Introduction

Example: Online 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’s and Bob’s concerns similar? How are they different?
- How does an attacker view the situation?

Bob’s security concerns(1)

- When I connect to the AOB site, can I trust that it is really the real AOB bank site?
- Whenever I want to do any transaction, can I access to the bank?
- Isn’t there any risk that anyone can access to my account with my permission?
- Aren’t my secrete information, such as password, PIN and the like, revealed to anyone else?

Bob’s security concerns(2)

- If I withdraw or deposit money, is the exact amount of money extracted or added from/into my account? Isn’t there any possibility for the amount of money to be altered during transaction?
- Is my personal information kept in secret? Might anyone know any my personal account information and transactions with my acknowledgement?
- Ans so on ...

Alice’s Security concerns(1)

- As an online banking service provider, she should address Bob’s security concerns.
- In addition, she should answer for the following security concerns.
- When any customer access to his account, is he a really authorized user?
- How can I limit any legal user’s access only to his own legitimate resources that he is entitled to do?

Alice’s Security concerns(2)

- How can I protect my assets and all customer information from any illegal penetration (or any unexpected accident such as disasters)?
- If an user withdraw $10,000 and later deny such transaction, how can I verify that his denial is false?
- How can I operate my bank 24/7 with an unexpected glitch?
- And so on ...

Bob's security concerns(1)

- ❑ When I connect to the A… I trust that it is really the real AOB bank s…
- ❑ Whenever I want to do any transaction… to the bank?
- ❑ Isn't there any risk that …ccess to my account with my permissio…
- ❑ Aren't my secrete information, such as password, PIN and the like, revealed to anyone else during transaction?

Server authentication

availability

user authentication

confidentiality

Bob's security concerns(2)

Integrity

- If I withdraw or deposit money, is the exact amount of money extracted or added from/i unt? Isn't there any possibility for the oney to be altered during transaction?

privacy

- Is my personal information kept in secret all the time? Might anyone know any my personal account information and transactions with my acknowledgement?
- Ans so on ...

Confidentiality

- Confidentiality, Integrity, and Availability
  - They are often call CIA.
- **Confidentiality**
  - prevent unauthorized *reading* of information

Integrity

- Alice and Bob must know the improper change of his own account balance whenever it happens.
- **Integrity:** detect unauthorized *modification(falsification)* of information

Availability

- The online bank system must be available whenever it’s needed online.
- **Availability:** the system should be available when needed
- A typical attack on availability is the Distriubted Denial of service (DoS) attacks.

Alice's Security concerns(1)

- As an online banking service provider, she should address Bob's security concerns.
- In addition, she should answer for the fol security con

client authentication

- When any o his account, is he a really authoriz

authorization

- How can I limit any legal user's access only to his own legitimate resources that he is entitled to do?

Alice’s Security concerns(2

access control

- How can I and all customer informati enetration (or any unexpected ac uch as disasters)?

non-repudiation

- If an user withdraw $10,000 and later deny such transaction, how can I verify that his denial is false?
- How can I operate my bank 24/7 with an unexpected glitch?
- And so on ...

Authentication

- How can Alice verify Bob? (client authentication)
- How can Bob verify Alice? (server authentication)
- Are there any other types of authentication?

Access Control

- **Access control** includes both authentication and authorization

List of security requirements for online banking

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Non-repudiation

Beyond access control(1)

- Is the system including servers well protected from any penetration including physical penetration?
  - It might be a minor concerns for the online banking system, since every server is located in physically protected places.
  - But devices are placed in unmanned, unprotected areas such as sensors or meters.
  - In that case we need to worry about any physical tampering and firmware protection, etc.

Beyond access control(2)

- And the security engineers need to worry about OS and database protection in the different senses from the security concerns that we considered before.

Software

- Cryptography, protocols, and access control are implemented in **software**
- What are security issues of software?
    - Real world software is complex and buggy
    - Software flaws lead to security flaws
    - How to reduce security flaws in software development?
    - And what about malware?

The People Problem

- People often break security
  - Both intentionally and unintentionally

Security Protocols

- In the online banking transaction, every information should be exchanged over the network between clients and servers.
  - Different from standalone transactions
- So, **network** security issues arise.
- How can we secure transactions over the network?
  - **Protocols** are critically important

List of security requirements for online banking

- Confidentiality
- Integrity
- Availability
- Authentication
- Authorization
- Non-repudiation
- Physical security
- OS(system) security
- Software
- People security

Conclusion

- Security problems are very complex in itself.
- Moreover, they are intertwined with many problems.
- The security requirements of one target system may be different from other target systems.
- So, there is no “the solution” for the problem.
- Rather, we need to view the security as the process.