에도 활용됨
  - 특정 유저의 개인키로 암호화된 내용은 해당 유저의 공개키로만 복호화 가능

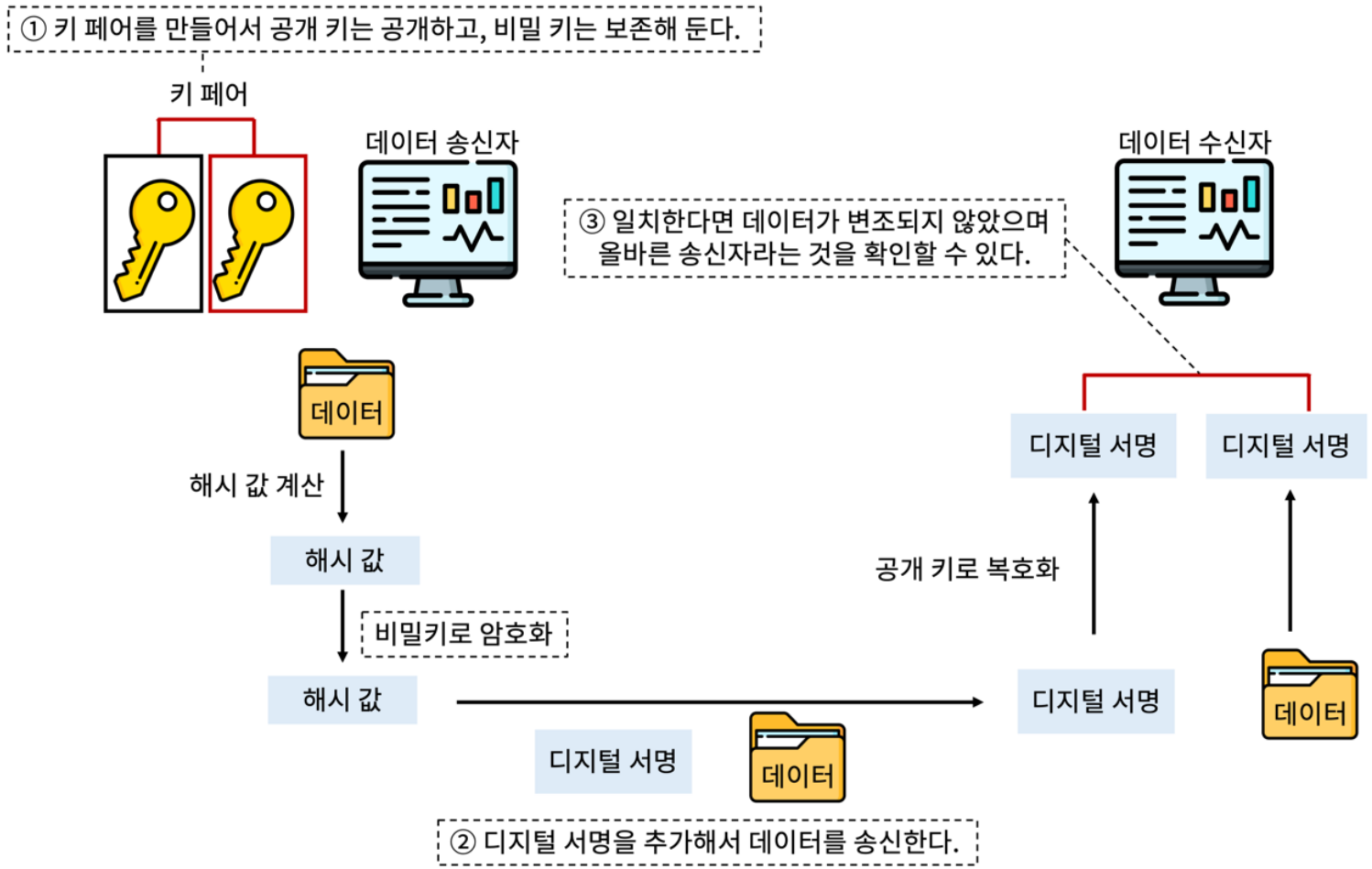
정보보안 기본 개념

전자 서명

- 네트워크를 통해 전달되는 문서에 대한 인증, 무결성, 부인 방지 제공
- 전자서명은 문서가 신원이 확인된 서명자에 의해 생성되었으며, 송수신 과정에서 문서의 내용이 수정되거나 조작되지 않았음을 증명함
- 문서 작성자의 개인키로 문서를 서명하여 전송하고, 수신자는 작성자의 공개키를 사용해 이를 검증

정보보안 기본 개념

전자 서명



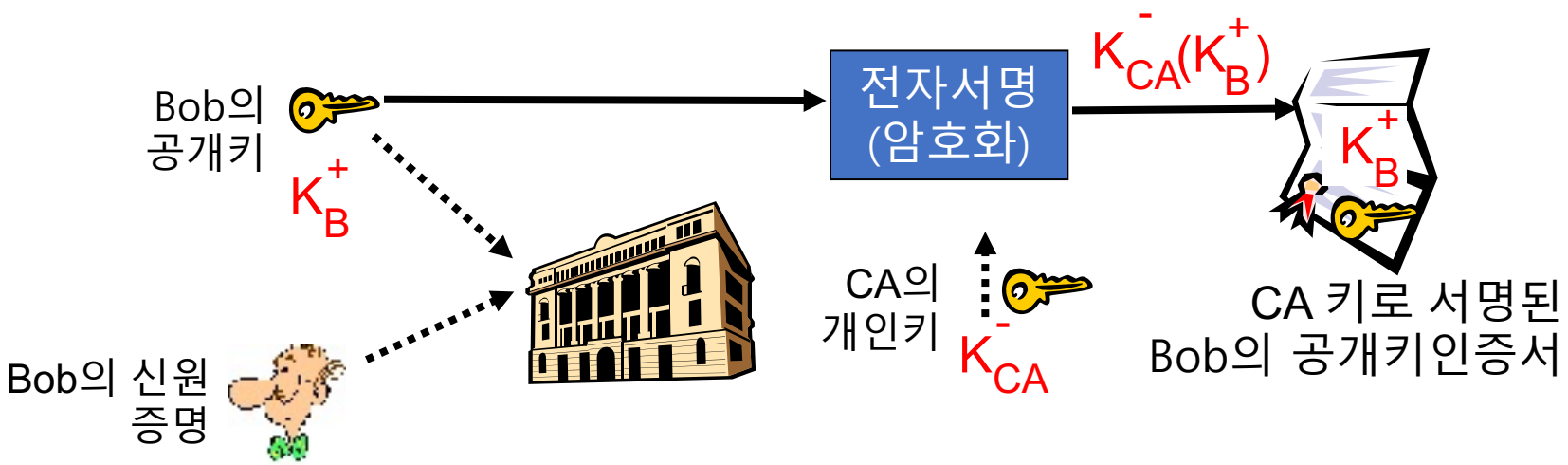
공개키 구조 (Public Key Infrastructure, PKI)

- 공개키의 문제점
  - Alice가 Bob의 공개키를 제 3의 경로에서 획득했을 때 (웹 사이트, 메일 등에서) 이것이 Bob의 공개키가 맞는지 확인할 수 없음
- 해결책
  - 신뢰할 수 있는 인증 기관(certification authority)에 공개키를 등록해서 사용

정보보안 기본 개념

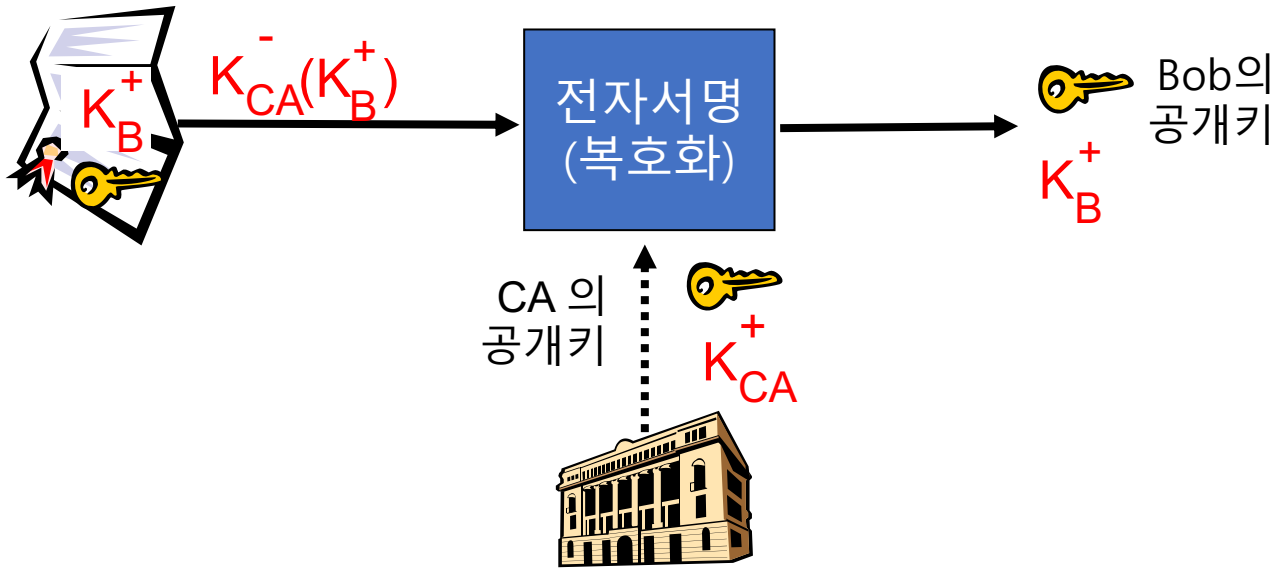
공개키 구조 (Public Key Infrastructure, PKI)

- 인증기관 (Certification Authority, CA): 특정 사용자와 공개키를 매핑하여 관리
- 사용자는 자신의 신원을 증명하고 공개키를 CA에 등록
- CA는 자신의 개인키로 사용자의 공개키에 서명하여 공개키 인증서 생성
- 추후 사용자의 공개키를 검증할 때 공개키 인증서를 활용



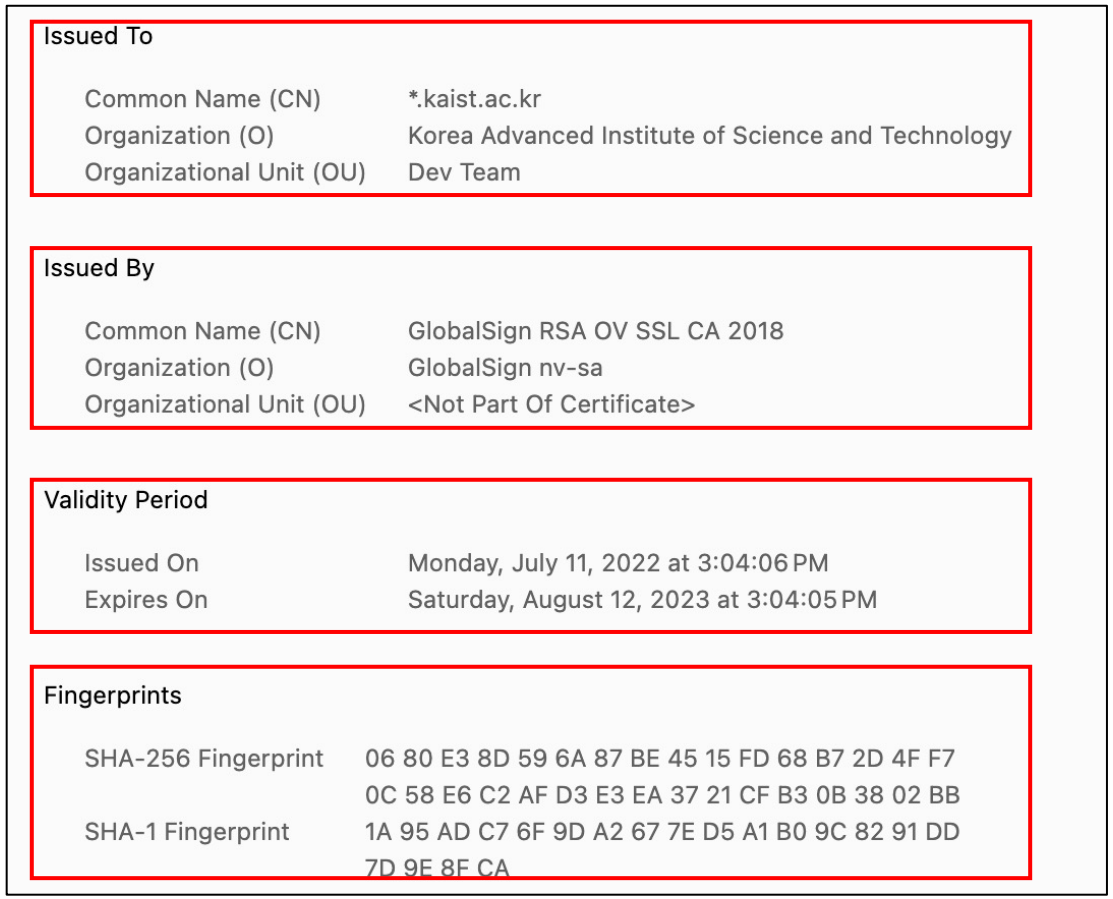
공개키 인증서 검증 과정

- Alice가 Bob의 공개키를 원할 때
  - Bob의 인증서를 받아 옴
  - CA의 공개키로 Bob의 인증서를 검증한 뒤 (복호화) Bob의 공개키를 얻음



정보보안 기본 개념

실제 공개키 인증서



Issued To

Common Name (CN)	*.kaist.ac.kr
Organization (O)	Korea Advanced Institute of Science and Technology
Organizational Unit (OU)	Dev Team

Issued By

Common Name (CN)	GlobalSign RSA OV SSL CA 2018
Organization (O)	GlobalSign nv-sa
Organizational Unit (OU)	<Not Part Of Certificate>

Validity Period

Issued On	Monday, July 11, 2022 at 3:04:06 PM
Expires On	Saturday, August 12, 2023 at 3:04:05 PM

Fingerprints

SHA-256 Fingerprint	06 80 E3 8D 59 6A 87 BE 45 15 FD 68 B7 2D 4F F7 0C 58 E6 C2 AF D3 E3 EA 37 21 CF B3 0B 38 02 BB
SHA-1 Fingerprint	1A 95 AD C7 6F 9D A2 67 7E D5 A1 B0 9C 82 91 DD 7D 9E 8F CA

인증서 소유자

인증서 발급자 (CA)

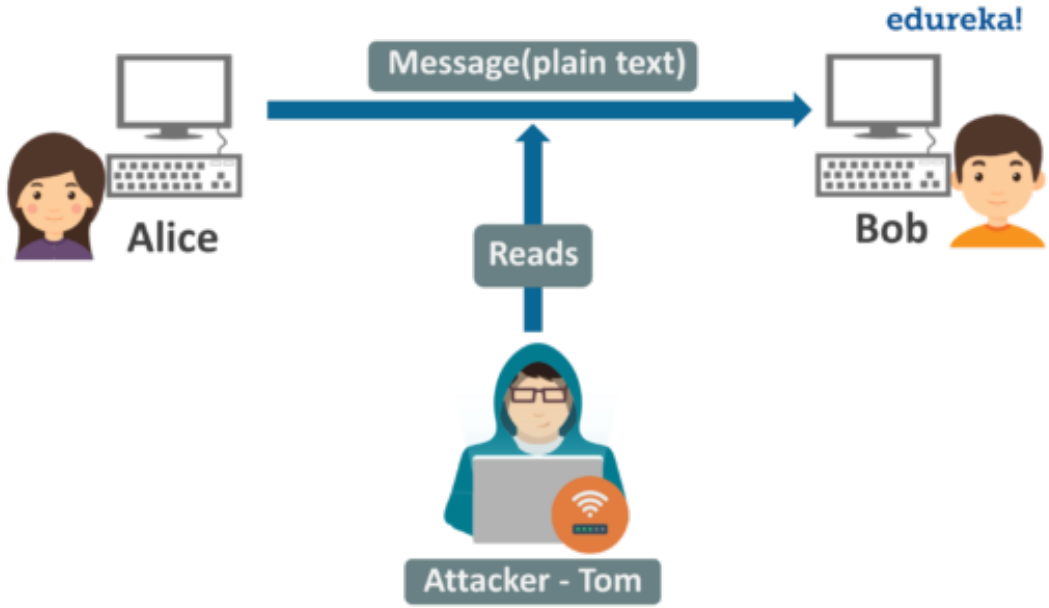
인증서 유효기간

CA의 전자서명

네트워크 보안

네트워크 보안의 정의

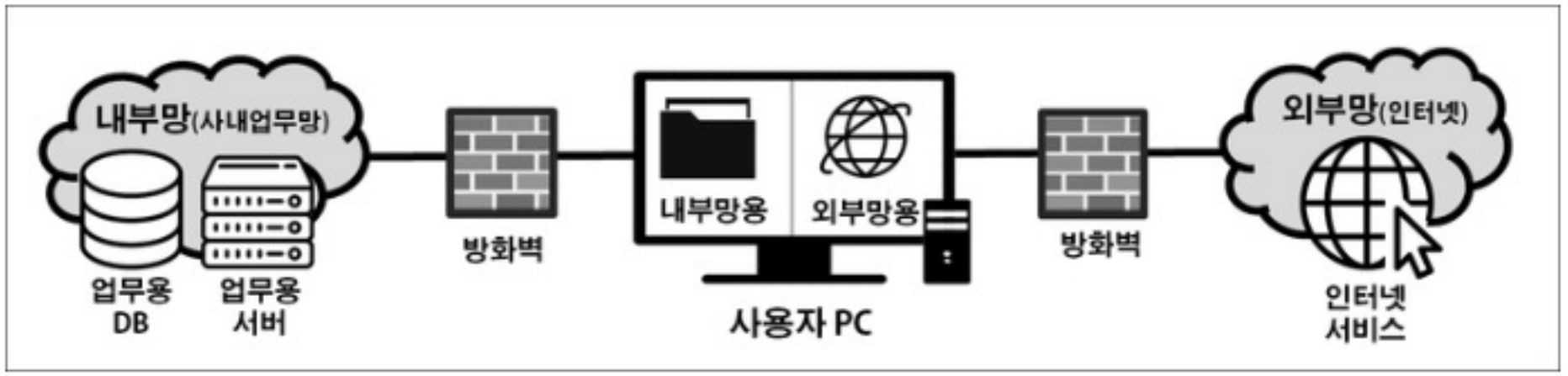
- 컴퓨터 네트워크(기업 네트워크 , 클라우드 네트워크 등)를 안전하게 유지하는 기술
- 네트워크 내 호스트의 통신에 대해 보안의 3요소 보장
- 관련 기술: 방화벽(firewall), 침입 방지 시스템(IDS), 침입 방지 시스템(IPS), 가상 사설망(VPN), 망 분리



네트워크 보안

네트워크 망 분리 (Network Segmentation)

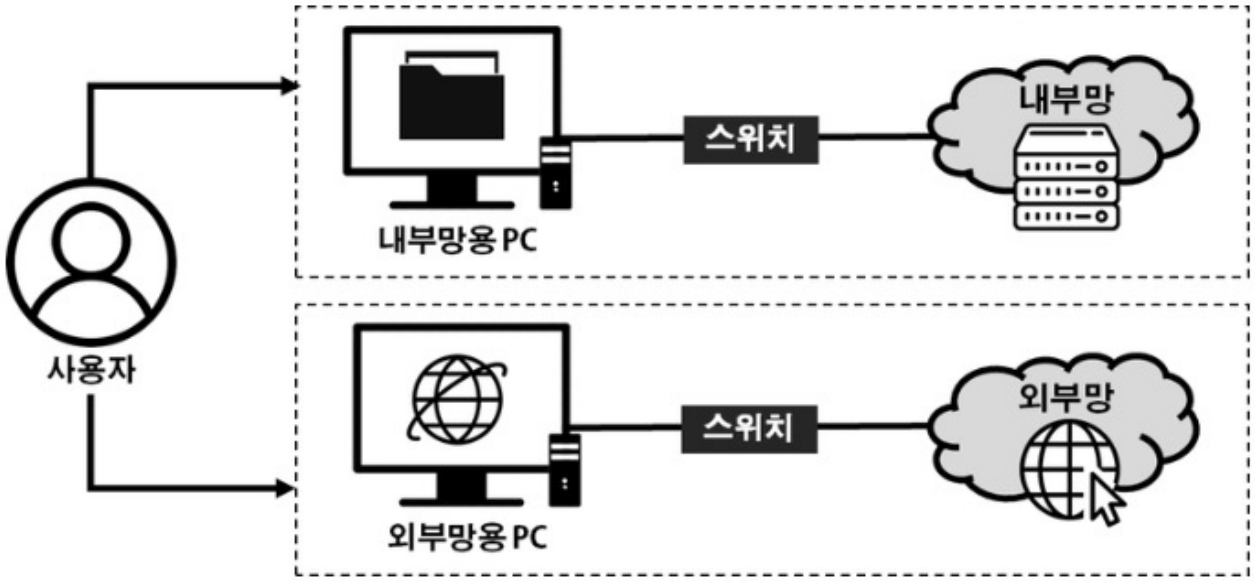
- 네트워크 내의 서로 다른 영역을 논리적으로 분리하는 보안 조치
  - 기업 네트워크에서 업무망 및 인터넷 망 분리
- 물리적 망 분리와 논리적 망 분리로 나뉨



네트워크 보안

물리적 망 분리

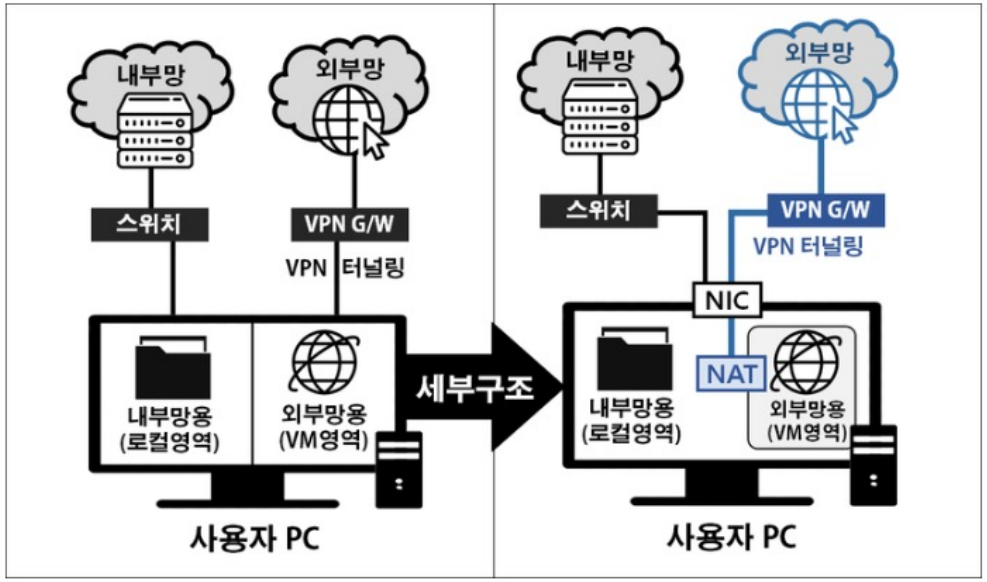
- 내/외부망에 각각 접속 가능 한 2대의 PC를 사용해 물리적으로 망을 분리



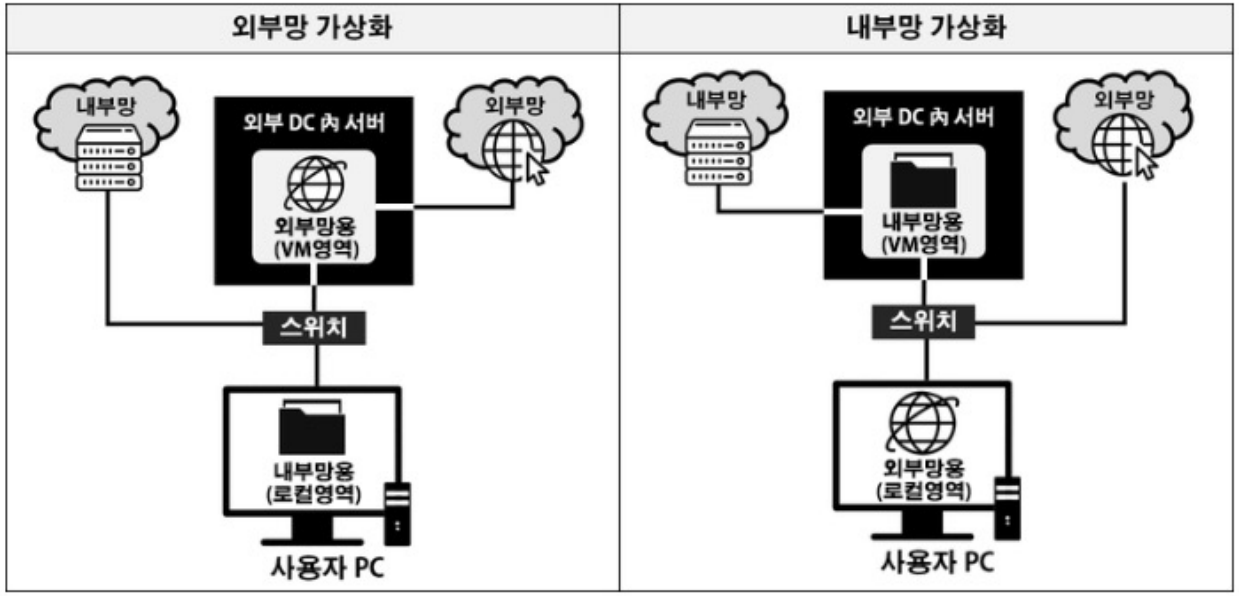
네트워크 보안

논리적 망 분리

- VM, VPN 등 가상화 기술을 사용해 하나의 PC에서 접속 가능한 네트워크를 논리적으로 분리



[Client-based computing]



[Server-based computing]

네트워크 보안

네트워크 공격

- DDoS 공격: 목표 시스템의 서비스를 마비 시킴
- 중간자 공격, Man-in-the-Middle attack: 목표 시스템의 통신을 네트워크 중간에서 조작
- 스니핑(sniffing) 공격: 목표 시스템의 통신을 네트워크 상에서 도청
- 스푸핑(spoofing) 공격: 다른 시스템으로 위장하여 목표 시스템과 통신

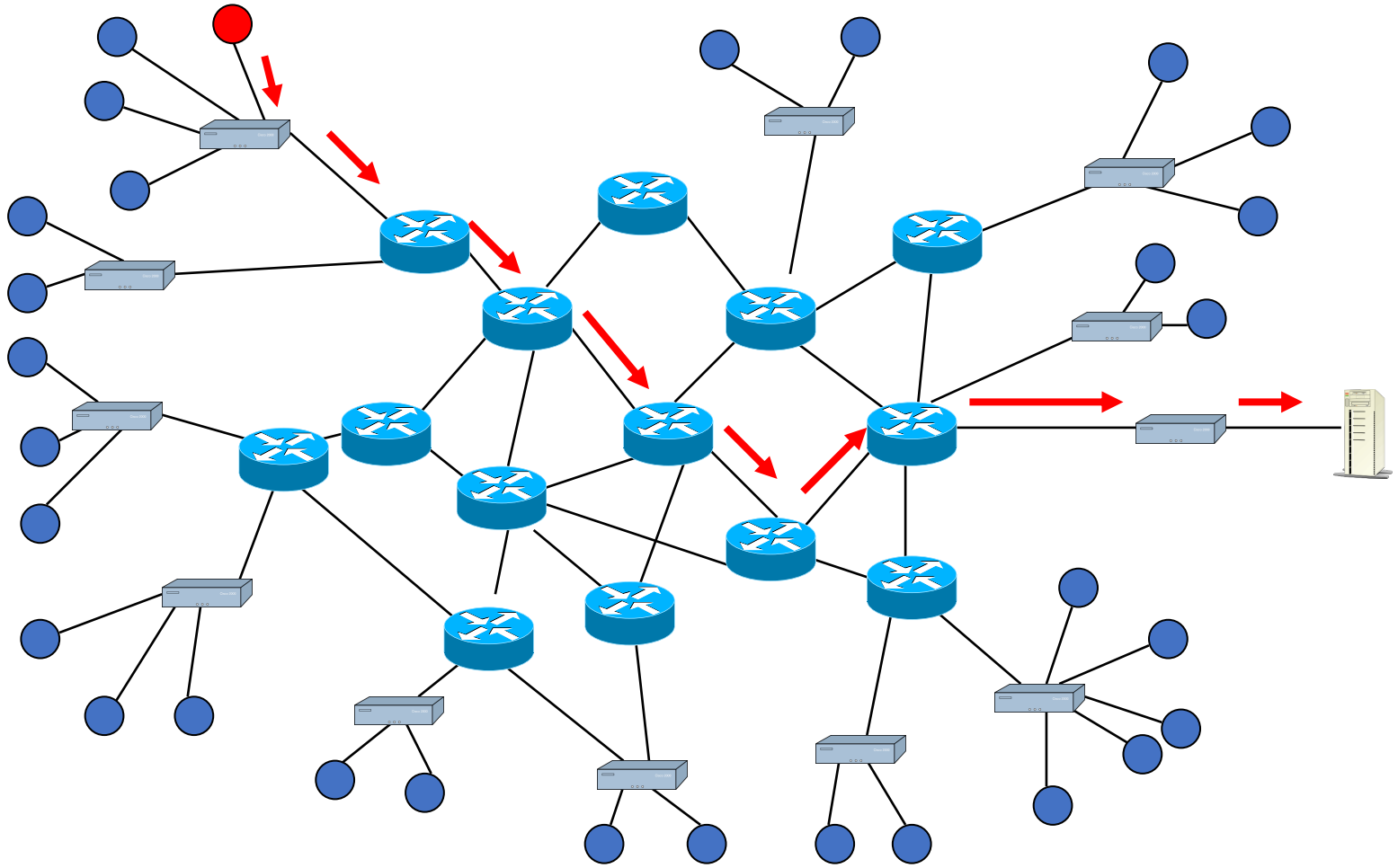
네트워크 보안

DoS and DDoS

- DoS (Denial of Service)
  - 특정 서버, 네트워크, 응용프로그램의 가용성을 침해하는 공격
- DDoS (Distributed Denial of Service)
  - 다수의 컴퓨터를 사용한 대규모의 DoS 공격

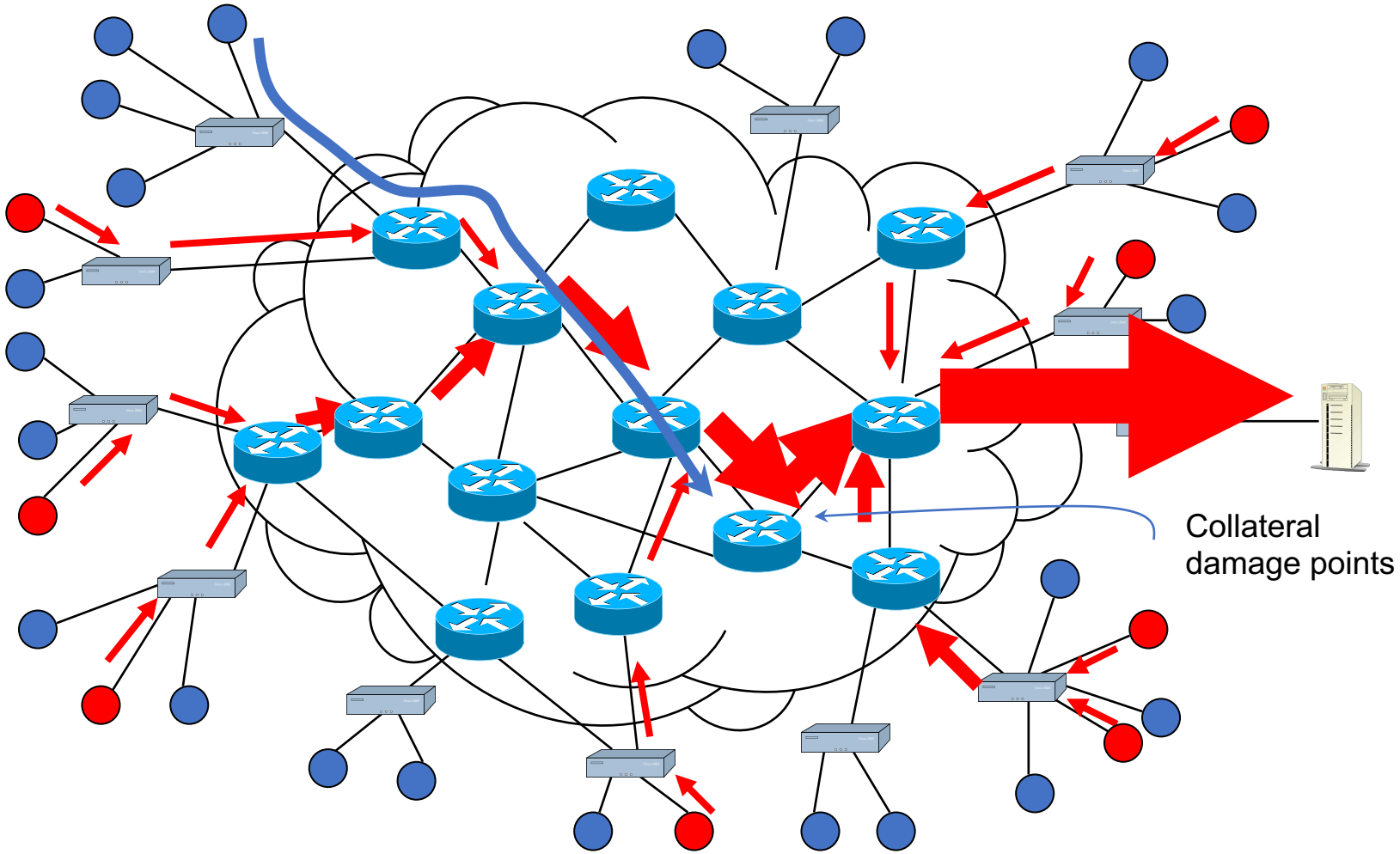
네트워크 보안

- DoS



네트워크 보안

- DDoS



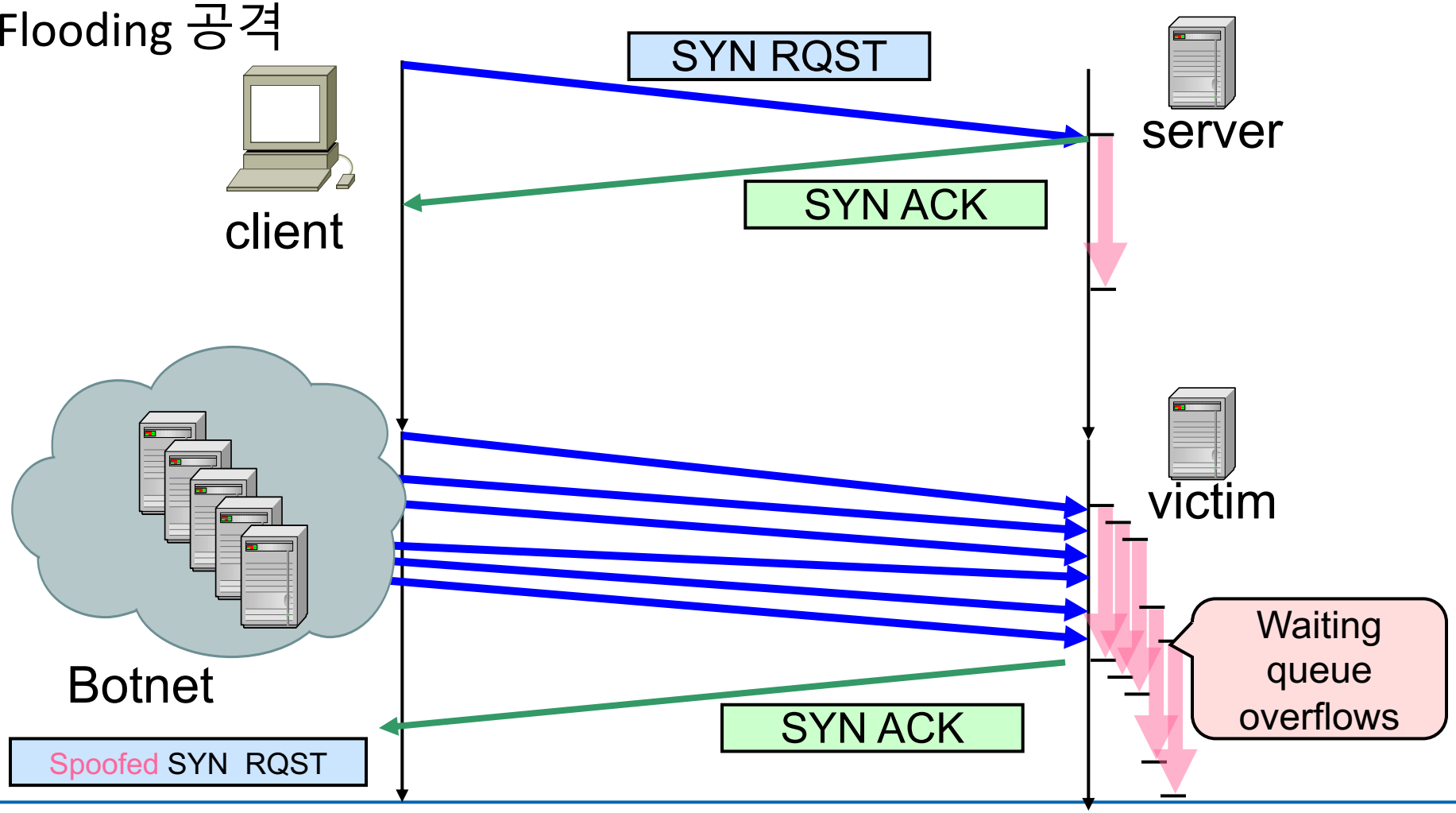
DDoS 공격의 종류

- 플러딩 공격(Flooding attack): 가장 일반적인 DDoS 공격으로 대용량의 패킷을 전송해서 공격
  - TCP SYN flooding
  - UDP flooding
  - ICMP flooding

- 증폭 공격(Amplification attack): 특정 프로토콜을 악용해 패킷의 크기를 증폭하여 공격
  - DNS amplification attack
  - NTP amplification attack

네트워크 보안

- TCP SYN Flooding 공격



네트워크 보안

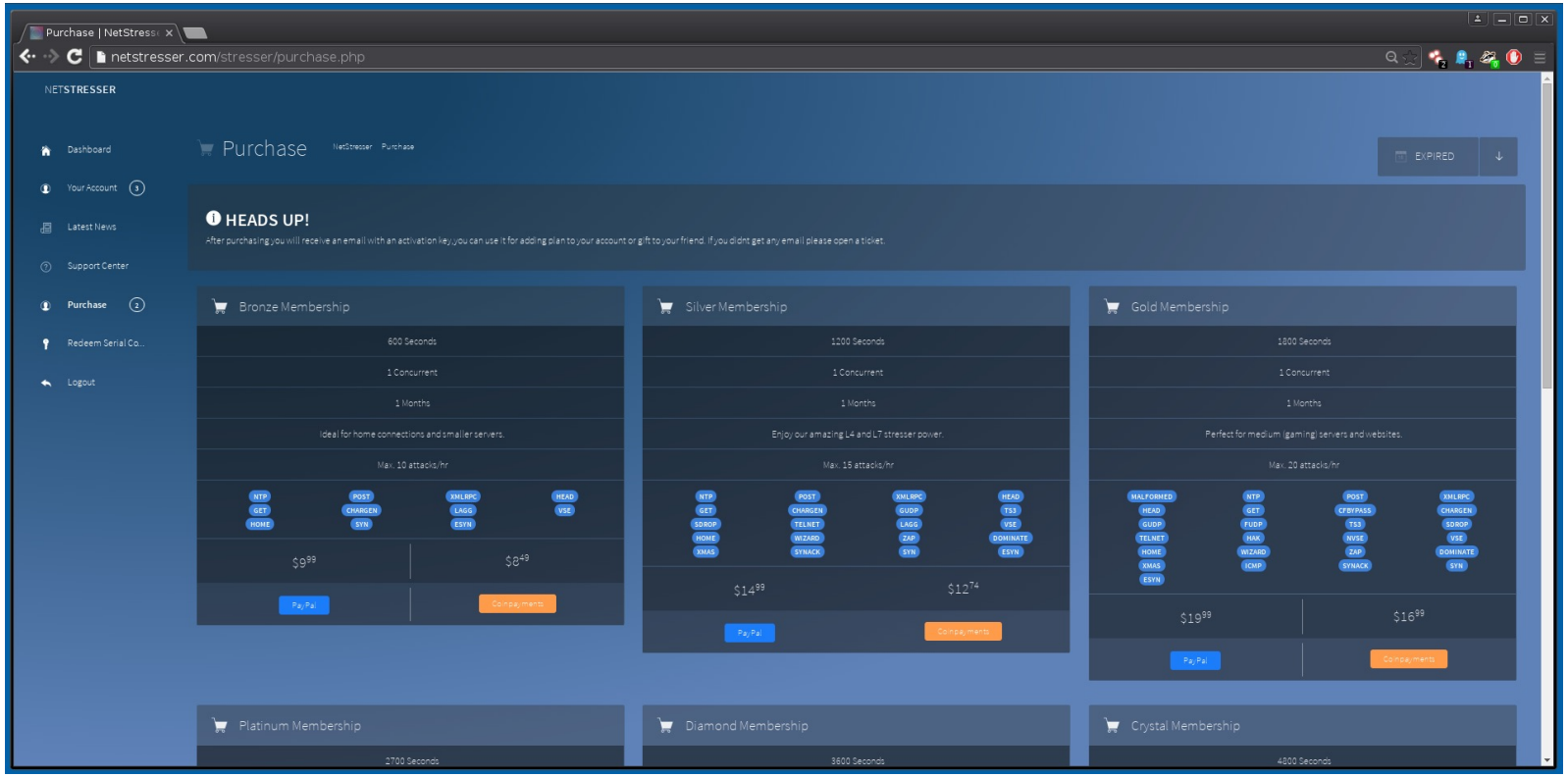
Why? Who?

- State-sponsored attackers (LARARUS, Bluenoroff, Andariel)

네트워크 보안

DDoS as a Service

- 다크웹을 통해 서비스 형태로 제공, 지불한 금액에 따라 전송되는 트래픽의 양이 결정됨 ($1000 -> 500Gbps)



- Popular DDoS as a Service
  - LizardStresser
  - Bang Stresser
  - uStress
  - NetStresser
  - vDoS

네트워크 보안

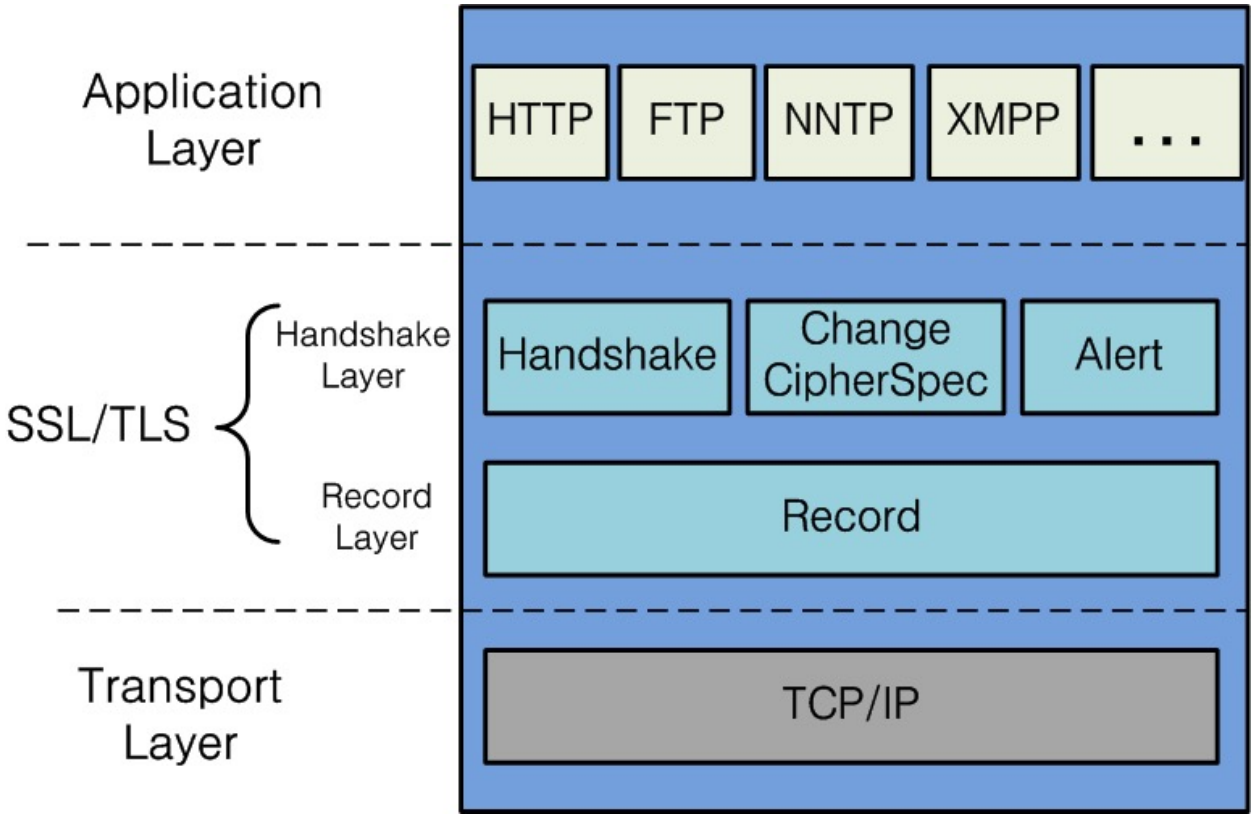
DDoS 공격의 방어

- 여분의 대역폭 확보
- 트래픽 필터링
  - IP 주소, 포트, 패킷 유형 등을 검사하여 유효한 패킷만 서비스로 전달
    - 방화벽, IPS 등 사용
  - 각 라우터에서 egress filtering 적용
- ISP와 협력
  - 공격 발생시 ISP에게 알려 upstream에서 공격 트래픽 차단
- CDN (Content Delivery Network) 활용
  - 여러 지역에 분산된 서버를 활용하여 트래픽을 분산 시켜서 대응

네트워크 보안

TLS (Transport Layer Security)

- 전송계층에서 동작하는 TCP 기반의 보안 프로토콜로, 전송 데이터의 기밀성, 무결성, 서버와 클라이언트간의 상호 인증 서비스를 제공한다.
- 주로 HTTP 트래픽 등을 보호하기 위해 사용되며 TLS를 적용한 HTTP 프로토콜을 HTTPS라고 부름



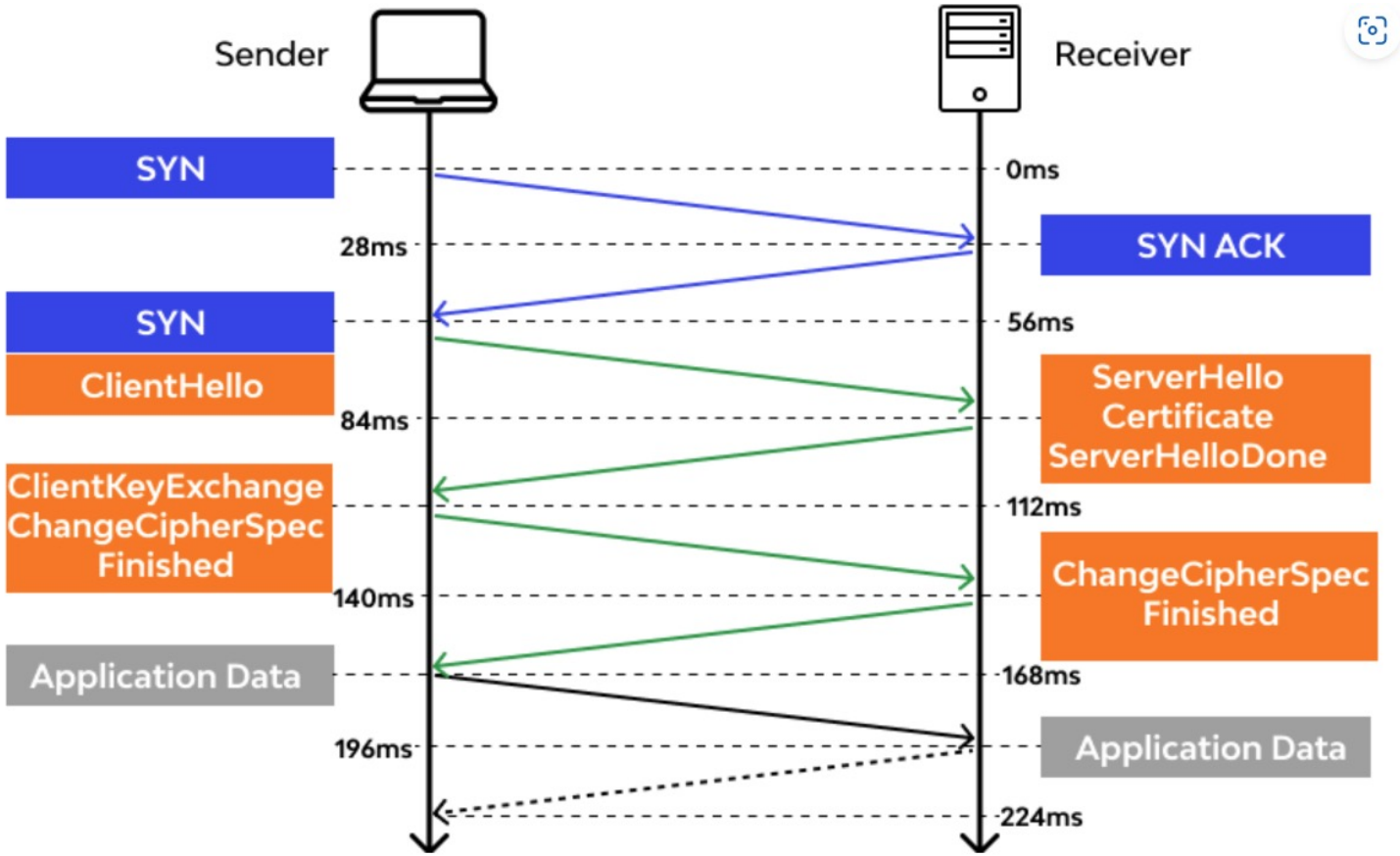
네트워크 보안

TLS 동작과정

1. TLS 연결 수립 (TLS handshake)
   - TCP 3-way 핸드세이크 후 서버와 클라이언트가 데이터 전송 시 사용할 암호화/인증/해시 알고리즘 합의
   - 서버와 클라이언의 상호 인증을 위한 인증서 교환 및 확인
2. 세션 키 교환 (change cipher spec)
   - 서버와 클라이언트가 데이터 암/복호화에 사용할 임시 (대칭)키를 교환
3. 데이터 전송 (record)
   - 서버와 클라이언트간의 데이터는 세션 키를 통해 암호화되며 무결성이 보장됨
4. 연결 종료
   - TCP 및 TLS 세션을 종료

네트워크 보안

- TLS 동작과정



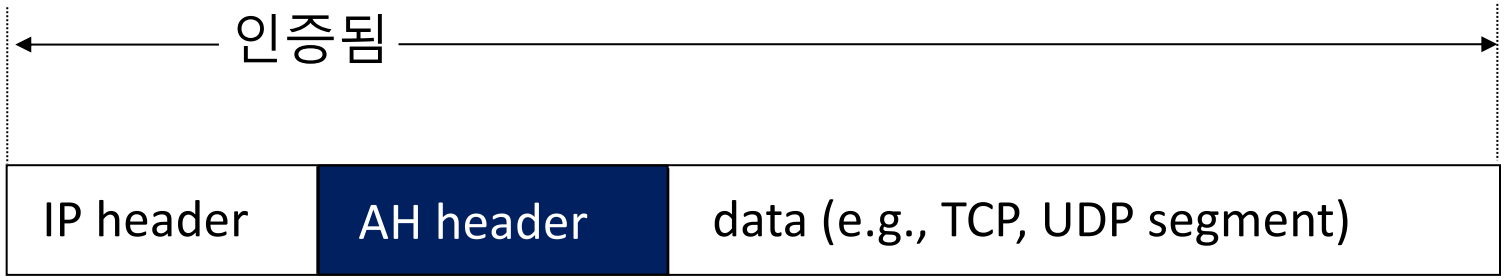
네트워크 보안

IPSec

- 네트워크 계층에서 IP 패킷 단위로 인증, 암호화, 키 관리를 지원하는 보안 프로토콜
- IPSec을 사용하는 호스트 사이에 일종의 보안 통로인 터널링(tunneling) 형성
- 전송 계층 하위에서 구현되기 때문에 응용 프로그램의 수정 불 필요
- 두 가지 보안 프로토콜 제공
  - 인증 헤더, Authentication header (AH)
  - 캡슐화된 보안 페이로드, Encapsulated security payload (ESP)

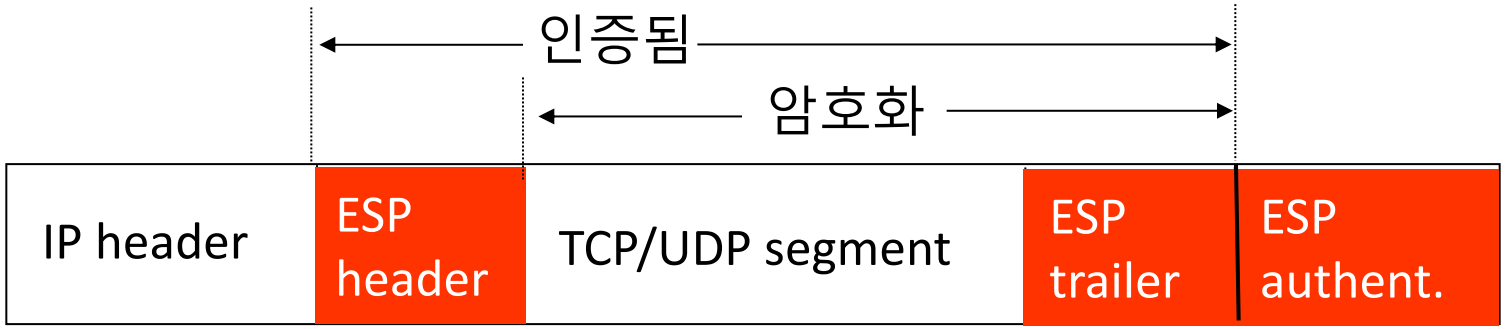
인증 헤더 (Authentication Header, AH)

- 데이터 발신지 인증, 데이터 무결성 제공 (기밀성은 제공하지 않음)
- 새로운 AH header가 IP header와 data 사이에 삽입됨



보안 페이로드 캡슐화 (Encapsulating Security Payload, ESP)

- 데이터 기밀성, 데이터 무결성, 발신지 인증 제공
- IP 패킷의 data 영역과 ESP trailer가 암호화됨
- ESP 인증 필드는 AH와 유사하며 옵션으로 사용됨



네트워크 보안

IPSec 운용 모드

- 수송 모드(Transport mode)
  - IP 헤더 이외 나머지 데이터 부분 만 보호하는 방식
  - 주로, 상위 계층 프로토콜만을 보호하기 위해 사용
  - 호스트 대 호스트 간에 주로 사용

- 터널 모드(Tunnel mode)
  - IP 패킷 전체를 보호하고, 그 앞에 새로운 IP 헤더를 추가하는 방식
  - `두 라우터 간에`, `호스트와 라우터 간에`, `두 게이트웨이 간에` 주로 사용 (VPN 구축)

네트워크 보안

TLS vs IPSec

- 두 프로토콜 모두 VPN (virtual private network) 구축에 사용됨

구분	TLS	IPSec
인증방식	인증서	비밀키 공유
보안성	End-to-End	Gateway-to-Gateway (전송모드) End-to-End (터널 모드)
접근성	어디서든 접근 가능	VPN 장비가 설치된 장소
도입비용	IPSec 보다 낮음	고비용
장점	설치 및 관리 용이	속도가 빠름, 모든 네트워크 트래픽 보호 가능
단점	클라이언트 소프트웨어 필요, 방화벽 설정 필요	설치가 복잡, 고비용

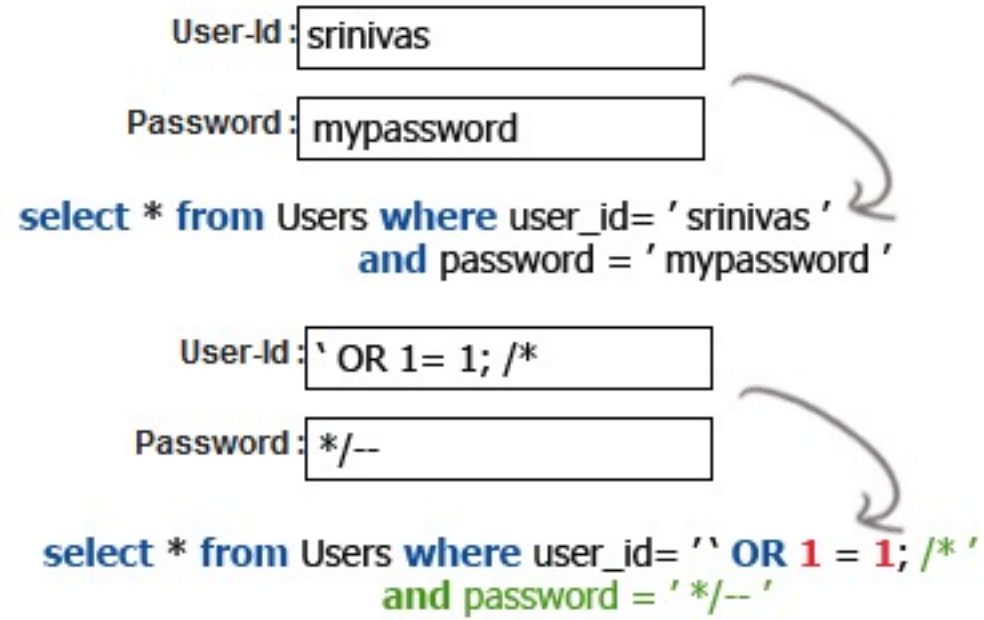
응용프로그램 보안

SQL 삽입 (SQL Injection)

- 웹 애플리케이션의 데이터베이스에 대한 보안 취약점을 이용한 공격
- 애플리케이션에 사용자 입력이 데이터베이스 쿼리에 그대로 삽입될 때 발생
- 공격자는 애플리케이션의 입력 필드에 SQL 명령문을 삽입하여 DB에 비정상적인 명령을 실행시키게 만들어 DB를 조작하거나 민감한 정보를 추출

응용프로그램 보안

- SQL 삽입 (SQL Injection)



정상적인 입력

쿼리문을 조작할 수 있는
비정상적인 입력

응용프로그램 보안

SQL 삽입 방어 방법

- **입력 검증**: 사용자 입력에 대한 엄격한 검증을 수행하여, SQL 구문이 입력될 수 없도록 함
- **Prepared Statements**: SQL 쿼리를 실행하기 전에, 변수를 바인딩하는 prepared statement를 사용해 사용자 입력이 쿼리의 일부로 해석되지 않게 함
- **ORM (Object-Relational Mapping)**: SQL 쿼리를 직접 작성하지 않고, ORM 프레임워크를 통해 DB 작업을 수행
- 계정 권한 제한: DB 계정은 필요한 최소한의 권한만을 가지도록 설정
- **웹 애플리케이션 방화벽 (WAF)**: WAF를 사용하여 의심스러운 트래픽과 악의적인 데이터 패턴을 차단

응용프로그램 보안

- Prepared Statement

```
String user = getUsername();
String password = getPassword();
String query = "SELECT user FROM user_table WHERE user=\"" + user + "\" and password=\
"" + password + "\"";
try {
    stmt = con.createStatement();
    ResultSet rs = stmt.executeQuery(query);
```

```
try (PreparedStatement stmt = conn.prepareStatement(
    "SELECT user FROM user_table WHERE user = ? and password = ?")) {
    stmt.setString(1, getUsername());
    stmt.setString(2, getPassword());
    ResultSet rs = stmt.executeQuery();
```

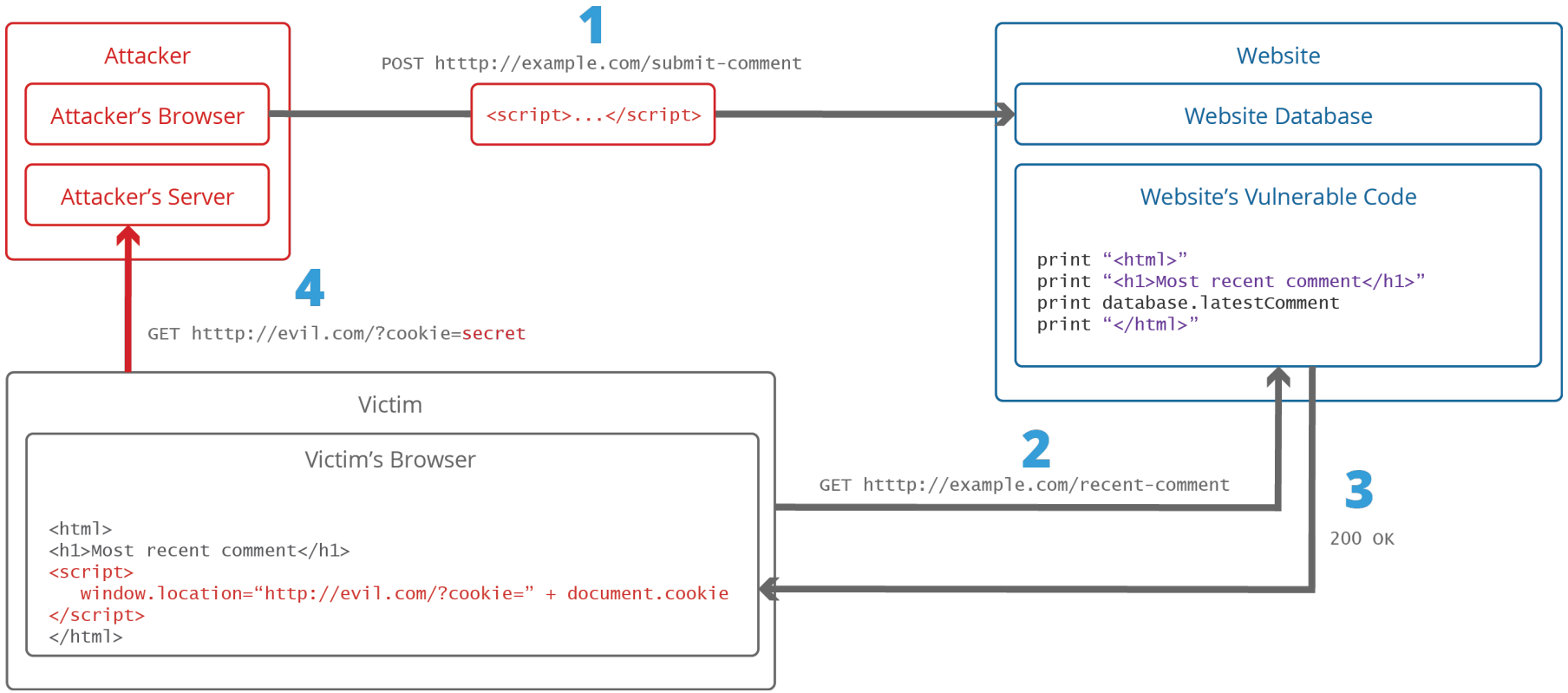
응용프로그램 보안

크로스사이트 스크립팅(Cross-site Scripting, XSS)

- 웹 애플리케이션의 취약점을 이용하여 공격자가 악의적인 스크립트를 주입하고, 이 스크립트가 다른 사용자의 브라우저에서 실행되게 만드는 공격
- 주로 웹 애플리케이션에서 사용자의 입력을 적절히 검증, 이스케이프 처리하지 않았을 때 발생
- 악성 스크립트는 사용자 세션을 가로채거나, 개인정보를 탈취하거나, 사용자를 속여 특정 행동을 하게 만드는 등 다양한 악의적인 행위를 수행함

응용프로그램 보안

- 크로스사이트 스크립팅(Cross-site Scripting, XSS)



XSS 방어 방법

- **입력 검증**: 모든 사용자 입력에 대해 엄격한 검증을 수행하며, 알려진 위험한 문자들을 차단
- **출력 이스케이프**: 사용자로부터 받은 데이터를 웹 페이지에 출력하기 전에 HTML 이스케이프 처리를 수행, 예를 들어, '<', '>', '&', '"'와 같은 문자를 HTML 엔티티로 변환
- **콘텐츠 보안 정책 (Content Security Policy, CSP)**: 웹 브라우저가 오직 신뢰할 수 있는 소스에서만 스크립트를 실행하도록 하여, 악의적인 스크립트의 실행을 차단
- **쿠키에 'HttpOnly' 플래그 설정**: JavaScript를 통한 쿠키 접근을 차단하여, 공격자가 XSS를 이용해 사용자의 세션 쿠키를 탈취하는 것을 방지
- **웹 애플리케이션 방화벽 (WAF)**: WAF를 사용하여 알려진 XSS 공격 시그니처를 가진 요청을 차단

정보보안 최신용어

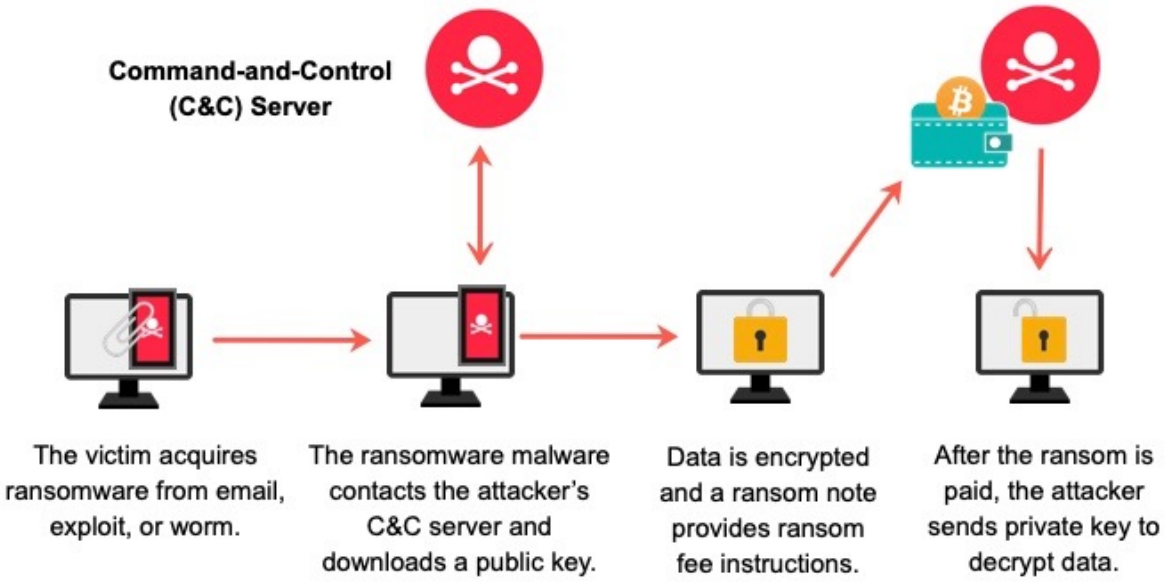
랜섬웨어 (Ransomware)

- 컴퓨터를 감염시킨 후 사용자의 파일이나 시스템에 대한 접근을 제한하고, 해당 파일이나 시스템에 대한 복원을 위해 금전적 보상을 요구하는 악성 코드
- 주로 문서 파일이나 시스템 내 주요 파일을 암호화함
- 복호화 키 제공을 빌미로 비트 코인 등의 금전 요구
- CryptoWall, Locky, WannaCry, Petya

정보보안 최신용어

랜섬웨어 (Ransomware)

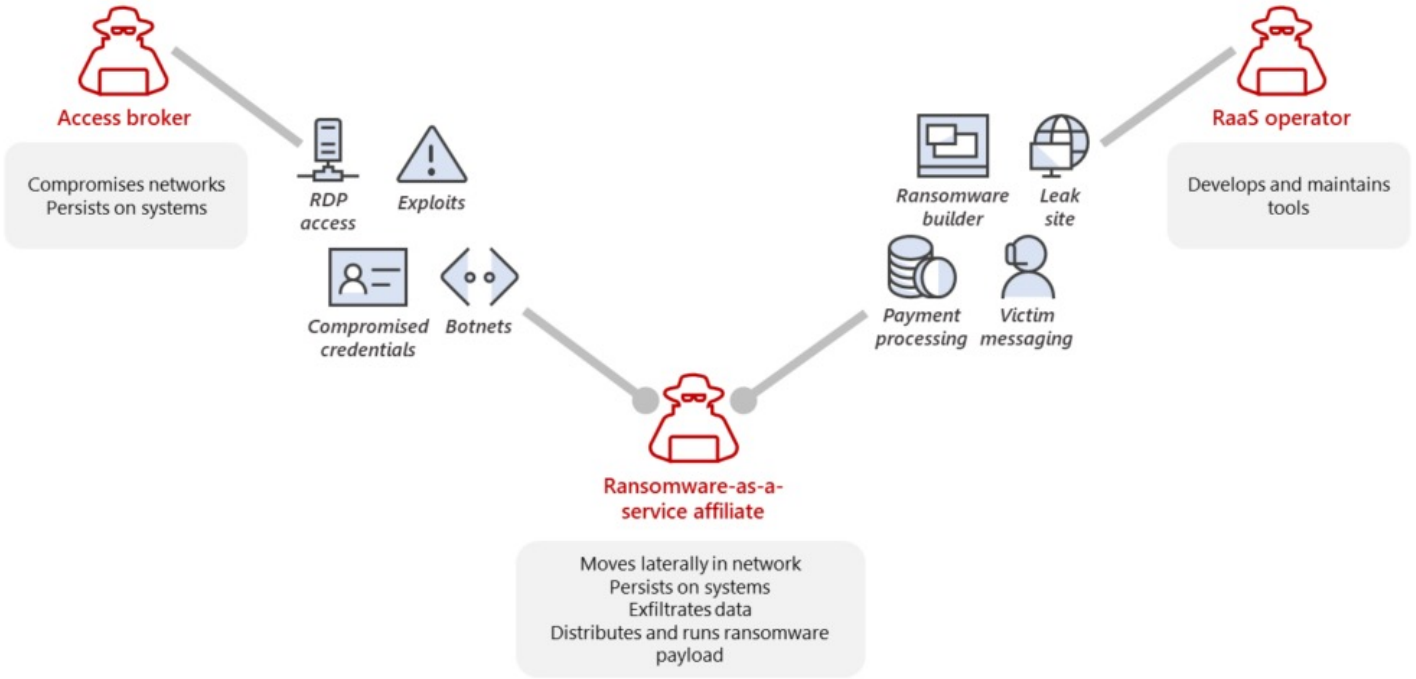
- 스팸 메일, 악성 사이트를 경로로 시스템에 침투
- 침투 즉시 시스템 암호화 하는 것이 아니라 C&C 서버의 명령을 기다림
- 명령에 따라 시스템의 내부 정보를 탈취한 뒤 암호화
  - 중요 문서 및 정보 탈취
  - 백도어 설치 및 인접 시스템으로 전파
  - AES, RSA, ChaCha20 사용
- 비용 지불을 확인한 뒤 복호화 키 제공



정보보안 최신용어

Ransomware as a Service (RaaS)

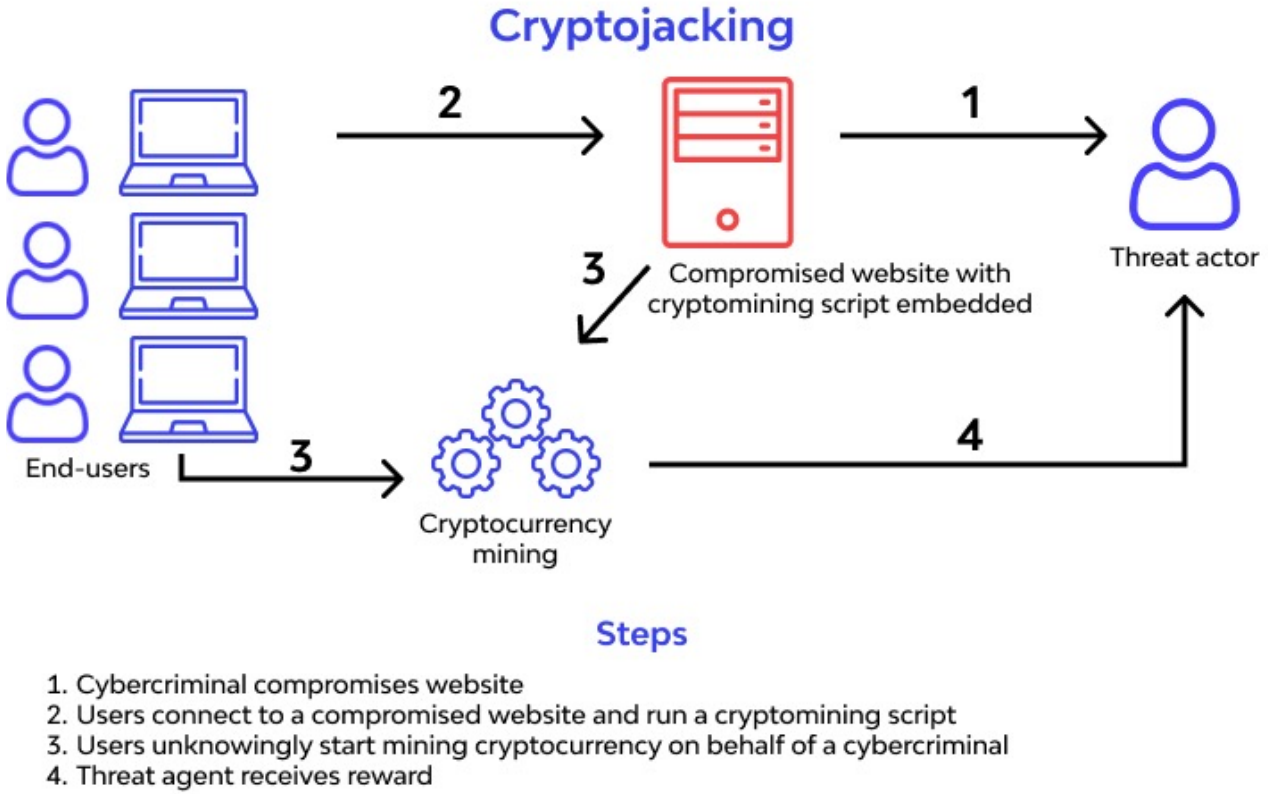
- 악성 코드 제작자들이 제작한 랜섬웨어를 타인이 구매하고 사용할 수 있도록 제공하는 서비스
- Dharma, LockBit, REvil, DarkSide



정보보안 최신용어

크랩토 재킹, Cryptojacking

- 악성코드가 사용자의 컴퓨터나 모바일 기기에서 암호화폐 채굴을 하도록 강제하는 공격 기술
- 공격자는 사용자의 컴퓨팅 자원을 이용하여 암호화폐를 채굴하고, 이를 자신의 지갑으로 이전하여 이득을 얻음



4. 정보보안 이해와 활용 영역 기출 문제

기출 문제 풀이

Q2

[보기]는 사이버 공격 사례를 설명하고 있다.
어떤 사이버 공격의 사례인지 올바른 것을 고르시오.

[보기]

- 워너크라이(WannaCry) : 2017년 5월 12일 전세계 150여개 국에서 최소 30만대 이상의 컴퓨터 시스템들이 감염. 감염된 시스템은 특정 확장자를 가지는 내부 파일들이 .WNCRY로 변경되고 파일 내용이 암호화되며, 감염시스템 화면에 안내문구를 표시한다.
- 클롭(Clop) : 2019년 3월 러시아 해킹그룹에 의해 제작됨, 국내 증권사 직원 PC가 감염되어 전산장애 발생. 파일을 암호화하고 확장자는 .Clop으로 변경된다.
- 갠드크랩(GandCrab) : 2018년 1월 처음 등장하여 전문지식 없이도 공격 가능한 서비스 형으로 제작이 가능하여 공격 증가의 주요 원인이 되었음. 파일을 암호화 하고 확장자는 .GDCB, .KRAB등으로 변경된다.

[답가지]

① 피싱(Phishing)
② 파밍(Pharming)
③ 랜섬웨어(Ransomware)
④ DDoS(Distributed Denial of Service)

기출 문제 풀이

Q4 다음 보기에서 설명하는 보안 기술을 무엇이라 하는가?

[망분리]

[보기]

- 주로 공공기관이나 기업에서 인터넷과 완전히 격리된 환경에서 업무를 볼 수 있도록 내부 네트워크를 분리하는 기술
- 해당 기술에는 논리적인 방법과 물리적인 방법이 있음

기출 문제 풀이 (시큐어 코딩)

Q5

김 대리가 수행하는 프로젝트에서는 개발 언어로 JAVA를 사용하며, 기본적으로 시큐어 코딩을 적용하여야 한다. [보기]는 외부의 입력을 통하여 "디렉터리 경로 문자열"을 생성하여 특정 처리를 하는 코드로, 시큐어 코딩을 적용하지 않은 상태이다. 다음 물음에 답 하시오. 단, 시큐어 코딩 조치 과정에서 상대 경로를 지정하는데 사용하지 않아야 할 문자는 "/" 한 종류만 고려하기로 한다.

1) [보기 1]의 코드에서 보안에 취약한 라인 번호를 제시하고 그 이유를 설명 하시오.

2) [보기 2]의 코드에서 각 취약점을 해결하기 위해 취해야 할 시큐어 코딩 조치를 박스 위치의 라인에 적용 하시오.

기출 문제 풀이 (시큐어 코딩)

[보기 1]은 외부로부터 파일 명을 입력 받고 그 앞에 상대 디렉터리 경로를 추가하여 해당 파일 객체를 생성하고 그 파일을 삭제하는 코드의 예이다. 각 명령 줄에 라인 번호를 편의 상 부여하였다.

참고 : Properties 클래스는 주로 어플리케이션의 환경 설정과 관련된 속성을 저장하는데 사용되며 데이터를 파일로부터 읽고 기록하는 편리한 기능을 제공한다.

[보기 1]

```
1: ……
2: public void f(Properties request) {
3:     ……
4:     String name = request.getProperty("filename");
5:     if(name != null && !"".equals(name)) {
6:         File file = new File("/usr/local/tmp/" + name);
7:         file.delete();
8:     }
9:     ……
10: }
```

디렉토리 경로 조작

Null pointer dereference

기출 문제 풀이 (시큐어 코딩)

[보기 2]는 [보기 1]에 대해 시큐어 코딩 조치를 취하기 위하여 완성하려는 코드이다.

[보기 2]

```
1: ……
2: public void f(Properties request) {
3:     ……
4:     String name = request.getProperty("filename");
5:     if (name != null && !"".equals(name)) {
6:         name = name.replace("/", " ");
7 :        File file = new File("/usr/local/tmp/" + name);
8:         if (file != null) file.delete();
9:     }
10: ……
11: }
```

기출문제 풀이

응용프로그램 보안

- EDR(Endpoint Detection Response) 솔루션의 주요 기능으로 옳지 않은 것은?

  ① 보안사고 탐지 영역

  ② 보안사고 통제 영역

  ③ 보안사고 확산 영역

  ④ 보안사고 치료 영역

- 정답:**3**, EDR은 보안사고를 탐지, 통제, 치료하는 기능을 가지고 있지만, 확산은 EDR의 주요 기능이 아닙니다.

기출문제 풀이

응용프로그램 보안

- 웹사이트의 쿠키(cookie)에 대한 설명으로 틀린 것은?

  ① 서버에서 생성하여 클라이언트에 저장

  ② 여러개의 값을 추가시 "/" 특수문자를 사용

  ③ 클라이언트의 개인정보를 저장할 수 있음

  ④ 세션관리, 개인화, 트래킹 등에 사용

- 정답: **2**, 쿠키에서 여러 값을 구분할 때는 일반적으로 세미콜론(;)을 사용합니다.

기출문제 풀이

응용프로그램 보안

- AI나 머신러닝의 이미지 인식에서 인간이 감지할 수 없는 노이즈나 작은 변화를 주어 AI 알고리즘의 잘못된 판단을 유도하는 공격은?

  ① Backdoor 공격

  ② Adversarial 공격

  ③ Poisoning 공격

  ④ Evasion 공격

- 정답: **2**, Adversarial 공격은 AI 모델을 속이기 위해 입력 데이터에 미세한 변화를 주는 공격 방식입니다.

기출문제 풀이

네트워크 보안

- UDP Flooding의 대응 방안으로 틀린 것은?

  ① 미사용 프로토콜 필터링

  ② 도착지 IP별 임계치 기반 차단

  ③ 패킷 크기 기반 차단

  ④ Anycast를 이용한 대응

- 정답: **2**, UDP Flooding 대응에는 주로 발신지 IP별 임계치 기반 차단이 사용됩니다. 도착지 IP별 차단은 적절하지 않습니다.

famous77@kaist.ac.kr