Sistem Terdistribusi 9

Security

Attention

- All information, tools, methods presented here are given for educational or security class purposes

The Security Problem

- Security must consider **external environment** of the system, and **protect** the system resources
- **Intruders** (crackers) attempt to **breach security**
- **Threat** is potential security violation
- **Attack** is attempt to breach security
- Attack can be **accidental** or **malicious**
- Easier to protect against **accidental** than malicious misuse

Security

- Everybody wants information
- Security requirements have changed
- Past: physical & administrative mechanisms
  - Locks
- Current: Automated tools with better mechanism
  - ACL
- Future: Secure communications
  - HTTPS
  - SSL/SSH
- Security technologies

Kenapa keamanan sulit?

- One hole is enough to blow the whole system (vulnerability)
- People are often the weakest link
  - Social engineering
- Complex to set up and use
  - People won't use complex system

Komponen Security (CIA-AN)

- **Confidentiality**: akses terhadap sistem komputer tidak boleh **dilakukan** oleh unauthorized users
- **Integrity**: aset sistem komputer tidak boleh **dimodifikasi** oleh unauthorized users
- **Availability**: Sistem harus dapat **selalu online/ada** sehingga dapat diakses oleh authorized users

Tambahan

- **Authenticity**: sistem mengetahui **asal muasal** suatu objek atau asal muasal modifikasi yang terjadi
- **Non-repudiation**: seseorang/sesuatu tidak dapat menyanggah bahwa dia melakukan sesuatu

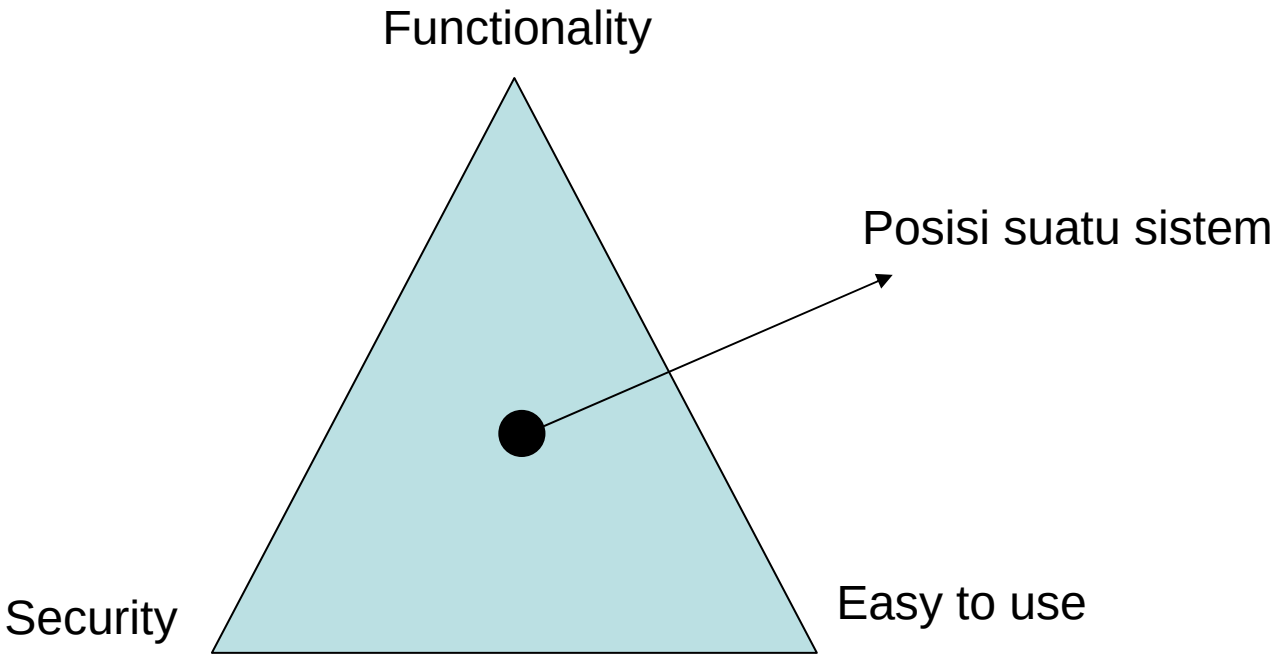
Ancaman

- Ancaman (**threat**) adalah:
  - Seseorang, sesuatu, kejadian atau ide yang menimbulkan bahaya bagi suatu asset
  - Threat muncul dari vulnerability (kelemahan sistem & desain)
- Serangan (**attack**) adalah realisasi dari threat.
- Klasifikasi threats:
  - Disengaja (mis. hacker penetration);
  - Tidak disengaja (mis. Mengirimkan file yang sensitif ke alamat yang salah)
- Threats yang disengaja dapat dibagi lagi :
  - Pasif – tidak kontak langsung (mis. monitoring, wire-tapping,);
  - Aktif – kontak langsung (mis. mengubah nilai transaksi finansial)

Tujuan Security

- **Prevention - Penjagaan**
  - Prevent attackers from violating security policy
- **Detection - Deteksi**
  - Detect attackers' violation of security policy
- **Recovery - Mereparasi**
  - Stop attack, assess and repair damage
  - Continue to function correctly even if attack happen

Segitiga Sistem



Tahapan penyerangan

- **Reconnaissance**
  - Mengumpulkan data mengenai target
    - Aktif dan pasif
- **Scanning**
  - Tanda dimulainya serangan, berusaha mencari jalan masuk
  - Misal scanning port
- **Gaining access**
  - Mendapatkan target
- **Maintaining access**
  - Mempertahankan akses dgn berbagai cara termasuk menanamkan program dan memperbaiki kelemahan
- **Covering tracks**
  - Menutupi jejak mereka

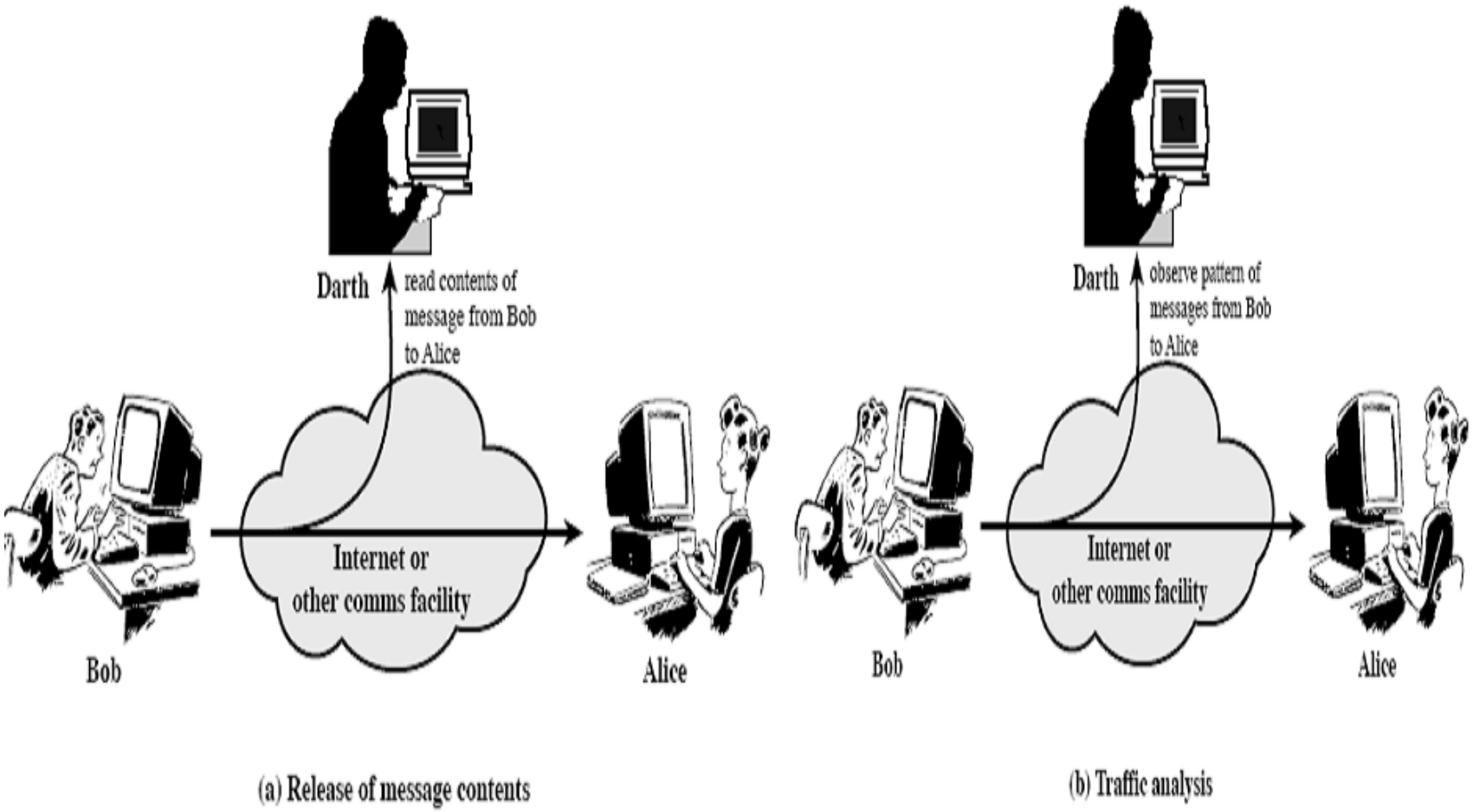
Level Serangan

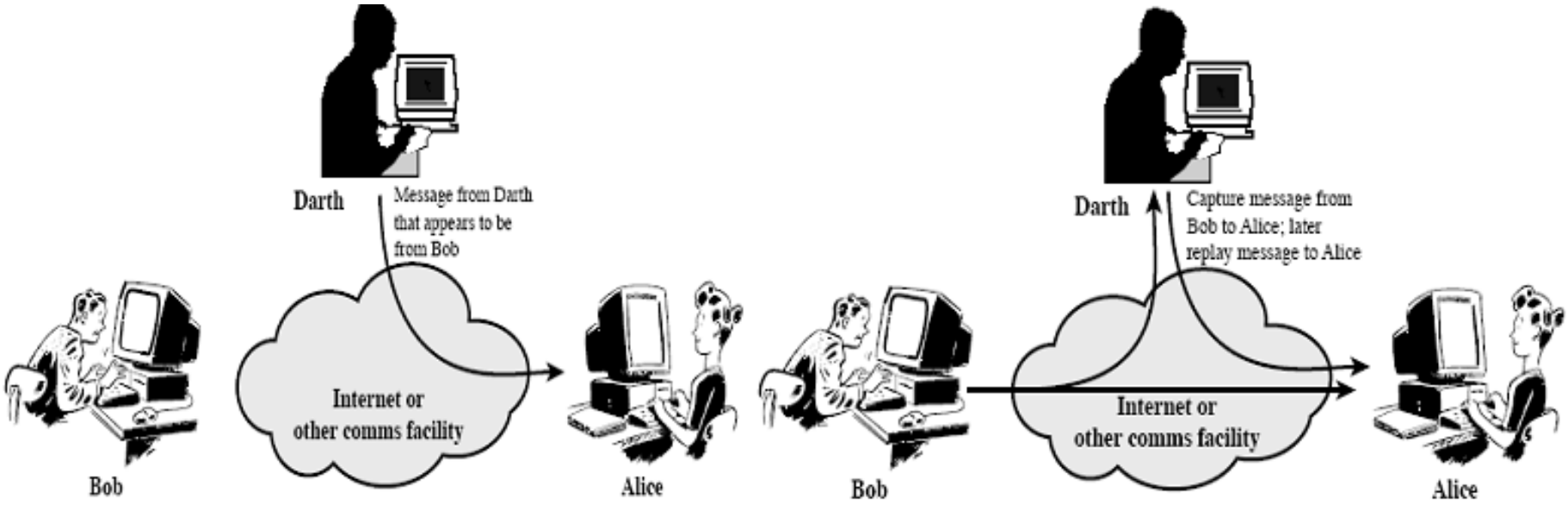
- Level Sistem Operasi
  - Kode konfigurasi umum
  - Patch & upgrade
- Level aplikasi
  - Aplikasi2 umum
  - Patch, Antivirus & Upgrade
- Level Shrink Wrap code
  - Menggunakan program2 bantu untuk serangan

System and Network Threats

- **Worms** – use spawn mechanism; standalone program
- Internet worm
  - Grappling hook program uploaded main worm program
- **Port scanning**
  - Automated attempt to connect to a range of ports on one or a range of IP addresses
- **Denial of Service**
  - Overload the targeted computer preventing it from doing any useful work
  - Distributed denial-of-service (DDOS) come from multiple sites at once

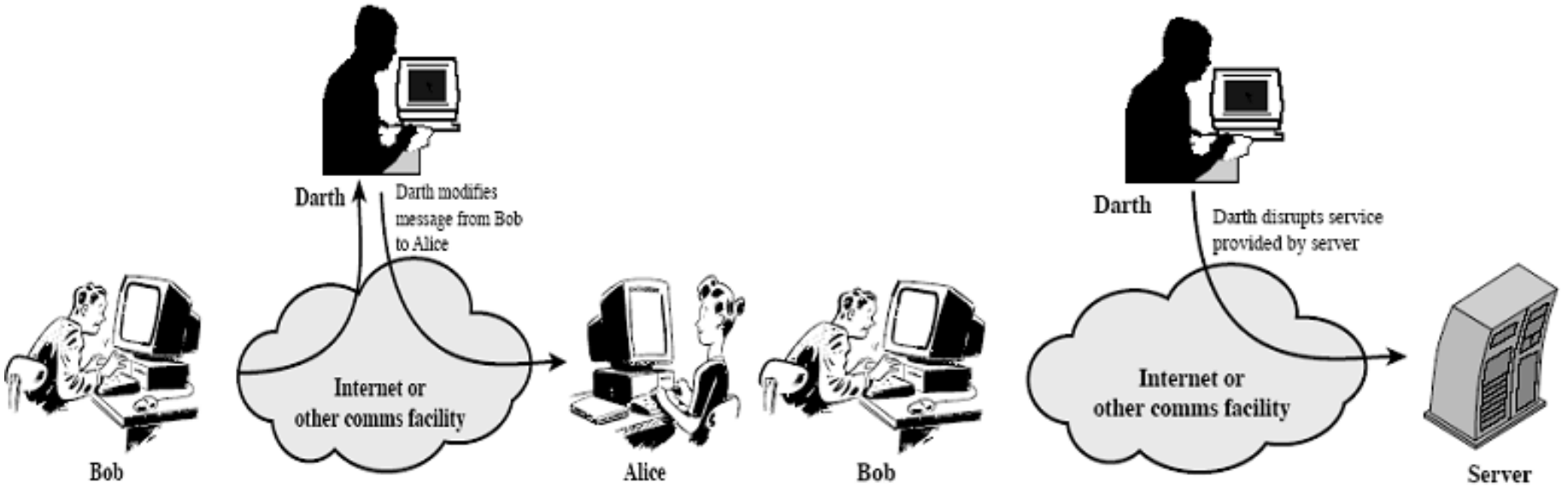
Interception





(a) Masquerade

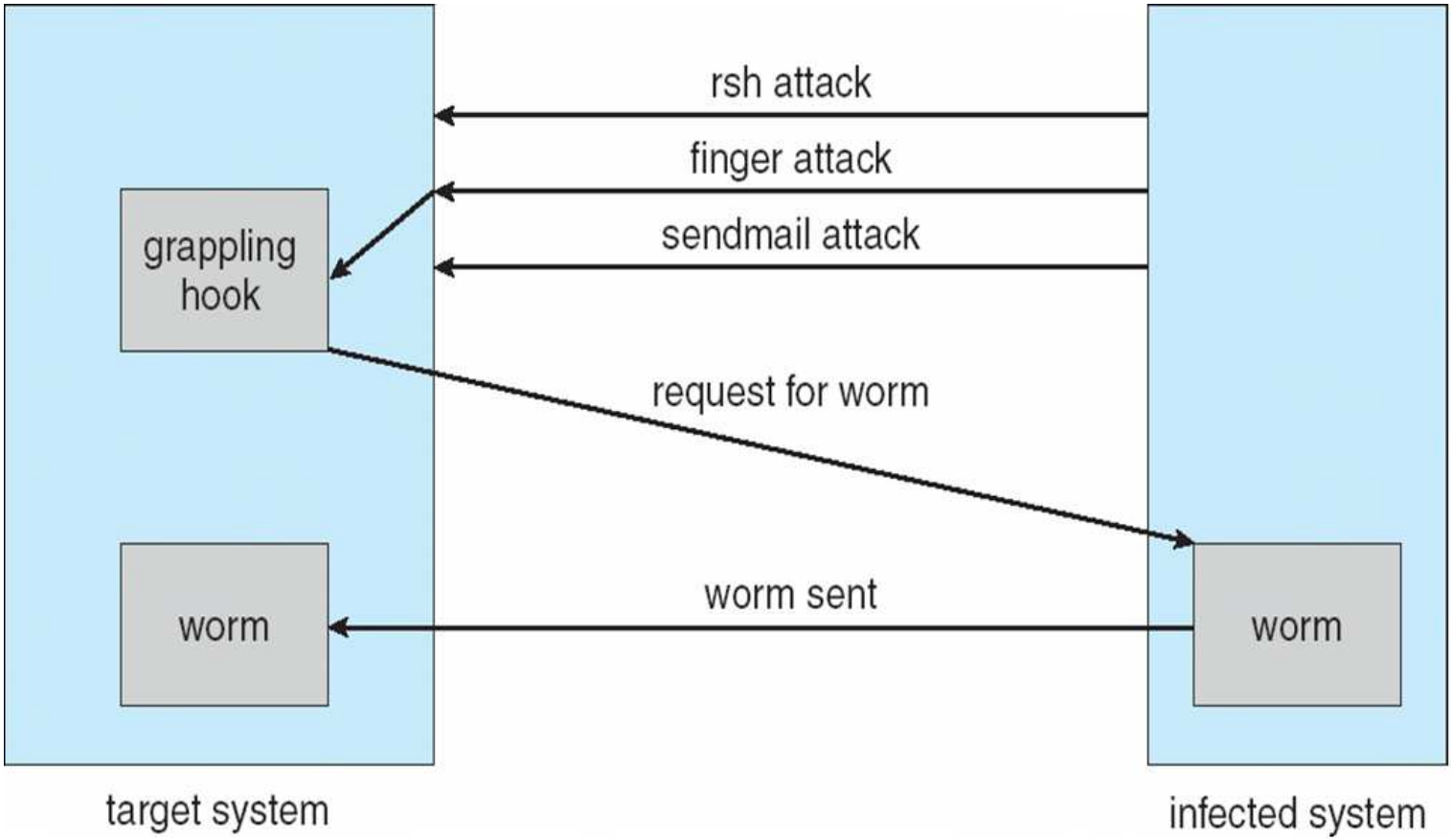
(b) Replay



(c) Modification of messages

(d) Denial of service

The Morris Internet Worm



Security Mechanism

- Encryption
  - Transform plaintext into ciphertext
  - Cryptography
- Authentication
  - Verify the identity of an entity
  - Digital signature
- Authorization
  - Verify the action performed by an entity
  - ACL (Access Control List)
- Auditing
  - Trace which entity access what
  - Logs file

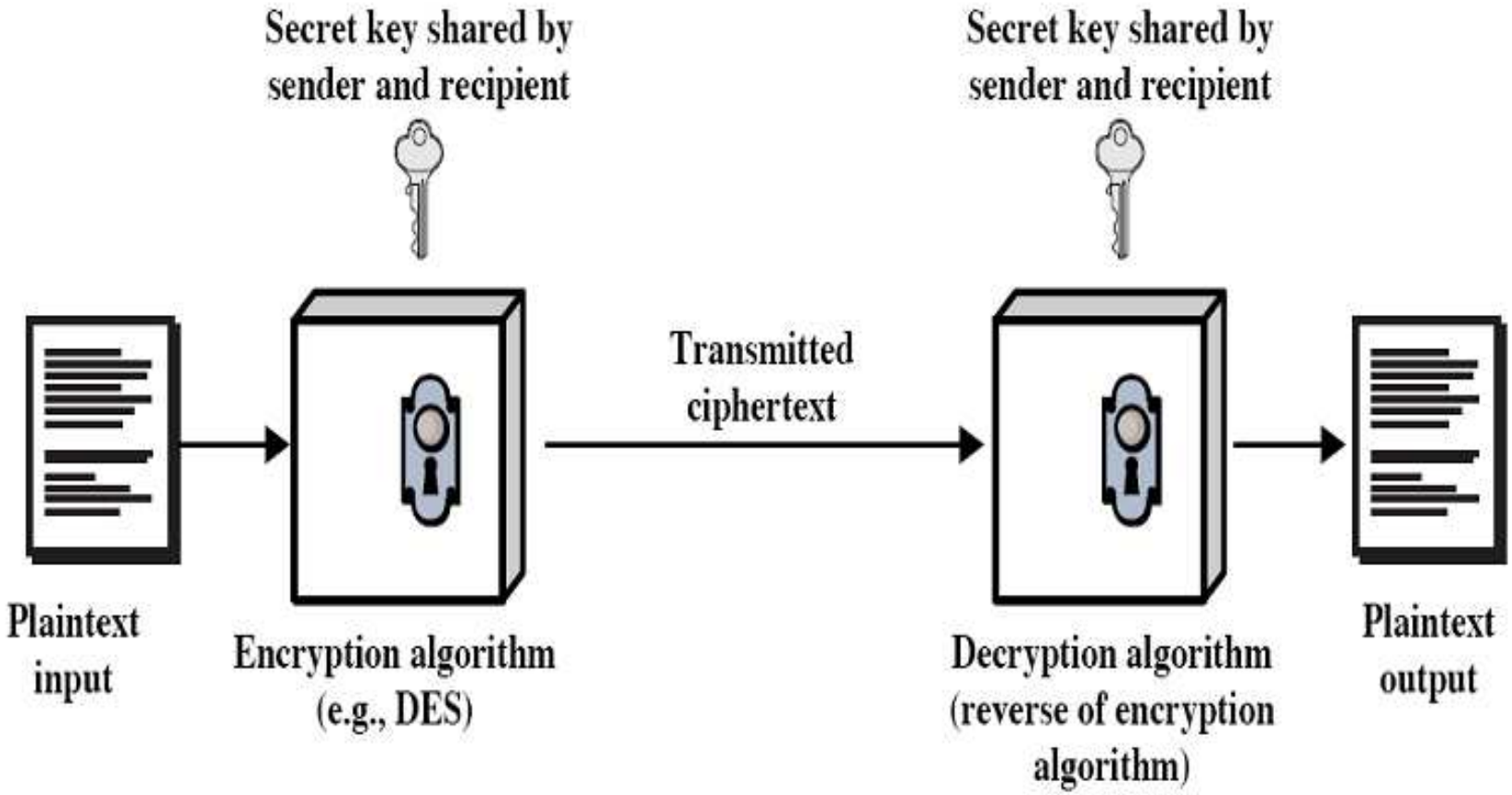
Cryptography

- Based on secrets
- Series of mathematics function
- Symetric key: AES (128 bit), RC4 (128 bit),...
  - Fast
  - Problem with key distribution (single key)
- Asymmetric key: RSA (1024 bit), RC (256 bit),...
  - Solve key distribution problem (public/private keys)
  - Slower
- Hybrid system
  - Pick key K (temporary)
  - Encrypt key K with public key system
  - Encrypt data with secret key system and K

Symmetric Encryption

- Same key used to encrypt and decrypt
  - $E(k)$ can be derived from $D(k)$, and vice versa
- DES is most commonly used symmetric block-encryption algorithm (created by US Govt)
  - Encrypts a block of data at a time
- Triple-DES considered more secure
- Advanced Encryption Standard (AES),
- RC4 is most common symmetric stream cipher, but known to have vulnerabilities
  - Encrypts/decrypts a stream of bytes (i.e wireless transmission)
  - Key is a input to psuedo-random-bit generator

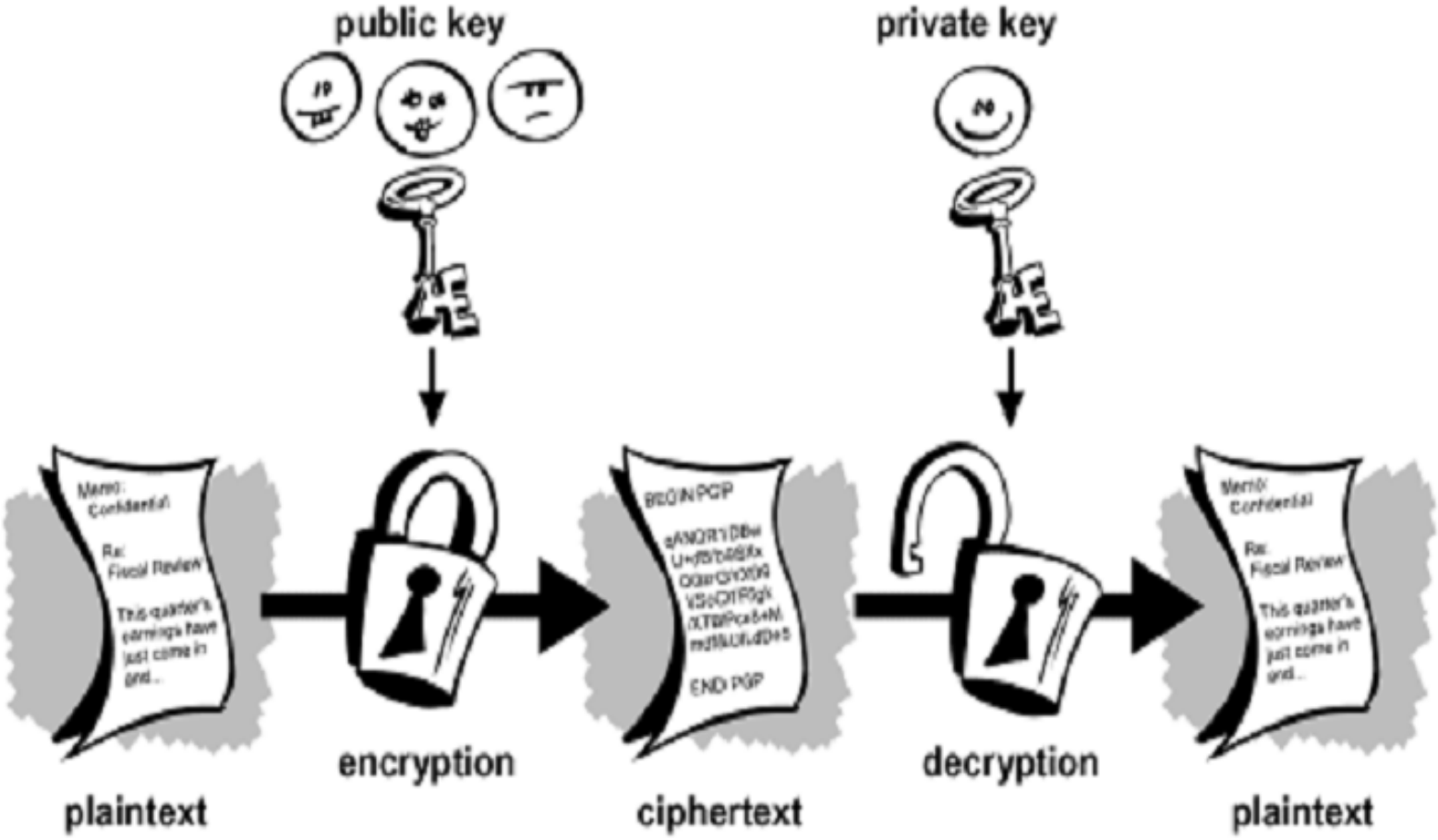
Symmetric Chiper



Asymmetric Encryption

- Public-key encryption based on each user having two keys:
  - public key – published key used to **encrypt data**
  - private key – key known only to individual user used to **decrypt data**
- Must be an encryption scheme that can be made public without making it easy to figure out the decryption scheme
  - Most common is RSA block cipher

Asymmetric chiper



Authentication

- Protecting the integrity of a message
- **Validating identity of originator**
- Non-repudiation of origin (dispute resolution)
- Three alternative functions used to create an authenticator:
  - Message encryption
  - Cryptographic checksum
  - Hash function

Hash Function

- Produce fixed-length hash value
- Value will change if one bit is changed
- Algorithm:
  - MD5 (32 digit – 128 bit)
  - SHA1 (40 digit - 160 bit)
  - SHA-256 (64 digit – 256 bit)
  - SHA-384 (96 digit – 384 bit)
  - SHA-512 (128 digit – 512 bit)

Digital Certificates

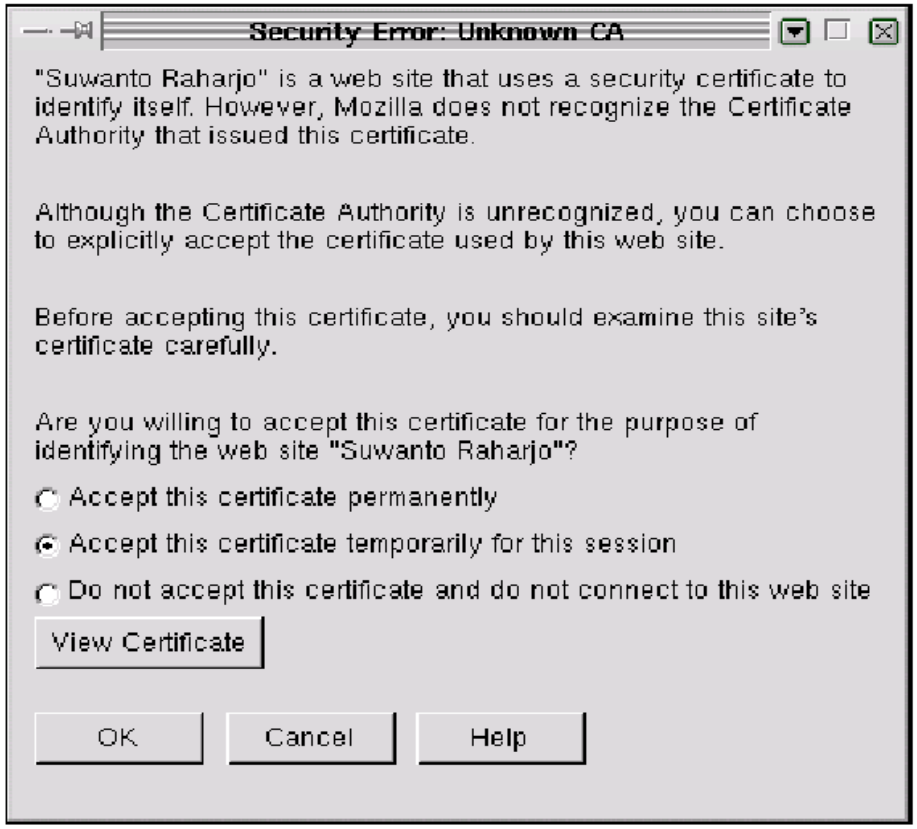
- Proof of who or what owns a public key
- Public key digitally signed a trusted party
- Trusted party receives proof of identification from entity and certifies that public key belongs to entity
- Certificate authority are trusted party – their public keys included with web browser distributions

Encryption Example - SSL

- SSL – Secure Socket Layer (also called TLS)
- Cryptographic protocol that limits two computers to only exchange messages with each other
  - Very complicated, with many variations
- Used between web servers and browsers for secure communication (eg. For: credit card numbers)
- The server is verified with a **digital certificate** assuring client is talking to correct server

SSL

- Netscape Corp (1996)
- Untuk Semua Protokol TCP
  - Telnet -> SSH
  - HTTP -> HTTPS
- Public Key Server
- Hashing
  - MD5 + SHA
- Certificate Authority



User Authentication

- Crucial to identify user correctly, as protection systems depend on **user ID**
- User identity most often established through *passwords*, can be considered a special case of either keys or capabilities
  - Also can include something user has and /or a user attribute
- Passwords must be kept secret
  - Frequent change of passwords
  - Use of “non-guessable” passwords
  - Log all invalid access attempts (3x)
- Passwords may also either be encrypted or allowed to be used only once

ACL

- List of permissions attached to an object/resources
  - Who has access to resource
  - What operation is allowed to be performed on the resources
- Example
  - Unix permission

Object	*Subjects*			
	S_1	S_2	S_3	S_4
`/etc/passwd`	read	read, write	–	read

Proteksi Data dalam jaringan

- Networks can be sniffed
- Lots of tools are available for FREE
- Not easily detectable
- Easy to encounter
- Use of secure communication protocol
  - SSH
  - SSL
  - HTTPS

Firewalling to Protect Systems and Networks

- A network firewall is placed between trusted and untrusted hosts
  - The firewall limits network access between these two security domains
- Can be tunneled or spoofed
  - Tunneling allows disallowed protocol to travel within allowed protocol (i.e. telnet inside of HTTP)
  - Firewall rules typically based on host name or IP address which can be spoofed
- Personal firewall is software layer on given host
  - Can monitor / limit traffic to and from the host
- Application proxy firewall understands application protocol and can control them
- System-call firewall monitors all important system calls and apply rules to them

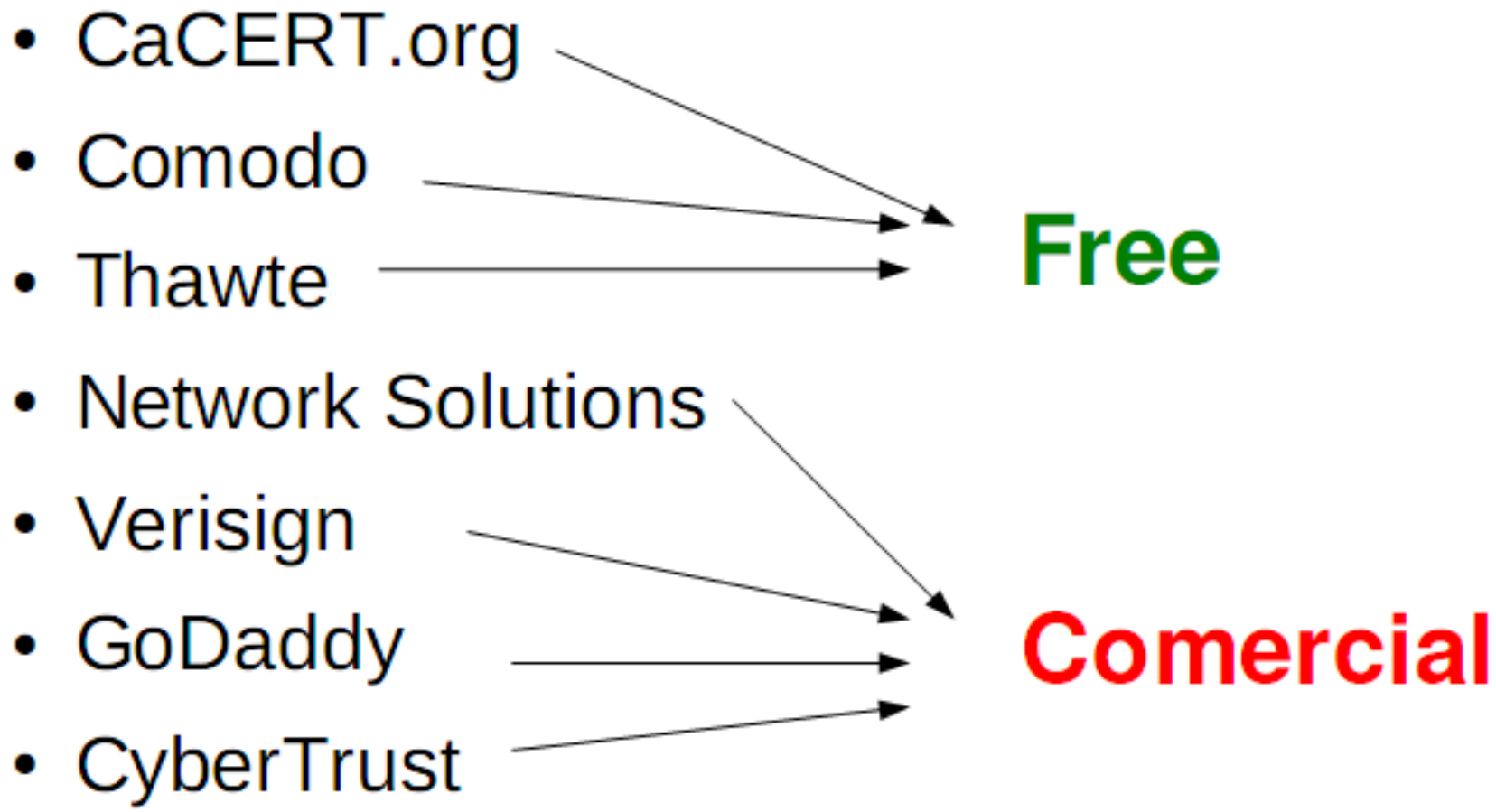
SSH

- Secure Shell
- Replaces telnet, rlogin, ftp, and rcp
- Encrypt messages before transmission
- Flexible configuration
- Example: OpenSSH

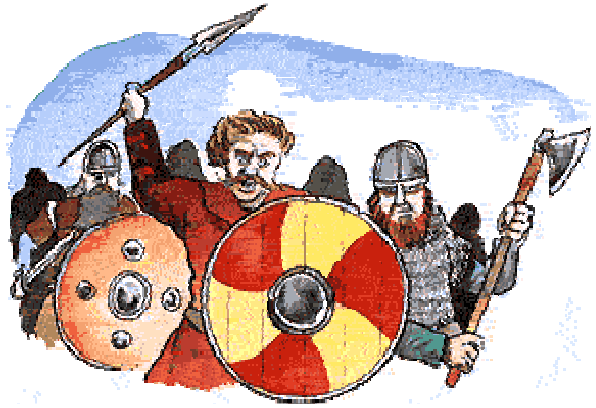
HTTPS

- Increase web security and client's trust
- Certificate signed by Certified Authority
- Protocol HTTPS
- Using SSL as the basis
- Running on port: 443 (default)

Penyedia Sertifikat



Web server attack



- Scan to find open ports
- Find out what's running on open ports (**banner grabbing**)
- Profile the server
  - Windows (look for Kerberos, NetBIOS)
  - Unix
  - Use TCP fingerprinting
- Probe for weaknesses on interesting ports
  - Default configuration files and settings (e.g. popular IIS ones)
  - Buffer overflows
  - Insecure applications
- Launch attack
  - Use exploit code from Internet…
  - …or build your own

Kelemahan security pada aplikasi web

http://www.owasp.org

Berikut adalah 10 kelemahan security teratas pada aplikasi web

- Masukan (input) yang tidak tervalidasi
- Broken Access Control
- Pengelolaan Autentikasi dan Session yang tidak baik
- Cross site scripting
- Buffer overflows
- Injections flaws
- Penyimpanan yang tidak aman
- Denial of Service
- Pengelolaan konfigurasi yang tidak aman
  - Register Global on PHP

Kelemahan security pada aplikasi web

Input yang tidak divalidasi

- Aplikasi web menerima data dari HTTP request yang dimasukkan oleh user
- Hacker dapat memanipulasi request untuk menyerang keamanan situs

Hal – hal yang harus diperhatikan ketika mengelola validasi:

- Tidak cukup hanya bergantung pada script client side yang biasa digunakan untuk mencegah masukan form ketika ada input yang invalid
- Penggunaan kode validasi untuk memeriksa masukan tidak mencukupi

Kelemahan security pada aplikasi web

Broken Access Control

- Pada aplikasi yang membedakan akses dengan menggunakan perbedaan ID, hanya menggunakan satu halaman untuk memeriksa user.
- Jika user berhasil melewati halaman login, maka dia bebas melakukan apa saja
- Permasalahan lain adalah:
  - ID yang tidak aman
    ID bisa ditebak
  - Ijin file
    File yang berisi daftar user bisa dibaca orang lain

Kelemahan security pada aplikasi web

Pengelolaan Autentikasi dan Session yang tidak baik

- Beberapa hal yang harus diperhatikan:
  - Password strength
  - Penyimpanan password
  - Session ID Protection

Kelemahan security pada aplikasi web

Buffer Overflows

- Pengiriman request yang dapat membuat server menjalankan kode kode yang tidak biasa (salah / tidak seharusnya)

Error Handling

- Examples: stack traces, DB dumps
- Helps attacker know how to target the app
- Inconsistencies can be revealing too
  - “File not found” vs. “Access denied”
- Fail-open errors
- Countermeasures
  - Code review
  - Modify default error pages (404, 401, etc.)

Error messages example

daily news

Warning: Too many connections
in **/web/include/classes/DBConnect_GFN.inc** on line **14**

Warning: mysql_query(): supplied argument is not a valid MySQL-Link resource in **/web/include/classes/DBConnect_GFN.inc** on line **35**
Too many connections
Warning: mysql_query(): supplied argument is not a valid MySQL-Link resource in **/web/include/classes/DBConnect_GFN.inc** on line **35**
Too many connections
Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in **/web/include/classes/StoryFetch.inc** on line **23**
Fatal error in class StoryFetch [1]

Kelemahan security pada aplikasi web

Injection Flaws

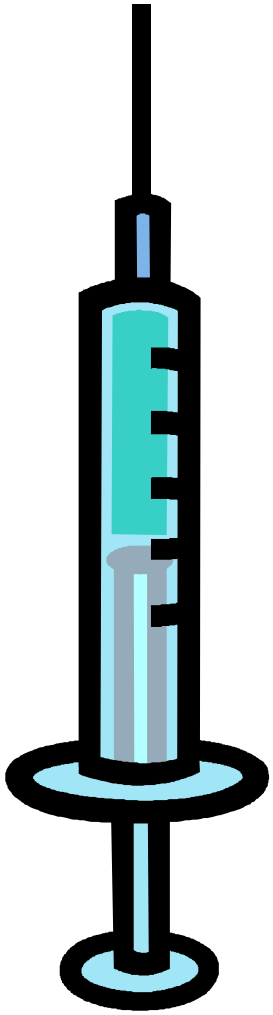
- Penyerang mengirimkan “inject” calls ke OS atau resource lain, seperti database
- Salah satu yang terkenal adalah SQL Injection

SQL Injection

- Cross platform, Cross language, Cross products
- Because of “Lack of input filter”
- Adds malicious SQL, Alter data, and Gain access

Command Injection

- Allows attacker to relay malicious code in form variables or URL
  - System commands
  - SQL
  - Interpreted code (Perl, Python, etc.)
- Many apps use calls to external programs
  - sendmail
- Examples
  - Path traversal: “../”
  - Add more commands: “; rm –r *”
  - SQL injection: “’ OR 1=1”
- Countermeasures
  - Verify all input
  - Avoid system calls (use libraries instead)
  - Run with limited privileges



SQL Injection

SQL Code:

```
$query = “SELECT *
FROM user
WHERE username='" . $user . "' AND
password=password('" . $passwd . "')";
```

Input (no password required):

```
coba' OR 1='1
```

Assumption: username is known

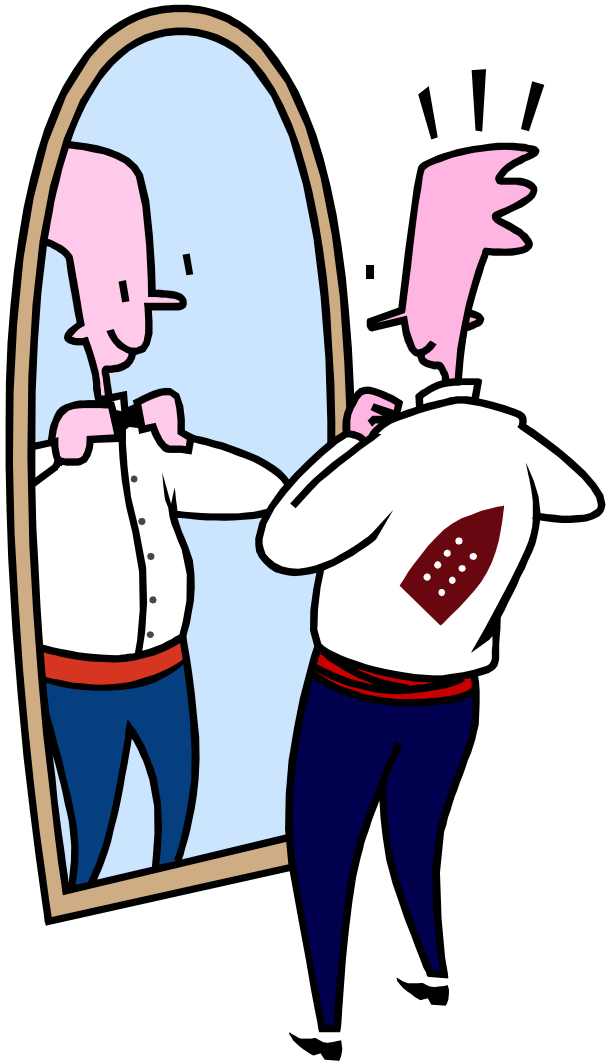
Output:

```
$query = “SELECT *
FROM user
WHERE username='coba' OR 1='1' AND
password=password('')
```

AND part will be executed first

Web/App Server Misconfiguration

- Tension between “work out of the box” and “use only what you need”
- Developers ≠ web masters
- Examples
  - Unpatched security flaws
  - Misconfigurations that allow directory traversal
  - Default accounts/passwords
- Countermeasures
  - Turn off all unused services
  - Set up and audit roles, permissions, and accounts
  - Set up logging and alerts



General Recommendations

- Hati-hati ketika merubah konfigurasi browser
- Jangan membuat konfigurasi yang mendukung scripts dan macros
- Jangan langsung menjalankan program yang anda download dari internet
- Browsing ke situs-situs yang aman
  - Mengurangi kemungkinan adanya malcode dan spyware
- Konfigurasi homepage harus hati-hati
  - Lebih baik gunakan blank.
- Jangan mempercayai setiap links (periksa dulu arah tujuan link itu)
- Jangan selalu mengikuti link yang diberitahukan lewat e-mail
- Jangan browsing dari sistem yang mengandung data sensitif
- Lindungi informasi anda kalau bisa jangan gunakan informasi pribadi pada web
- Gunakan stronger encryption
  - Pilih 128-bit encryption atau 256
- Gunakan browser yang jarang digunakan
  - Serangan banyak dilakukan pada web browser yang populer
- Minimalkan penggunaan plugins
- Minimalkan penggunaan cookies
- Perhatikan cara penanganan dan lokasi penyimpanan *temporary files*

NEXT

- Naming Service