교과목 : 정보보호

1. 정보보호 개요

2023학년도 2학기
Suk-Hwan Lee

References

Textbook
- Mark Stamp, Information Security: Principles and Practice, Second edition, & Lecture Note
- William Stallings, Cryptography and Network Security, Seventh Edition

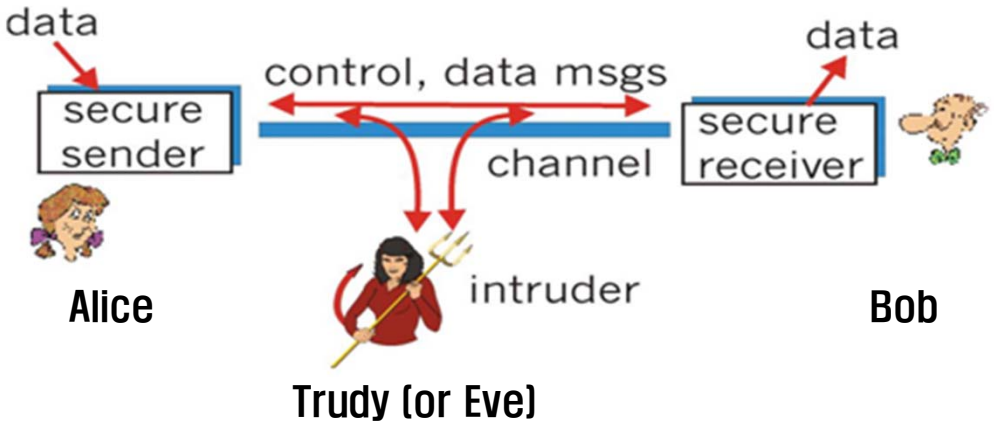
참조
- Stanford Univ., https://crypto.stanford.edu/~dabo/courses/OnlineCrypto/
- 부산대, Computer Security, Lecture Note
- 단국대, Introduction to Software Security, Lecture Note
- 명지대, Computer Security, Lecture Note
- 서울과학기술대, Information Protection Theory, Lecture Note
- York Univ. Network Security & Forensics, Lecture Note
- 해시넷, http://www.hash.kr/
- Wikipedia
- Cryptographics, https://cryptographics.info/all-cryptographics/#
- etc.....

Python cryptography
- https://www.tutorialspoint.com/cryptography_with_python/cryptography_with_python_modules_of_cryptography.htm
- https://pypi.org/project/cryptography/
- https://cryptography.io/en/latest/
- etc....

1. The Cast of Characters

- Alice and Bob are the good guys
- Trudy is the bad guy

  (Trudy is our generic "intruder")



Alice's Bank

- Alice opens Alice's Online Bank (AOB)
- What are Alice's security concerns?
- If Bob is a customer of AOB, what are his security concerns?
- How are Alice and Bob concerns similar? How are they different?
- How does Trudy view the situation?

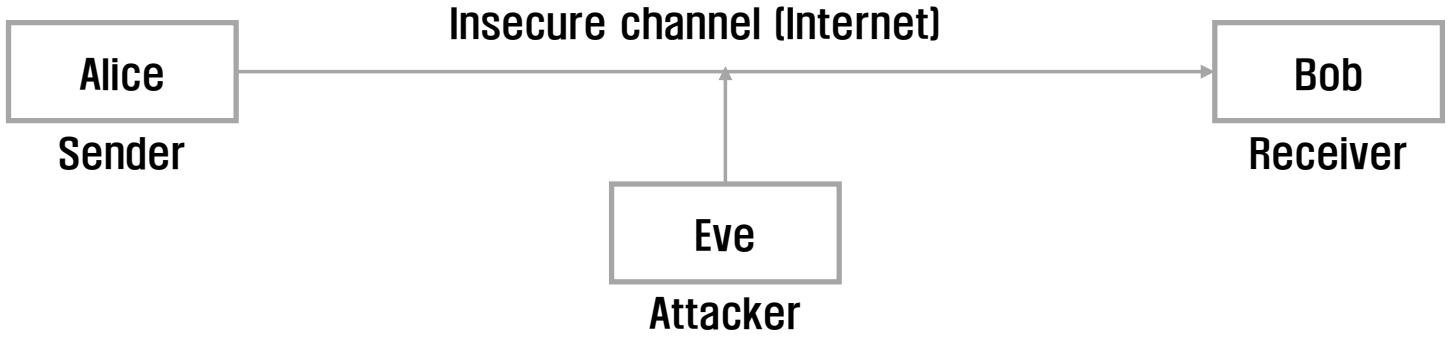
1. The Cast of Characters

- Most common characters are Alice, Bob, Eve, Trudy, etc.
- Other characters;
  - 홀수번째 알파벳에는 여성 이름을, 짝수번째 알파벳에는 남성 이름을 사용하는 게 일반적이다.

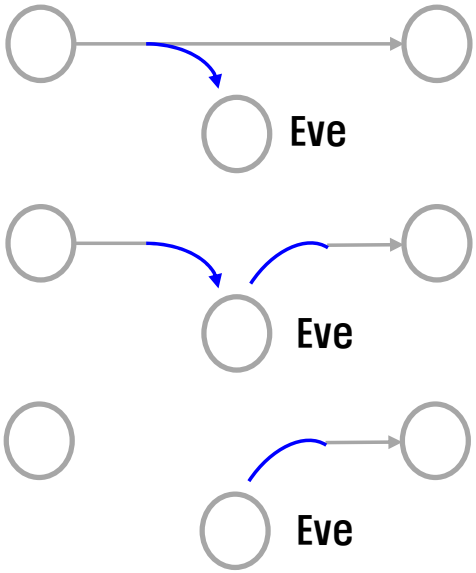
- ✓ Alice and Bob : 통신 과정의 첫번째와 두번째 당사자, 보통 앨리스가 밥에게 메시지를 보내려 한다고 가정
- ✓ Carol, Carol, Charlie : 통신 과정의 세 번째 당사자
- ✓ Chuck : 통신 과정의 악의있는 세 번째 당사자
- ✓ Craig : 비밀번호를 훔치려는 자
- ✓ Dave, Dan, David : 통신 과정의 네 번째 당사자
- ✓ Eve : '엿듣는 사람'이라는 뜻의 'eavesdropper'에서 온 것이며, 소극적 공격자
- ✓ Faythe : 신뢰할만한 조언자, 통신 과정의 여섯번째 당사자로 Frank를 쓴다.
- ✓ Grace : Government Representitave
- ✓ Heidi : 멍청한 암호제작자(mischievous designer)
- ✓ Isaac : ISP(Internet Service Provider), Ivan : Issuer
- ✓ Justin : 법원(justice system)
- ✓ Mallory : 악의적인(malicious), 적극적 공격자
- ✓ Matilda : Merchant
- ✓ Oscar : Opponent, Olivia : Oracle
- ✓ Peggy : Prover, Plod : police
- ✓ Sybil : 익명 공격자(pseudonymous attacker)
- ✓ Trudy : 침입자(intruder)
- ✓ Trent : trusted arbitrator
- ✓ Victor : 검증자 Verifier
- ✓ Zoe : 암호 프로토콜의 맨 마지막 당사자

[출처] Wikipedia, https://en.wikipedia.org/wiki/Alice_and_Bob

Basic Communication Scenario for Cryptography



Threats



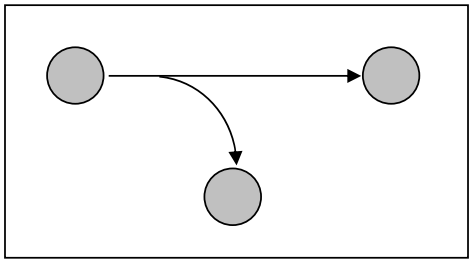
Eavesdropping
→ **Confidentiality** (기밀성으로 방지)

Modification
→ **Integrity** (무결성으로 방지)

Impersonation
→ **Authentication** (인증으로 방지)

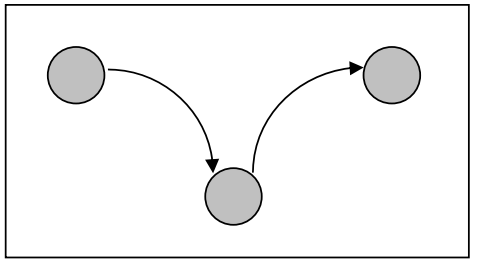
Confidentiality (or Privacy) (기밀성)

- Eve should not be able to read Alice's message to Bob
- *AOB must prevent Eve(Trudy) from learning Bob's account balance*
- Confidentiality: prevent unauthorized reading of information

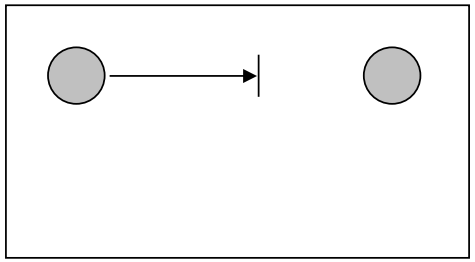


(Data) Integrity (무결성)

- Bob want to be sure that Alice's message has not been altered
- i.e. contain no modification, insertion or deletion
- *Trudy must not be able to change Bob's account balance*
- *Bob must not be able to improperly change his own account balance*
- Integrity: prevent unauthorized writing of information



Availability (가용성)



- A system or a system resource should be accessible and usable
  - ✓ Upon demand by an authorized system entity,
  - ✓ according to performance specifications for the system

- AOB's information must be available when needed
- Alice must be able to make transaction
  - ✓ If not, Bob'll take his business elsewhere
- Availability: Data is available in a timely manner when needed
- Availability is a "new" security concern
  - ✓ In response to denial of service (DoS)

Authentication (인증)

- Bob wants to be sure that his communication partner is Alice

Non-repudiation (부인방지)

- Alice cannot claim that she did not send the message, if she actually sent it.
- This service is particularly important in electronic commerce applications, where it is important that a consumer cannot deny the authorization of a purchase.

Access Control (접근제어)

- Prevention of unauthorized use of a resource
- This service controls
  - ✓ who can have access to a resource
  - ✓ under what conditions access can occur
  - ✓ and what those accessing the resource are allowed to to

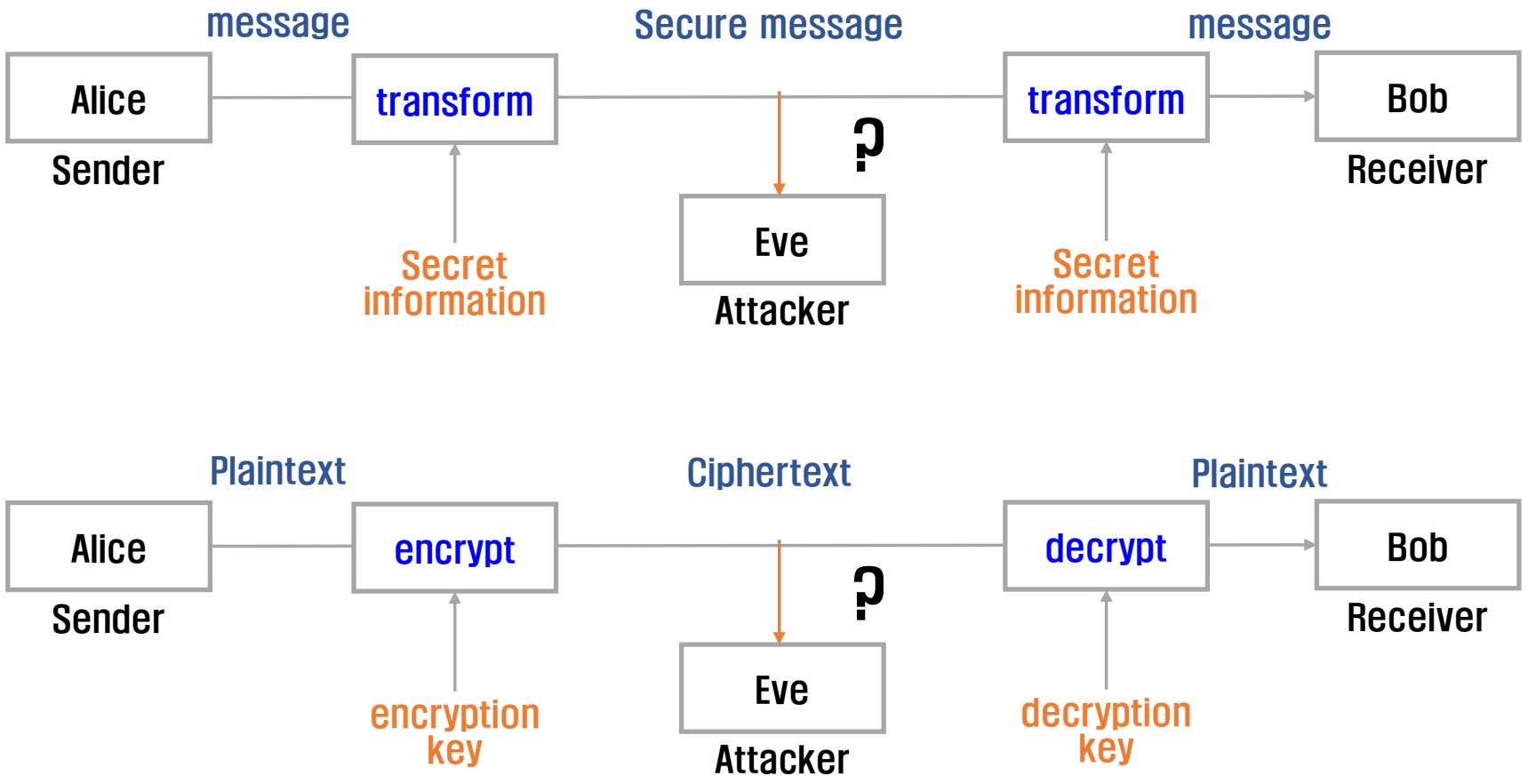
Cryptographic Mechanisms

Confidentiality → Encryption algorithm
- ✓ Classical cryptosystems
- ✓ Symmetric key algorithm (DES, AES)
- ✓ Public key algorithms (RSA, ElGamal)

Integrity
Authentication → Digital Signature
- ✓ RSA signature
- ✓ DAS

MAC(Message Authentication Code)

Confidentiality Model



3. Beyond CIA

- CIA are only beginning of the Information Security

- Case 1: when Bob logs on his computer
  - ✓ How does Bob's computer know that "Bob" is really Bob and not Trudy?
- Bob's password must be verified
  - ✓ This requires some clever cryptography
- What are security concerns of pwds?
- Are there alternatives to passwords?

3. Beyond CIA

- CIA are only beginning of the Information Security

- Case2: when Bob logs into AOB
  - ✓ how does AOB know that "Bob" is really Bob?
- As before, Bob's password is verified
- Unlike standalone computer case, network security issues arise
- What are network security concerns?
  - ✓ Protocols are critically important
  - ✓ Crypto also important in protocols

- Once Bob is *authenticated* by AOB, then AOB must restrict actions of Bob
  - ✓ Bob can't view Charlie's account info
  - ✓ Bob can't install new software, etc.
- Enforcing these restrictions is known as authorization
- **Access control (접근제어)** includes both authentication(인증) and authorization(권한)

3. Beyond CIA

- Cryptography, protocols, and access control are implemented in **software**
- What are security issues of software?
  - ✓ Most software is complex and buggy
  - ✓ Software flaws lead to security flaws
  - ✓ How to reduce flaws in software development?

- Some software is intentionally evil
  - ✓ Malware: computer viruses, worms, etc.
- How do the malwares work?
- What can Alice and Bob do to protect themselves from malware?
- What can Trudy do to make malware more "effective"?

3. Beyond CIA

- Operating systems enforce security
  - ✓ For example, authorization
- OS: large and complex software
  - ✓ Window 10 has about 50 Million lines of code! (Microsoft community)
  - ✓ Subject to bugs and flaws like any other software
  - ✓ Many security issues specific to OSs
  - ✓ Can you trust an OS?

4. Security Life Cycle

- First defining a *security policy*
- Then choosing some *mechanism* to enforce the policy
- Finally providing *assurance* that both the mechanism and the policy are sound

- Security/policy: What the sys supposed to do?
- Implementation/mechanism: How does it do it?
- Correctness/assurance: Does it really work?
- Human nature: Can the sys survive "clever" user?
- The focus of the text book (lecture)
  - Implementation/mechanism
  - Why?

A security policy is a definition of what it means to be secure for a system, organization or other entity.

(https://en.wikipedia.org/wiki/Security_policy)

4. Major parts

- The lecture consists of four major parts

  - ✓ Cryptography
  - ✓ Access control
  - ✓ Protocols
  - ✓ Software

4. Major parts

Cryptography

- Secret codes”
- The book covers
  - ✓ Classic cryptography
  - ✓ Symmetric ciphers
  - ✓ Public key cryptography
  - ✓ Hash functions
  - ✓ Advanced cryptanalysis

Access Control

- Authentication
  - ✓ Passwords
  - ✓ Biometrics and other
- Authorization
  - ✓ Access Control Lists and Capabilities
  - ✓ Multilevel security (MLS), security modeling, covert channel, inference control
  - ✓ Firewalls and Intrusion Detection Systems

Protocols

- Simple authentication protocols
  - ✓ “Butterfly effect” — small change can have drastic effect on security
  - ✓ Cryptography used in protocols
- Real-world security protocols
  - ✓ SSL (Secure Sockets Layer) / TLS (Transport Layer Security) / HTTPS (Hyper Text Protocol Secure)
  - ✓ IPSec (Internet Protocol Security)
  - ✓ Kerberos (computer-network authentication protocol)
  - ✓ GSM security (Global System for Mobile Communications, ETSI)

Software

- Software security-critical flaws
  - ✓ Buffer overflow
  - ✓ Other common flaws
    - Incomplete Mediation
    - Race Conditions
- Malware
  - ✓ Specific viruses and worms
  - ✓ Prevention and detection
  - ✓ The future of malware
- Software reverse engineering (SRE)
  - ✓ How hackers "dissect" software
- Digital rights management (DRM)
  - ✓ Shows difficulty of security in software
  - ✓ Also raises OS security issues
- Limits of testing
  - ✓ Open source vs closed source

Software

- Operating systems
  - ✓ Basic OS security issues
  - ✓ "Trusted" OS requirements
  - ✓ NGSCB["n-scub"]: Microsoft's trusted OS for PC
    - Next Generation Secure Computing Base
- Software is a big security topic
  - ✓ Lots of material to cover
  - ✓ Lots of security problems to consider

General Notation for Cryptography

[Textbook] William Stallings, Cryptography and Network Security, Seventh Edition

Symbol	Expression	Meaning
D, K	D(K, Y)	Symmetric decryption of ciphertext Y using secret key K
D, PR_a	D(PR_a, Y)	Asymmetric decryption of ciphertext Y using A's private key PR_a
D, PU_a	D(PU_a, Y)	Asymmetric decryption of ciphertext Y using A's public key PU_a
E, K	E(K, X)	Symmetric encryption of plaintext X using secret key K
E, PR_a	E(PR_a, X)	Asymmetric encryption of plaintext X using A's private key PR_a
E, PU_a	E(PU_a, X)	Asymmetric encryption of plaintext X using A's public key PU_a
K		Secret key
PR_a		Private key of user A
PU_a		Public key of user A
MAC, K	MAC(K, X)	Message authentication code of message X using secret key K
GF(p)		The finite field of order p, where p is prime.The field is defined as the set Z_p together with the arithmetic operations modulo p.
GF(2^n)		The finite field of order 2^n
Z_n		Set of nonnegative integers less than n
gcd	gcd(i, j)	Greatest common divisor; the largest positive integer that divides both i and j with no remainder on division.

$$\mathbf{C} = \mathrm{E}(\mathbf{K}, \mathbf{P}) = \mathbf{PK} \bmod 26$$

$$\mathbf{P} = \mathrm{D}(\mathbf{K}, \mathbf{C}) = \mathbf{CK}^{-1} \bmod 26 = \mathbf{PKK}^{-1} = \mathbf{P}$$

$$C = \mathrm{E}(K_2, \mathrm{E}(K_1, P))$$

$$P = \mathrm{D}(K_1, \mathrm{D}(K_2, C))$$

General Notation for Cryptography

Symbol	Expression	Meaning
mod	$a \bmod m$	Remainder after division of a by m
mod, $\equiv$	$a \equiv b \pmod m$	$a \bmod m = b \bmod m$
mod, $\not\equiv$	$a \not\equiv b \pmod m$	$a \bmod m \neq b \bmod m$
dlog	$\text{dlog}_{a,p}(b)$	Discrete logarithm of the number b for the base a (mod p)
φ	$\phi(n)$	The number of positive integers less than n and relatively prime to n. This is Euler's totient function.
Σ	$\sum_{i=1}^{n} a_i$	$a_1 + a_2 + \cdots + a_n$
Π	$\prod_{i=1}^{n} a_i$	$a_1 \times a_2 \times \cdots \times a_n$
$\mid$	$i \mid j$	i divides j, which means that there is no remainder when j is divided by i
$\mid, \mid$	$\mid a \mid$	Absolute value of a

General Notation for Cryptography

Symbol	Expression	Meaning
$\|$	$x \| y$	x concatenated with y
$\approx$	$x \approx y$	x is approximately equal to y
$\oplus$	$x \oplus y$	Exclusive-OR of x and y for single-bit variables; Bitwise exclusive-OR of x and y for multiple-bit variables
$\lfloor, \rfloor$	$\lfloor x \rfloor$	The largest integer less than or equal to x
$\in$	$x \in S$	The element x is contained in the set S.
$\longleftrightarrow$	$A \longleftrightarrow (a_1, a_2, \ldots a_k)$	The integer A corresponds to the sequence of integers $(a_1, a_2, \ldots a_k)$