소프트웨어 개발 보안 구축

송민호

유튜브 주소: https://youtu.be/ezx2tF_KTcE

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

Secure SDLC

암호 알고리즘

서비스 공격 유형

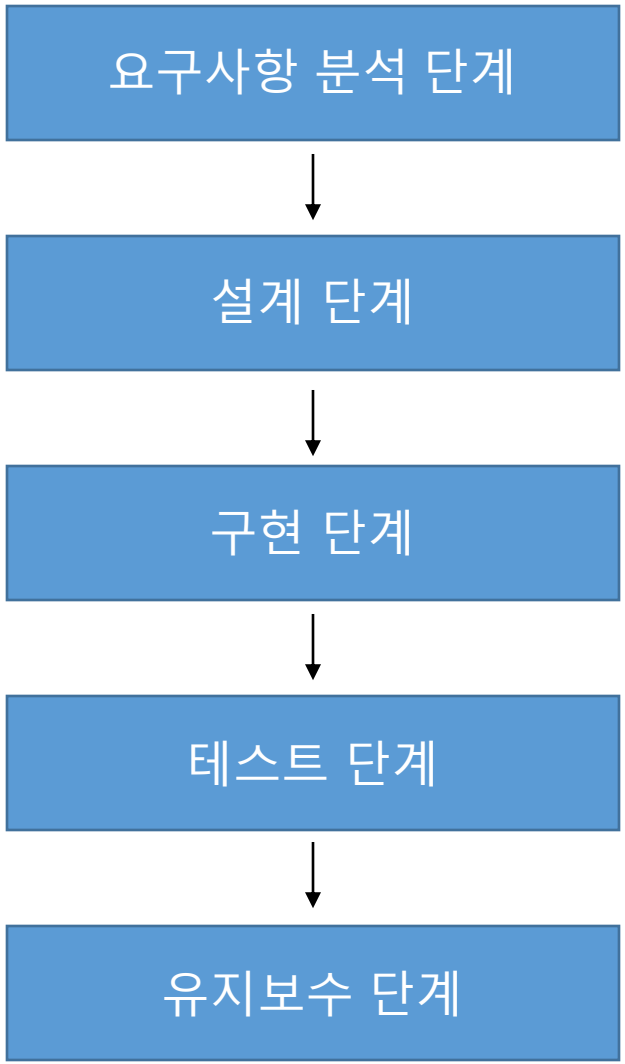
Secure SDLC

SDLC에 보안 강화를 위한 프로세스를 포함한 것

- Secure SDLC의 대표적인 방법론
  - CLASP
    - SDLC의 초기 단계에서 보안을 강화하기 위해 개발된 방법론
  - SDL
    - 마이크로소프트 사에서 안전한 소프트웨어 개발을 위해 기존의 SDLC를 개선한 방법론
  - Seven Touchpoints
    - 소프트웨어 보안의 모범사례를 SDLC에 통합한 방법론

Secure SDLC

SDLC 단계별 보안 활동



Secure SDLC

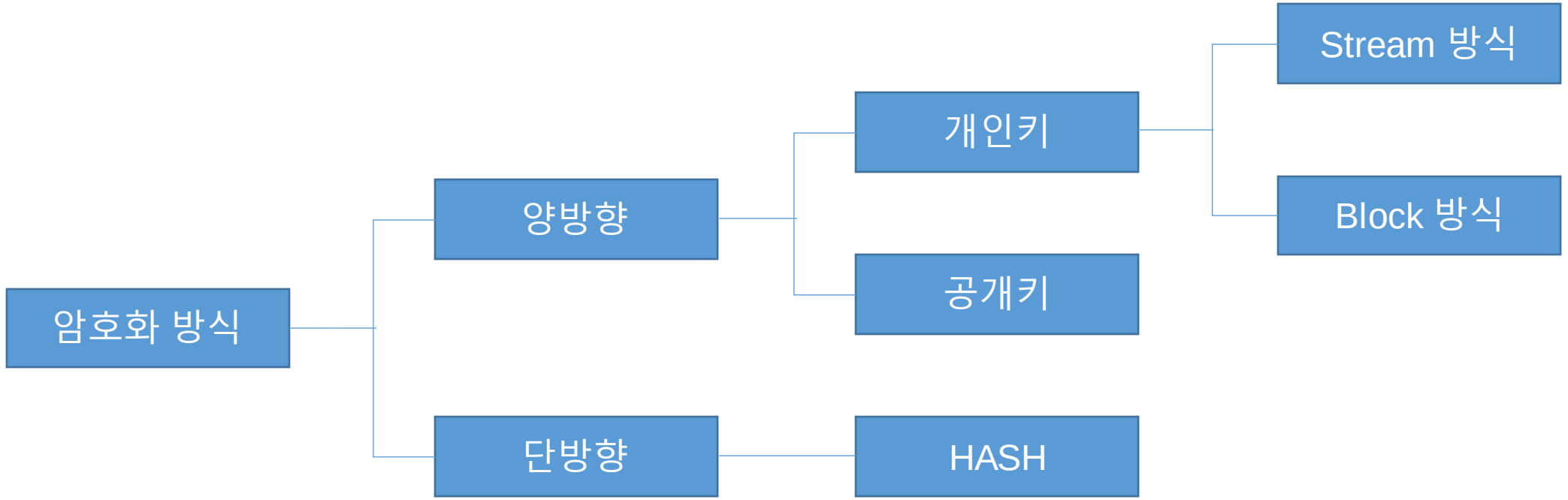
소프트웨어 개발 보안 요소

보안 요소	설명
기밀성 (Confidentiality)	• 시스템 내의 정보와 자원은 인가된 사용자에게만 접근이 허용됨 • 정보가 전송 중에 노출되더라도 데이터를 읽을 수 없음
무결성 (Integrity)	시스템 내의 정보는 오직 인가된 사용자만 수정할 수 있음
가용성 (Availability)	인가 받은 사용자는 시스템 내의 정보와 자원을 언제라도 사용할 수 있음
인증 (Authentication)	• 시스템 내의 정보와 자원을 사용하려는 사용자가 합법적인 사용자인지를 확인하는 모든 행위 • 대표적 방법: 패스워드, 인증용 카드, 지문 검사 등
부인 방지 (NonRepudiation)	데이터를 송・수신한 자가 송・수신 사실을 부인할 수 없도록 송・수신 증거를 제공함

암호 알고리즘

정보를 보호하기 위해 평문을 암호화된 문장으로 만드는 방법

- 암호 방식 분류



암호 알고리즘

개인키 암호화 기법

- 동일한 키로 데이터를 암호화하고 복호화하는 암호화 기법

개인키 암호화 기법의 종류	설명
스트림 암호화 방식	• 평문과 동일한 길이의 스트림을 생성하여 비트 단위로 암호화 하는 방식 • 종류: LFSR, RC4
블록 암호화 방식	• 한 번에 하나의 데이터 블록을 암호화 하는 방식 • 종류: DES, SEED, AES, ARIA

암호 알고리즘

공개키 암호화 기법

- 암호화할 때 사용하는 공개키는 사용자에게 공개하고, 복호화할 때의 비밀키는 관리자가 비밀리에 관리하는 암호화 기법
- 관리해야 할 키의 수가 적지만, 암호화/복호화 속도가 느리다
- 종류: RSA

암호 알고리즘

양방향 알고리즘의 종류

알고리즘	특징
SEED	• KISA에서 개발한 블록 암호화 알고리즘 • 블록 크기는 128비트이며, 키 길이에 따라 128, 256으로 분류됨
ARIA	• 국가정보원과 산학연협회가 개발한 블록 암호화 알고리즘
DES	• 미국 NBS(NIST)에서 발표한 개인키 암호화 알고리즘 • 블록 크기는 64비트, 키 길이는 56비트이며 16회의 라운드를 수행함 • DES를 3번 적용하여 보안을 더욱 강화한 3DES도 있음
AES	• NIST에서 발표한 개인키 암호화 알고리즘 • DES의 한계를 느낀 NIST에서 공모한 후 발표 • 블록 크기는 128비트이며, 키 길이에 따라 AES-128, AES-192, AES-256으로 분류됨
RSA	• MIT의 Rivest, Shamir, Adelman에 의해 제안된 공개키 암호화 알고리즘 • 큰 숫자를 소인수분해 하기 어렵다는 것에 기반하여 만들어짐

암호 알고리즘

해시(Hash)

- 임의의 길이의 입력 데이터나 메시지를 고정된 길이의 값이나 키로 변환하는 것

해시 함수	특징
SHA 시리즈	• NSA가 설계, NIST에 의해 발표됨 • 초기 개발된 SHA-0 이후 SHA-1이 발표되었고, 다시 SHA-2라고 불리는 SHA-224, SHA-256, SHA-384, SHA-512가 발표됨
MD5	• R.Rivest가 MD4를 대체하기 위해 고안한 암호화 해시 함수 • 블록 크기가 512비트이며, 키 길이는 128비트임
N-NASH	• 일본의 NTT에서 발표한 암호화 해시 함수 • 블록 크기와 키 길이가 모두 128비트임
SNEFRU	• R.C.Merkle가 발표한 해시 함수 • 32비트 프로세서에서 구현을 용이하게 할 목적으로 개발됨

서비스 공격 유형

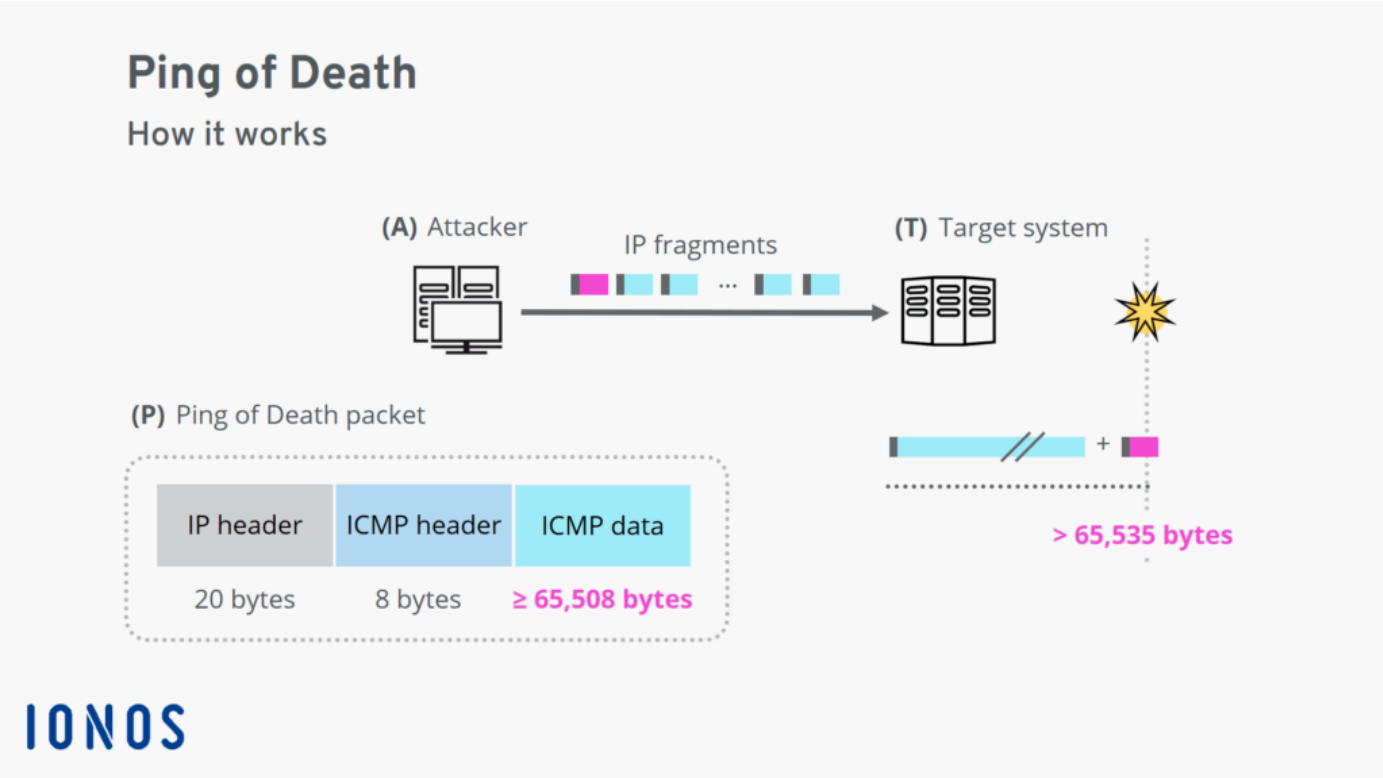
대량의 데이터를 한 곳의 서버에 집중적으로 전송함으로써, 표적이 되는 서버의 정상적인 기능을 방해하는 것

- 주요 서비스 거부 공격의 유형
  - Ping of Death
  - SMURFING
  - SYN Flooding
  - TearDrop
  - Land Attack
  - DDos 공격

서비스 공격 유형

Ping of Death

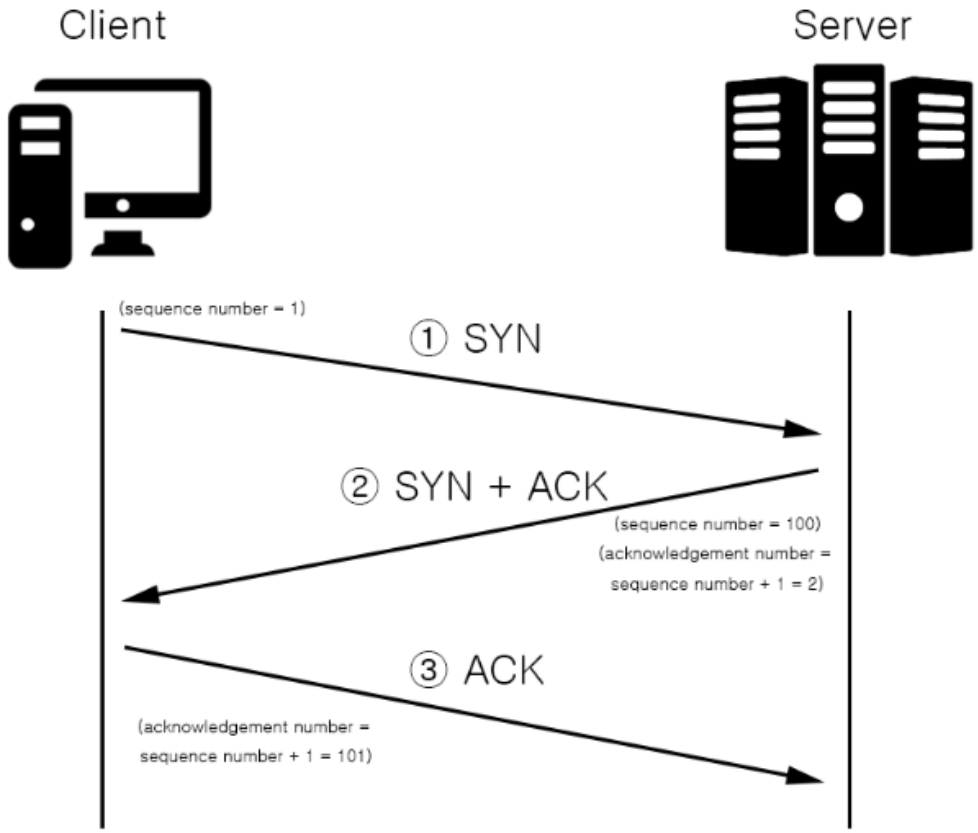
- 패킷의 크기를 인터넷 프로토콜 허용 범위 이상으로 전송하여 공격 대상의 네트워크를 마비시키는 서비스 거부 공격 방법



서비스 공격 유형

SYN Flooding

- 3-way-handshake 과정을 의도적으로 중단시킴으로써 공격 대상지인 서버가 대기 상태에 놓여 정상적인 서비스를 수행하지 못하게 하는 공격 방법

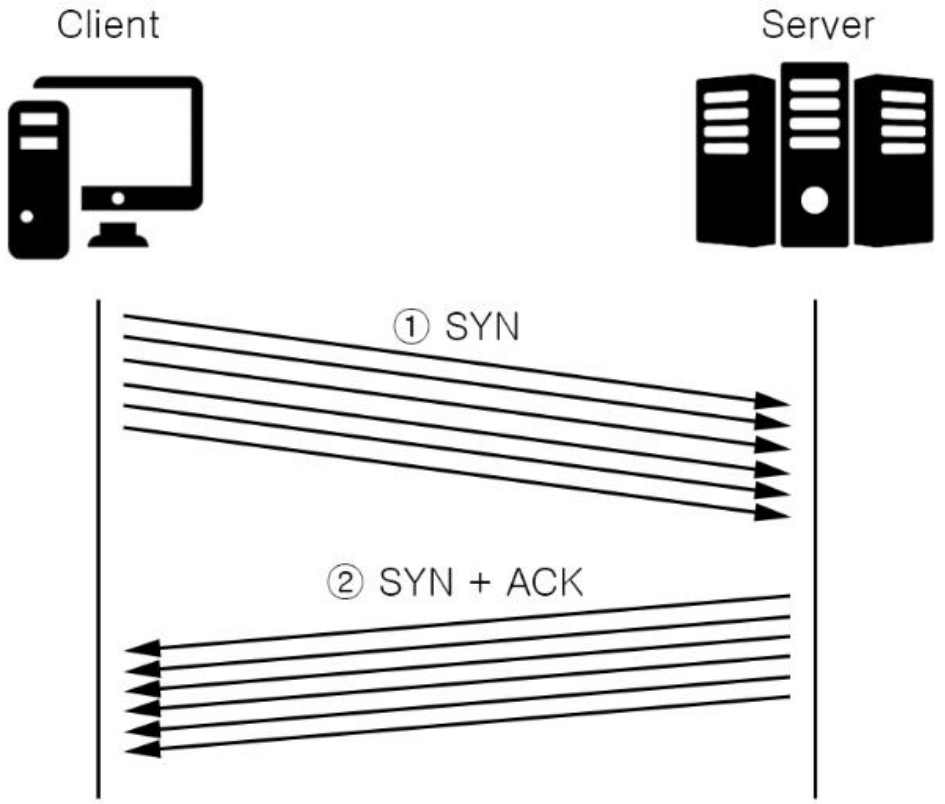


서비스 공격 유형

SYN Flooding

- Server는 Client의 접속을 받아들이기 위해, RAM에 일정 공간을 확보

- Client가 ACK 패킷을 보내지 않게 되면 Server는 Client의 연결을 받아들이기 위해 RAM 공간을 점점 더 많이 확보해둔 상태에서 대기



Q & A