Computational Thinking

2017 2학기

12-정보보호

박종혁 교수 (컴퓨터공학과)

jhpark1@seoultech.ac.kr

http://www.parkjonghyuk.net

서울과학기술대학교

SEOULTECH SEOUL NATIONAL UNIVERSITY OF SCIENCE & TECHNOLOGY

학습개요

- 12장 정보 보호
  1. 보안이란 무엇인가?
  2. 기초 토대
  3. 사이버범죄의 일반적인 형태
  4. 어떻게 보호할 것인가? 단계1: 인증
  5. 어떻게 보호할 것인가? 단계2: 인가
  6. 모든 위험의 문제
  7. 몇가지 좋은 방법들
  8. 좋은 전략
  9. 참고문헌
- 조별발표
  - 조별 10분 발표

학습목표

- 기본적인 보안 관련 어휘에 친숙해진다.
- 보안이 기밀성, 무결성, 가용성의 3개의 구성요소를 가지고 있음을 이해한다.
- 바이러스, 악성코드, 스푸핑, 릴레이 공격, 네트워크 스니핑, 스패밍, 어깨너머로 훔쳐보기, 휴지통 뒤지기, 신원 도용, 서비스 거부, 사회공학, 피싱을 포함하여 사이버범죄의 일반적인 형태를 이해한다.
- 일반적으로 사용되는 인증 기술들과 이들이 어떻게 동작하는지를 이해한다.
- 두 단계 인증과 이것이 어떻게 더 나은 보안을 제공하는지를 이해한다.
- 읽기, 쓰기, 실행, 그리고 소유 인가 사이의 차이를 이해한다.

학습목표

- 보안 목적을 위해 사용되는 ID의 유일성에 대한 필요를 이해한다.
- 피해의 잠재적인 비용과 침해의 가능성의 두 부분의 등급으로서 위험을 설명할 수 있다.
- 단방향과 양방향 암호, 방화벽, 안티바이러스 소프트웨어, 소프트웨어 갱신, 파일 백업, 그리고 로그 파일을 포함하여 일반적인 완화 전략을 사용하는 목적과 시점을 이해한다.
- 가장 약한 연결부 보호하기, 공격 외관 줄이기, 철저하게 방어하기, 구획으로 나누기, 그리고 쉽게 신뢰하지 않기를 포함하여 몇 가지 기본적인 보안 원리를 인지하고 적용할 수 있다.
- 개방성이 어떻게 보안에 기여하는지 이해한다.

❖ **정보 보호(information security)**
- 정보를 여러가지 위협으로 부터 보호하는 것

❖ **자산(asset)**
- 보호를 필요로 하는 대상

❖ **공격자(attacker)**
- 잠재적으로 해를 끼칠 수 있는 사람

❖ **취약점(vulnerabilities)**
- 자산이 쉽게 공격받는 방식

❖ **완화(mitigation)**
- 취약점을 상쇄하거나 감소시키려는 어떤 시도

❖ **이용(exploit)**
- 소프트웨어나 하드웨어 및 전자 제품의 버그, 취약점 등 설계상 결함을 이용해 공격자의 의도된 동작을 수행하도록 만들어진 데이터 조각

❖ **위협(threat)**
- 취약점이 공격자에게 나쁘게 이용되는 것

❖ **침해(breach)**
- 자산에 대해 실질적인 손해를 끼치는 것

❖ **물리적 보안(physical security)**
- 하드웨어 장치를 보호하는 것

❖ **매개체(vector)**
- 공격자가 컴퓨터나 네트워크에 접근하기 위해 사용하는 경로나 방법

❖ **흰색 모자(white hat)**
- 보안 관점에서 좋은 행위

❖ **검정 모자(black hat)**
- 보안 관점에서 바람직하지 않은 행위

❖ 보안의 3가지 특징

1. 기밀성(Confidentiality) : 정보에 대한 접근이 적절히 제한 되어야만 한다.
2. 무결성(integrity) : 정보가 믿을 수 있고 신뢰할 만한 가치가 있다.
   - 데이터 무결성(data integrity)
   - 소유자 무결성(owner integrity)
3. 가용성(availability) : 정보 시스템이 정상적으로 사용 가능한 정도

그림 12.1 정보의 3가지 기초적인 외관

❖ **보안 보장(security assurance)**
- 보안 시스템들이 충분히 튼튼하다는 것을 보장하는 것.

❖ **아마추어 해커(script kiddies)**
- 크래킹을 위해 다른 사람이 개발한 스크립트나 프로그램을 사용하는 해커

❖ **사이버범죄(cybercrime)**
- 컴퓨터, 통신, 인터넷 등을 악용하여 사이버 공간에서 행하는 범죄

❖ **컴퓨터 바이러스(computer virus)**
- 스스로를 복제하여 컴퓨터를 감염시키는 컴퓨터 프로그램

12.3 사이버범죄의 일반적인 형태

- **스푸핑(spoofing)**
  - MAC 주소, IP주소, 포트 등을 속여 공격하는 것
- **릴레이 공격(relay attack)**
  - 공격의 발원지를 다른 컴퓨터인 것 처럼 속이는 것
- **네트워크 스니핑(network sniffing)**
  - 네트워크상의 정보를 엿듣는 행위
- **평문(plaintext)**
  - 누구나 그 내용을 보면 그 내용을 이해할 수 있는 문서.
    즉 암호화되지 않은 메시지를 의미한다.
- **어깨너머로 훔쳐보기(shoulder surfing)**
  - 정보를 뒤에서 몰래 훔쳐보는 기법
- **휴지통 뒤지기(dumpster diving)**
  - 휴지통에서 중요 정보를 찾아내는 기법

❖ **서비스 거부 공격(DoS: denial-of-service attack)**
- 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격

❖ **스팸(spam)**
- 불특정 다수의 사람들에게 보내는 광고성 메시지

❖ **쿠키(cookies)**
- 인터넷 사용자가 어떠한 웹사이트를 방문할 경우, 웹사이트의 서버에서 사용자 컴퓨터에 설치하는 작은 기록정보 파일

❖ **신원 도용(identity theft)**
- 유출한 개인정보를 이용하여 타인인 것처럼 가장하는 행위

❖ 인증을 위해 사용될 수 있는 4개의 요소

1. 주체가 알고 있는 것(something the subject knows)
2. 주체가 소유하고 있는 것(something the subject possesses)
3. 주체에 내재하고 있는 것(something the subject is)
4. 주체가 위치하는 곳(somewhere the subject is located)

그림 12.2 인증 토큰

❖ 보안에서의 두 가지 개체

- 자산(assets) : 가치가 있는 대상
- 주체(subjects) : 자산에 접근하는 프로세스, 사람, 장치

그림 12.3 신원, 인증, 인가

❖ **수많은 침해사고 시나리오가 존재한다.**

- 보안에서 완전한 방어는 있을 수 없다.
- 해결책(solution)보다 전략(strategy)라는 단어를 사용

❖ **위험(risk)**

- 침해 가능성과 피해 정도라는 두 가지 것들의 조합

❖ **정보보호 문제를 완화시키기 위한 6가지 전략**

1. 암호화
2. 방화벽 (스팸 필터를 포함하고 있는)
3. 안티바이러스 소프트웨어
4. 소프트웨어 업데이트(갱신)
5. 백업
6. 로그 파일

❖ 암호화(encryption)

- 양방향 암호화(two-way encryption) : 암호화와 복호화가 모두 가능하다.
- 단방향 암호화(one-way encryption) : 오직 암호화만이 가능하다

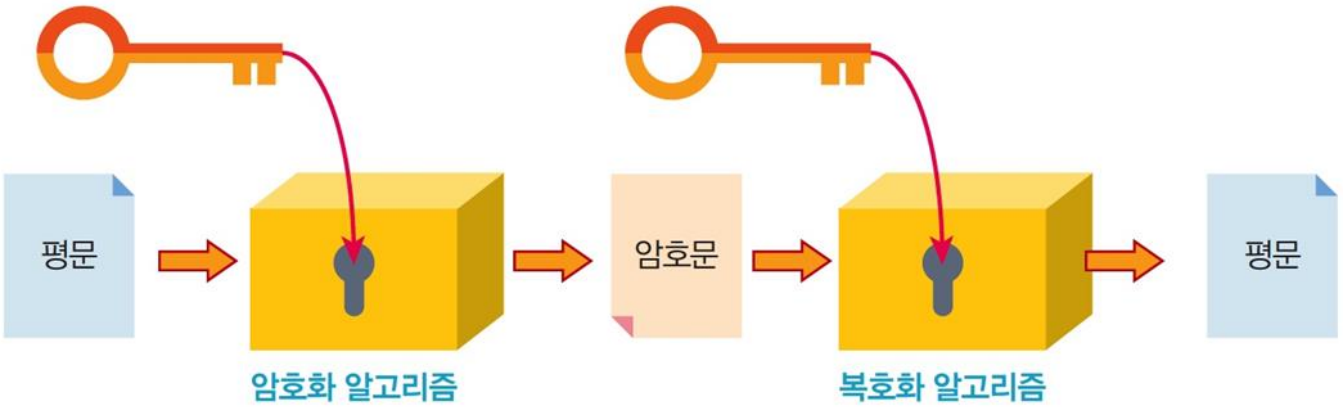


그림 12.4 양방향 암호화

❖ 암호화(encryption)

- 양방향 암호화(two-way encryption) : 암호화와 복호화가 모두 가능하다.
- 단방향 암호화(one-way encryption) : 오직 암호화만이 가능하다

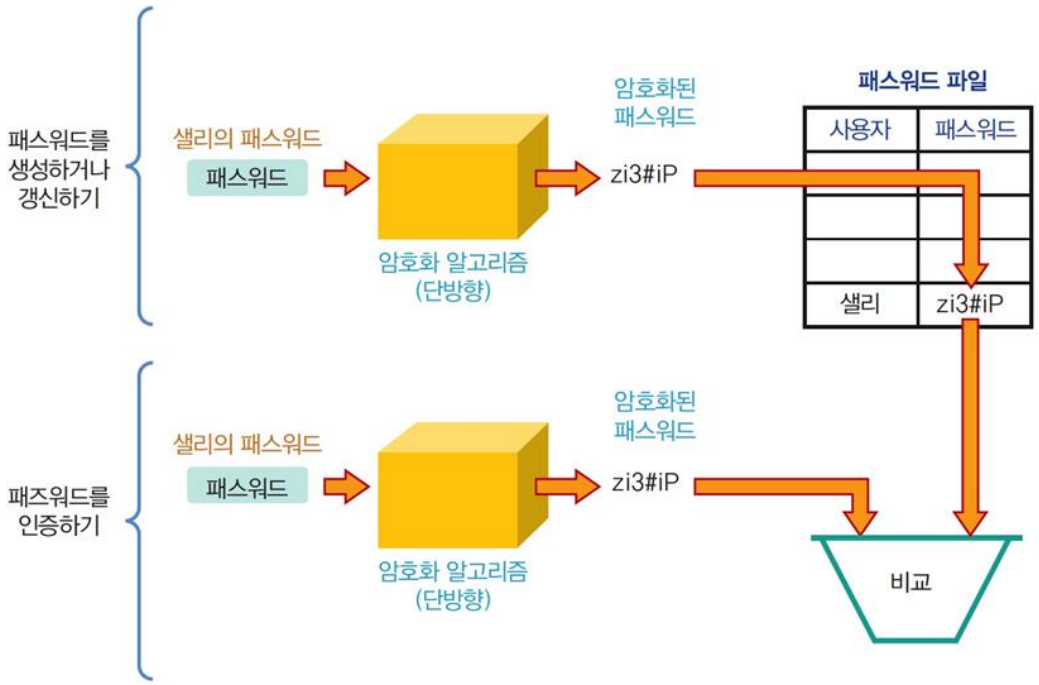


그림 12.5 패스워드를 저장하고 인증하기 위해 단방향 암호화 사용하기

❖ 공개키 암호 (public key encryption)

- 2개의 키를 사용하는 양방향 암호이다.
- 제인의 개인키(private key) : 오직 제인만이 알 수 있다.
- 제인의 공개키(public key) : 누구나 알 수 있다.

❖ 공개키 암호를 이용하는 두 가지 방법

- 개인키로 암호화 – 공개키로 복호화
  - 이는 데이터 암호화가 목적이다.
- 공개키로 암호화 – 개인키로 복호화
  - 이는 데이터 무결성 보전이 목적이다.

❖ 공개키 암호를 이용하는 두 가지 방법

1. 공개키로 암호화
- 개인키로 복호화

2. 개인키로 암호화
- 공개키로 복호화

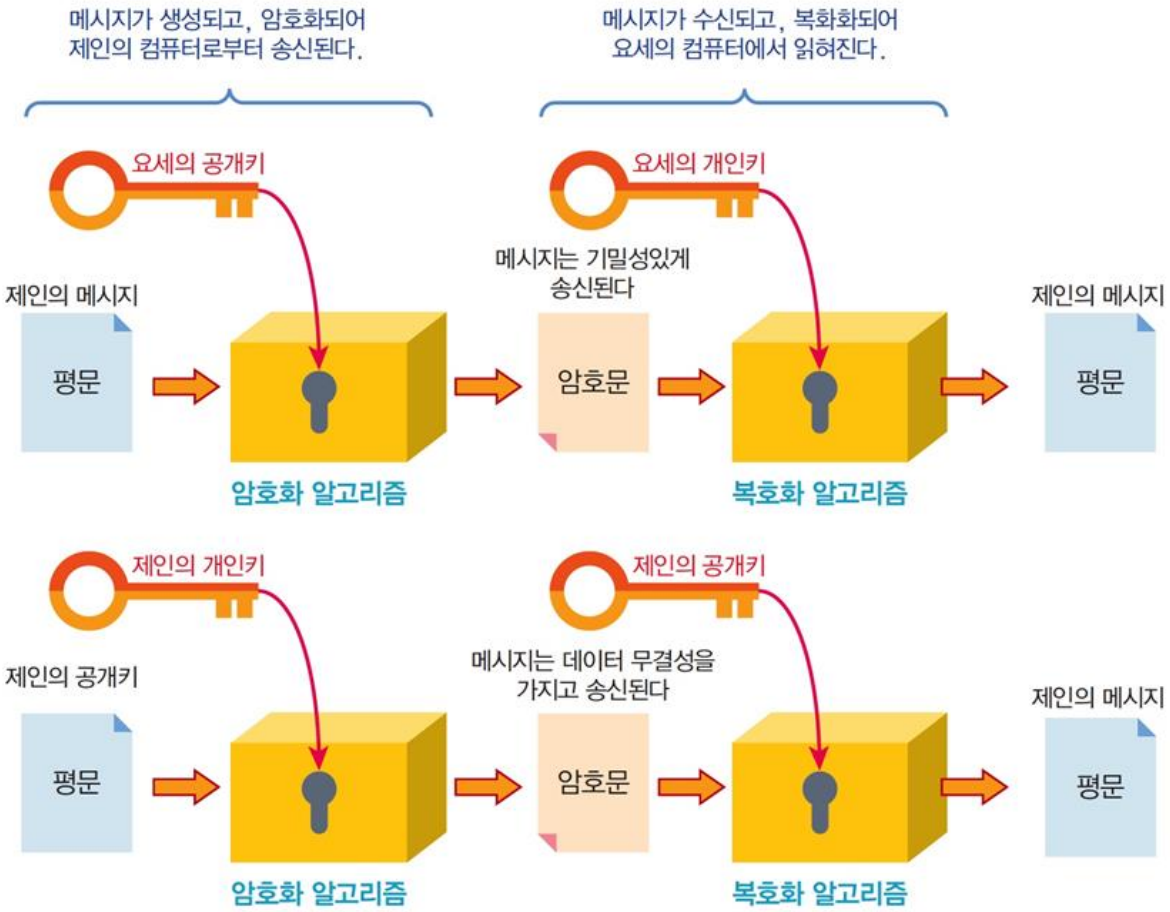


그림 12.6 공개키 암호를 사용하는 두 가지 방법

❖ **디지털 서명(digital signature)**

- 데이터 무결성, 소유자 무결성을 확신
- MD (Message Digest) : 메시지 축약. 메시지의 무결성 입증에 사용된다.

❖ **인증서(certificate)**

- 컴퓨터 내부에 존재하는 파일
- 공개키와 특정인의 신원을 연관시켜 준다.

❖ **인증기관(certificate authorities: CAs)**

- 신뢰할 만한 인증서의 근본을 서비스하는 회사

❖ 디지털 서명(digital signature)

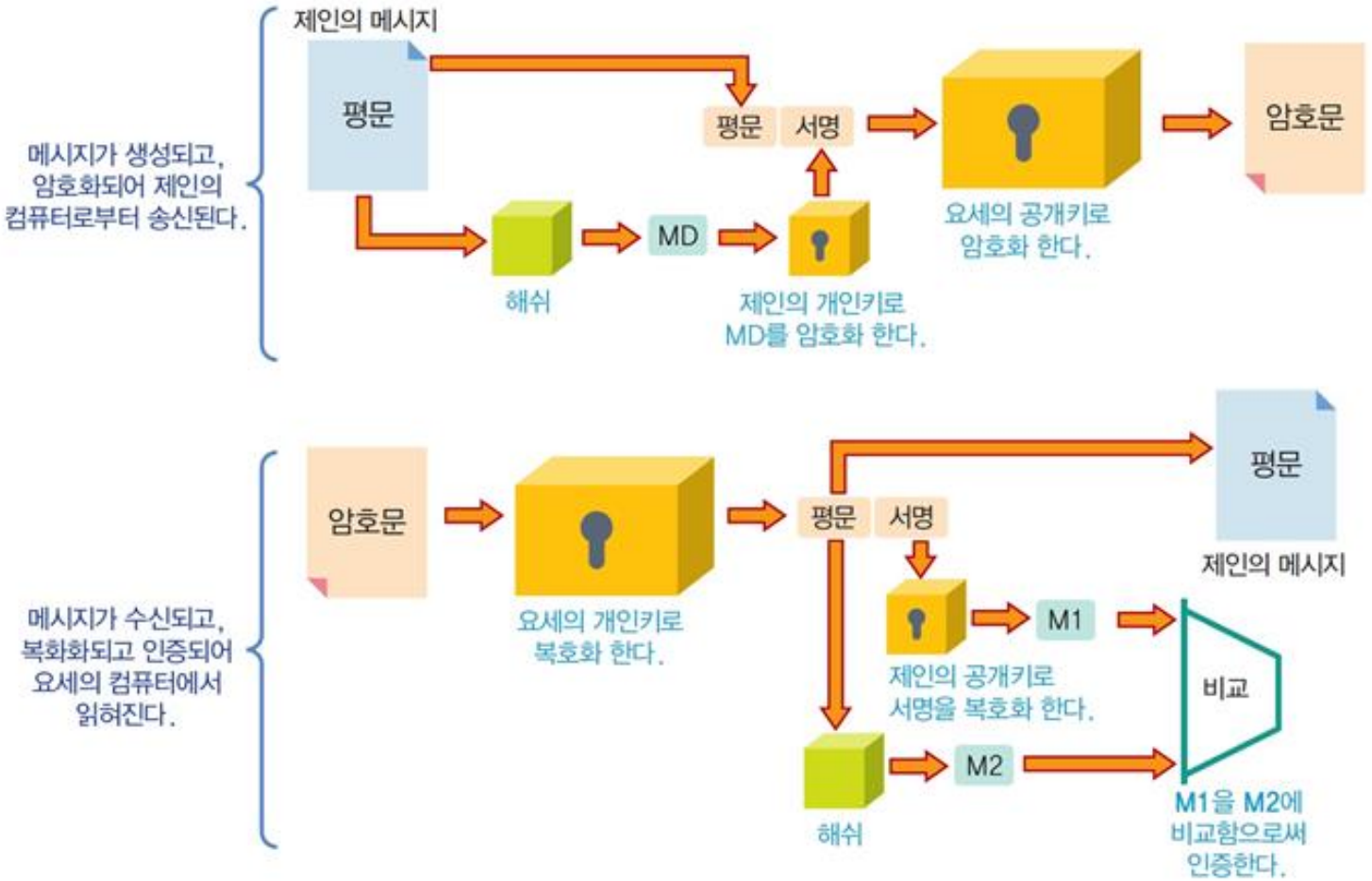


그림 12.7 디지털 서명을 포함하는 공개키 암호 사용하기

❖ 방화벽(firewall)

- 일부 네트워크 트래픽을 허용하거나 차단하도록 정의
- 방화벽의 두 가지 형태
  - 하드웨어 장치
  - 컴퓨터 시스템 내의 소프트웨어 방화벽

인바운드 규칙

이름	사용	작업
KakaoTalk	예	허용
KakaoTalk	예	허용
Microsoft Office Outlook	예	허용
nProtect Online Security Starter	예	허용
VMware Authd Service	예	허용
VMware Authd Service (private)	예	허용
VMware Workstation Server	예	허용
VMware Workstation Server (private)	예	허용
AllJoyn 라우터(TCP-In)	예	허용
AllJoyn 라우터(UDP-In)	예	허용
AllJoyn 라우터(UDP-In)	예	허용
ALYac	예	허용

◀ Windows OS 내부의 소프트웨어 방화벽

❖ **접근 제어 목록(access control list, ACL)**

- 블랙 리스트 : 공격자의 IP목록
- 스팸 필터 : 사용자의 행위를 기반으로 필터가 설정됨

❖ **거짓 양성(false positive)**

- 허용되어야 할 메시지를 차단하는 경우에 발생

❖ **컴퓨터 바이러스(computer virus)**

: 스스로를 복제하여 컴퓨터를 감염시키는 컴퓨터 프로그램

❖ **안티바이러스 소프트웨어(antivirus software)**

: 컴퓨터가 바이러스에 감염되는 것을 방지하기 위한 소프트웨어

❖ **비트 서명(bit signature)**

:각 바이러스가 가지는 특정한 비트열

❖ **소프트웨어 결함(software faults)**

: 사용자에게 피해를 야기할 수 있는 소프트웨어의 취약점

❖ **소프트웨어 갱신(software update)**

- 소프트웨어 결함을 해결하기 위한 방법

❖ **소프트웨어 패치(software patch)**

- 소프트웨어 갱신 방법
- 사용자는 자동 혹은 수동으로 갱신을 확인하여 적용하여야 한다.

❖ 발견 및 복구(detect and recover)

- 백업(backup)
  - 하드웨어 고장을 보완하기 위해 사용된다.
  - 보안 공격으로 파괴된 시스템을 복구한다.

❖ **로그 파일(log files)**

: 컴퓨터를 사용하는 동안 일어난 사건들이 기록된 파일

- 사용자 로그인
- 파일 사용
- 파일 읽기
- e-메일 송/수신

12.8 좋은 전략

1. 가장 취약한 연결부 보호하기
2. 공격 외관 축소하기
3. 철저하게 방어하기
4. 구획으로 나누기
5. 쉽게 신뢰하지 않기
6. 오픈 소프트웨어 사용하기

12.8.1 가장 취약한 연결부 보호하기

❖ 보안 시스템에서 가장 취약한 연결부는 사용자

❖ 사회공학(social engineering)공격 완화

- 보안 정책
- 보안 교육

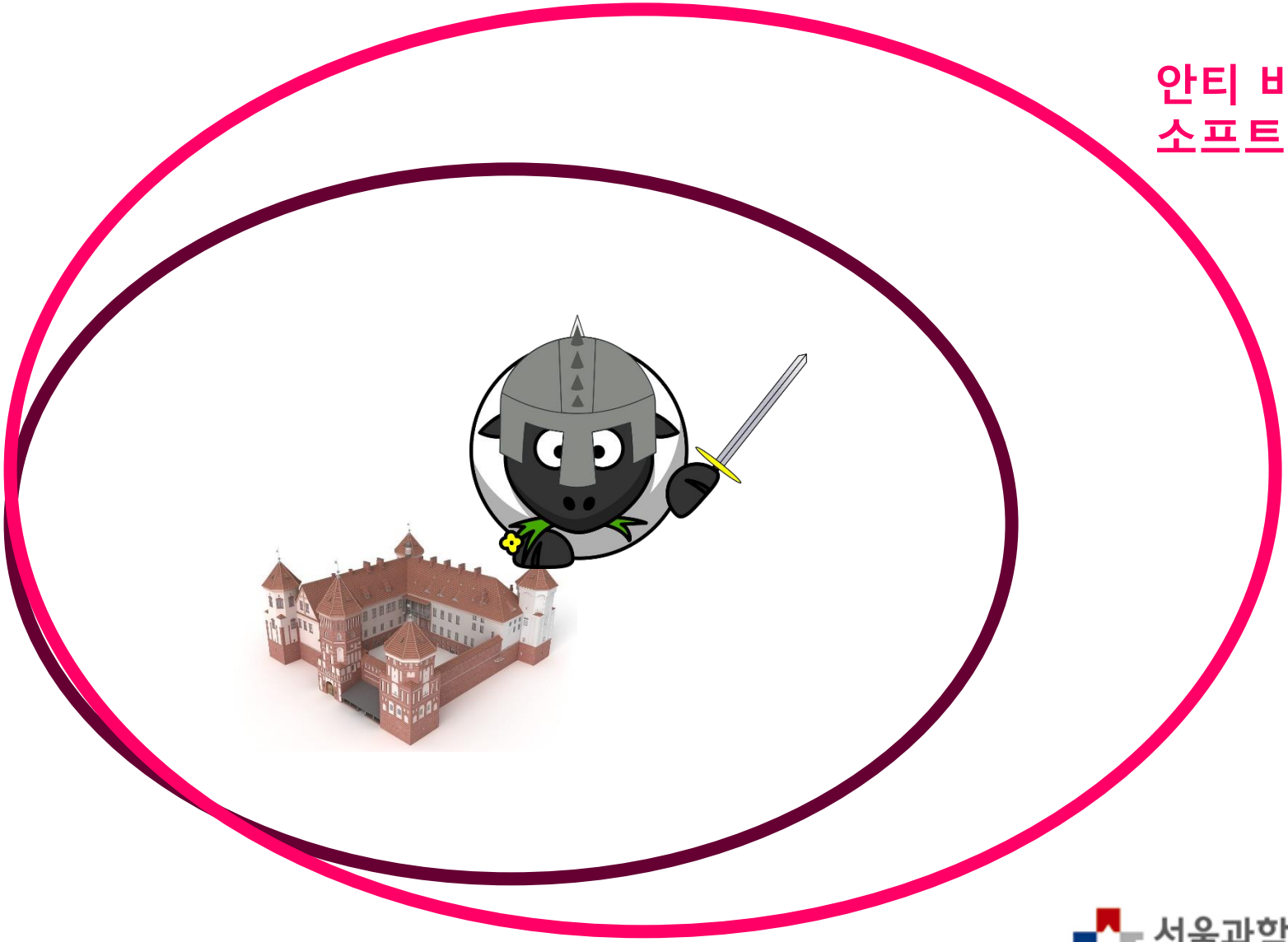
❖ **공격 외관(attack surface)**

: 잠재적인 공격 매개체를 포함하고 있는 취약점의 범위

❖ **공격 외관 축소하기**

- 인터넷을 사용하지 않을 때 네트워크에서 분리
- 불필요한 데이터는 안전하게 처리
- 파일 완전 삭제
- 안티바이러스 소프트웨어 사용

12.8.3 철저하게 방어하기



❖ **자산을 별도의 구획으로 세분화하여 독립적으로 보호하기**

❖ **알 필요가 있는 정책(need-to-know policy)**

- 공격 외관을 최소화한다.
- 권한 구획을 나누고, 꼭 필요한 권한만을 부여한다.

❖ **미러링(mirroring)**

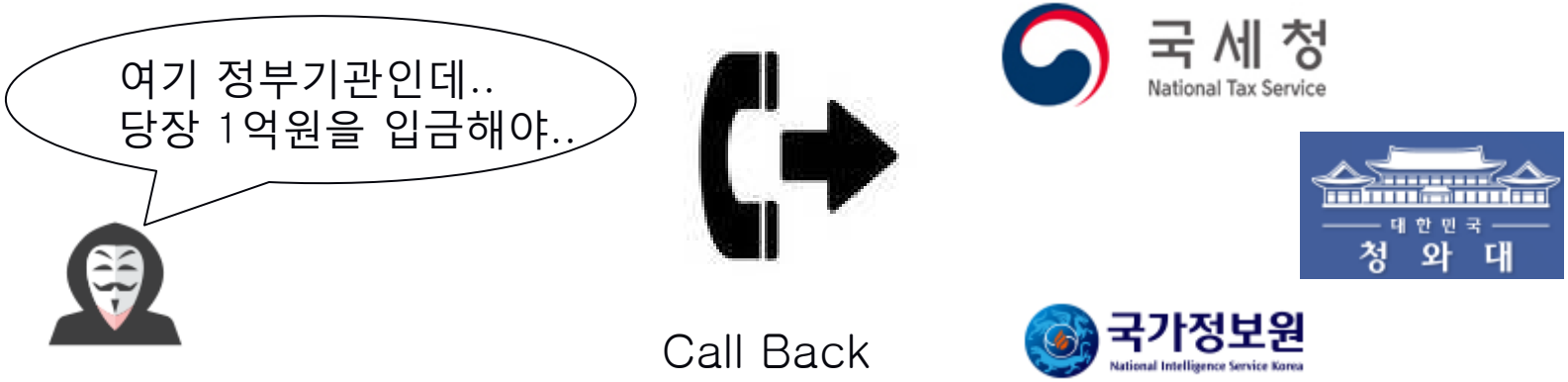
- 전체 데이터의 동일한 사본을 생성하여 별도로 저장한다.

❖ 피싱(phishing)

- private data와 fishing의 합성어
- 전자우편 또는 메신저를 신뢰할 수 있는 기관에서 보낸 것처럼 가장하여, 개인 정보를 빼내는 기법

❖ 콜백(callback)

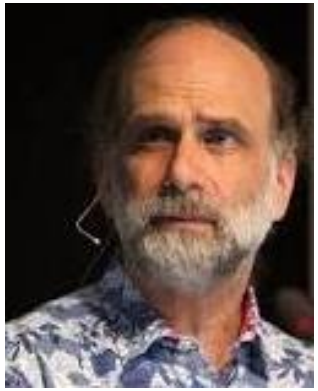
- 신뢰할 수 있는 주소로 다시 연락하여 정보를 확인한다.



❖ 공개 소프트웨어(open software)

- 소스코드가 공개되므로, 많은 사람들이 소프트웨어를 검사하여 취약점을 찾아낼 수 있다.
- 많은 공격시도를 견뎌낸 암호는 안전하다고 간주된다.

12.9 언제 이 내용을 사용할 것인가?



기술이 여러분의 보안 문제를 해결할 수 있다고 생각한다면, 여러분은 문제를 이해하지 못한 것이고 기술을 이해하지 못한 것이다.

- 브루스 슈나이어 (Bruce Schneier)

12.9 참고문헌

- 생각하는 프로그래밍, 윤성준,조상민 역, 인사이트, 2014
- 벤츠 타는 프로그래머, 정금호 저, 제이펍, 2013
- 컴퓨터과학이 여는 세계, 이광근 저, 인사이트, 2015
- 소프트웨어 전쟁, 백일승 저, 더하기북스,2015
- 김대수, “소프트웨어와 컴퓨팅 사고”, 생능출판, 2017
- 천인국, “어서와 파이썬은 처음이지!”, 인피니티북스, 2016