Information Security
CS3002
(Sections BDS-7A/B, BSE-7A)
Lecture 03

Instructor: Dr. Syed Mohammad Irteza

Assistant Professor, Department of Computer Science

26 August, 2024

Basic Problems

- *Networks are insecure*: (most) communications are made in clear
- LANs operate in *broadcast*

- Geographical connections are *NOT* made through *end-to-end dedicated lines* but:
  - through *shared lines*
  - through third-party routers
  - *weak user authentication* (normally password-based)

- There is *no server authentication*
- Software contains many *bugs*!

Basic Problems

- Low problem understanding (i.e., *no awareness*)
- *Mistakes by human beings* (especially when overloaded, stressed, …)
- Human beings have a *natural tendency to trust*
- Complex interfaces / architectures *can mislead the user* and lead to *erroneous behaviors*
- *Performance decrease* due to the application of security (i.e., tradeoff)
- Ask for the (involuntary) user's participation to the attack action
- Usually *naive users* are targeted (e.g. "do immediately change your password with the following one, because your PC is under attack") ...
- But *experienced users* are targeted too (e.g. by copying an authentic mail but changing its attachment or URL)

Roots of Insecurity

- "Defensive strategies are reactionary"
- "Thousands - perhaps millions - of systems with weak security are connected to the Internet"
- "The explosion in use of the Internet is straining our scarce technical talent. The average level of system administrators has decreased dramatically in the last 5 years"
- "Increasingly complex software is being written by programmers who have no training in writing secure code"
- "Attacks and attack tools transcend geography and national boundaries"
- "The difficulty of criminal investigation of cybercrime coupled with the complexity of international law means that prosecution of computer crime is unlikely"

ICT Security

- ICT (*Information and Communication Technologies*) refers to *technologies that provide access to information through telecommunications*.
- ICT *security* is the set of *products, services, organization rules and individual behaviors* that protect the ICT system of a company.

- Three main components of any system are:
  - *Hardware*
  - *OS and applications*
  - *Communication*

  - Cloud - (Optional)

Security Design Principles

Principle of …

- Least Privilege
- Separation of privilege
- Fail-safe defaults
- Complete mediation
- Economy of mechanism
- Least Common Mechanism
- Psychological acceptability

Principle of Least Privilege

- Provide *bare minimum* privileges to a program or user to function properly
- *Temporary elevation* should be relinquished immediately
- *Granularity* of privileges

Advantage

- *Abuse of privileges* is restricted
- *Damage caused* by the compromised user or application is *reduced*

Separation of Privilege

- Access should *not* be *granted* based on a *single condition*
- *Multiple conditions* should be *required* to achieve access to restricted resources

Examples:

- *Two persons* to sign checks
- *Password login + OTC (one-time code)* to perform financial transactions

Fail-Safe Defaults

- The default configuration of a system should have a conservative approach…
  - *Default access* to an object is *none*
  - *Explicit access* to an object *should be given*

Examples

- Access Control Lists
- Firewall rules

Complete Mediation

- Instead of *one time check*, every access to a resource must be checked for compliance with a protection scheme
- Restricts the *caching* of information
- *Security vs performance* issue (or tradeoff)

- *Whenever a subject attempts to read an object, the operating system should mediate the action.* First, it determines if the subject can read the object. If so, it provides the resources for the read to occur. If the subject tries to read the object again, the system should again check that the subject can still read the object. Most systems would not make the second check. They would cache the results of the first check, and base the second access upon the cached results.
    - UNIX file descriptor
    - DNS cache poisoning

Principle of Economy of Mechanism

- Simplicity in design and implementation of security measures

- A *simple secure framework* provides…
  - Fewer errors
  - Development, testing and verification of security measures is easy
  - Less assumptions

Least Common Mechanism

- In shared systems with multiple users, mechanisms allowing resources to be *shared* by more than one user should be *minimized*
- *Separate channel* for users
- *Separation of network resources*

Principle of psychological acceptability

- Security mechanism should *not make the resources difficult to access*
- User interface should be *well designed* and *intuitive*
- Security related setting should consider the *expectation* of *ordinary users*

Secure Communication and Storage

- Vulnerable components
  - Channels
  - Processes (clients, servers)

- Security properties:
  - Authentication
  - Authorization
  - Confidentiality
  - Integrity
  - Availability

Types of cryptographic functions

- *Secret/symmetric key cryptographic* function
  - Uses 1 key
  - Fast computation

- *Public/Asymmetric key cryptographic* function
  - Uses 2 keys
  - Slow computation

- *Hash functions*
  - Uses no keys
  - Very fast computation

Key Terms (Chapter 8, Whitman/Mattord, 6ed)

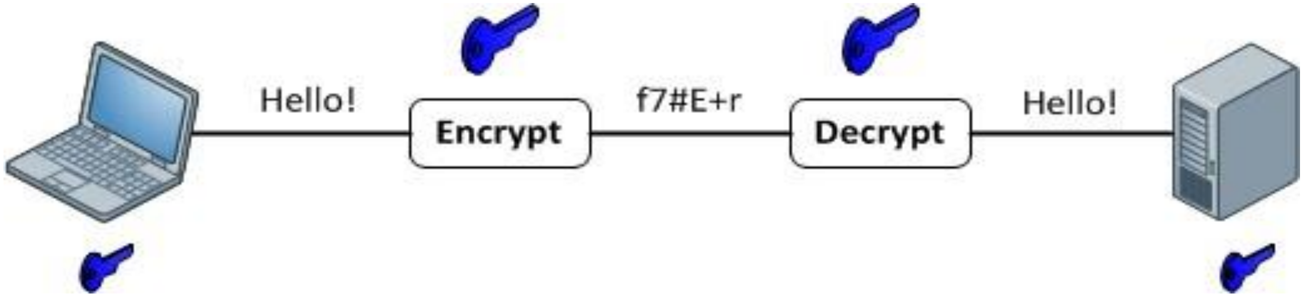
- Cryptanalysis: The process of obtaining the *plaintext message* from a *ciphertext message* without knowing the *keys* used to perform the encryption.
- Cryptography: The process of *making* and *using codes* to secure information
- Cryptology: The *field of science* that *encompasses cryptography* and *cryptanalysis*

Key terms

- *Plaintext*
  - Readable message or data that needs to be protected
- *Encryption Algorithm*
  - Algorithm to perform various substitutions and transformations on the plaintext
- *Secret key*
  - Used as input to the algorithm, transformations depend on the key
- *Ciphertext*
  - Scrambled message produced as output
- *Decryption Algorithm*
  - Produces the original plaintext

Symmetric/secret key encryption

- Also called ***conventional cryptography***
- Sender and receiver must both know the *secret key*
- Uses techniques like *confusion and diffusion* to encrypt/decrypt data



Symmetric encryption uses

- Transmitting over *secure channel*
- Secure storage on *insecure media*

- Authentication
  - *Strong authentication*: prove the knowledge of a secret without revealing it

- Integrity check
  - Checksum* vs cryptographic checksum
  - Message Authentication Code (MAC)/MIC

* see https://en.wikipedia.org/wiki/Internet_checksum (*if you have not studied Comp. Networks*)

Substitution Ciphers

- A *substitution cipher* exchanges one value for another—for example, it might exchange a letter in the alphabet with the letter three values to the right, or it might substitute one bit for another bit four places to its left.
- A 3-character substitution to the right (i.e., Caesar Cipher) results in the following transformation of the standard English alphabet.

Initial alphabet: ABCDEFGHIJKLMNOPQRSTUVWXYZ yields

Encryption alphabet: DEFGHIJKLMNOPQRSTUVWXYZABC

- Within this substitution scheme, the plaintext MOM would be encrypted into the ciphertext PRP

Substitution Ciphers

- Resources:
  - Caesar Cipher (Shift) - Online Decoder, Encoder, Solver, Translator (dcode.fr)
  - 16.2: Substitution Ciphers - Mathematics LibreTexts