인덕대학교

운영체제 보안2
- 암호화

컴퓨터소프트웨어학과

김병국 교수

학습목표

- 파일을 암호화 할 수 있다.
- 체크섬 툴을 활용할 수 있다.

목차

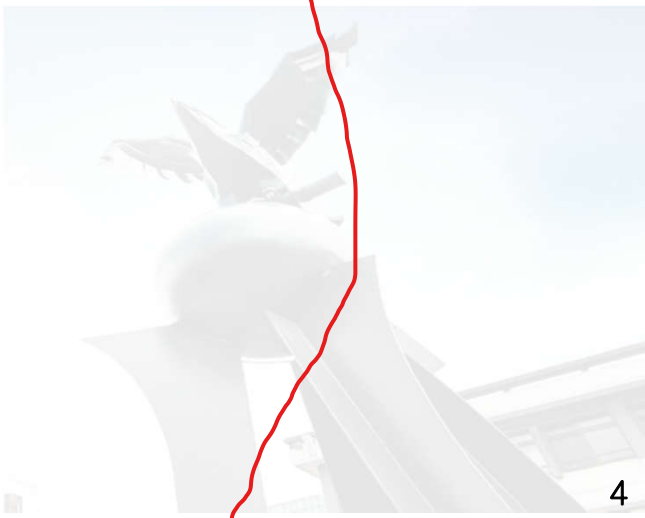
- 암호화
- 실습

4. 암호화 (1/4)

❑ 관련 기본 용어

- 평문(Plain Text) : 본래의 메시지
- 암호문(Cipher Text) : 암호화된 메시지
- 암호화(Encryption) : 평문에 대하여 암호문으로 변환하는 작업
- 복호화(Decryption) : 암호문에서 평문으로 변환하는 작업
- 키(Key) : 암호화 또는 복호화를 위한 열쇠

- 해쉬(Hash) : 암호화의 일종(복호화 불가), 결과물(암호문)들의 비교를 통해 이들이 동일한 평문임을 입증하는 용도로 사용



4. 암호화 (2/4)

❑ OpenSSL

- 네트워크기반의 암호화된 데이터 통신을 위한 TLS(Transport Layer Security)와 SSL(Secure Sockets Layer) 프로토콜을 위한 오픈소스
- Eric A. Young과 Tim Hudson이 개발
- C 언어로 구현된 라이브러리
- 암호화 관련 다양한 유틸리티 함수들을 제공
- 다양한 운영체제 지원 : 유닉스 계열 운영체제(솔라리스, 리눅스, BSD), 윈도우, Mac OS
- HTTPS 사이트를 포함한 다양한 인터넷 서버에서 폭넓게 사용 중

OpenSSL
Cryptography and SSL/TLS Toolkit

- 제공되는 암호화 알고리즘
  - 관련 명령어: openssl enc -help
  - 지원 암호화 방식: 200여개 (확인 명령: openssl enc -list)

4. 암호화 (3/4)

❑ 명령 옵션 (1/2)

- -<ciphername> : 사용할 암호화 알고리즘 이름
- -in <filename> : 입력 파일명
- -out <filename> : 출력 파일명
- -salt / -nosalt : salt 사용(기본값) / 미사용

salt 용도

- 암호와 과정에서 주어진 KEY 값에 일부 첨가제(salt) 넣고 처리.
- Rainbow 사전 해킹을 방지하려는 목적.

4. 암호화 (4/4)

❑명령 옵션 (2/2)

- -e : 암호화 수행(기본값)
- -d : 복호화 수행(-e 옵션과 같이 쓸 수 없음)
- -K <KEY> : 키 값 설정
- -iv <벡터값> : 초기 벡터값
- -p : 생성된 KEY와 초기 벡터값을 출력

5. Hexa 보기 툴

❑Hexa 출력

- 특수문자들에 대한 화면 출력 불가
- 텍스트 출력을 위한 터미널의 경우 특수문자는 별도의 기능을 수행
  - 예: ₩n ← 새로운 열로 이동
  - ₩r ← 가장 왼쪽 첫 칸으로 이동
  - ^j, ^m ← 엔터
- 명령어: hexdump
- 유용한 옵션: -C (대문자)
  - Hex 데이터에 대한 ASCII 문자도 같이 출력

6. 암호화 실습 (1/3)

❑RC4 암호화/복호화

- 암호화

```
kali@kali:~/OperatingSystem/12_3$ openssl enc -rc4 -K 1234567890 -in passwd.txt
 -out passwd.txt.enc -p
hex string is too short, padding with zero bytes to length
salt=7A802E49CD7F0000
key=12345678900000000000000000000000
kali@kali:~/OperatingSystem/12_3$
```

- 복호화

```
kali@kali:~/OperatingSystem/12_3$ openssl enc -d -rc4 -K 1234567890 -in passwd.t
xt.enc -out passwd.txt.dec -p
hex string is too short, padding with zero bytes to length
salt=7A70C44C167F0000
key=12345678900000000000000000000000
kali@kali:~/OperatingSystem/12_3$
```

6. 암호화 실습 (2/3)

❑AES 암호화/복호화

- 암호화

```
kali@kali:~/OperatingSystem/12_3$ openssl enc -aes-128-cfb -K 1234567890 -iv 0 -
in passwd.txt -out passwd.txt.enc
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
kali@kali:~/OperatingSystem/12_3$
```

- 복호화

```
kali@kali:~/OperatingSystem/12_3$ openssl enc -d -aes-128-cfb -K 1234567890 -iv
0 -in passwd.txt.enc -out passwd.txt.dec
hex string is too short, padding with zero bytes to length
hex string is too short, padding with zero bytes to length
```

6. 암호화 실습 (3/3)

❑ 체크섬

- MD5
- SHA256
- SHA512

```
kali@kali:~/OperatingSystem/12_3$ md5sum passwd.txt
4d4eb8b3af703a067b81ce7add1754cd  passwd.txt
kali@kali:~/OperatingSystem/12_3$ sha256sum passwd.txt
fd5cdca71803925e8596229439c89ba023c457e345e0daa2bc6c138f88c09102  passwd.txt
kali@kali:~/OperatingSystem/12_3$ sha512sum passwd.txt
eba5cedbff97f07b364d5b5815423b02a66beee190e7c6af132335697f2421795f33b07a27baf98b
b929a274f1d9ca618300649700ee3ea6c8efe203b4061e5c  passwd.txt
kali@kali:~/OperatingSystem/12_3$
```

수고하셨습니다.