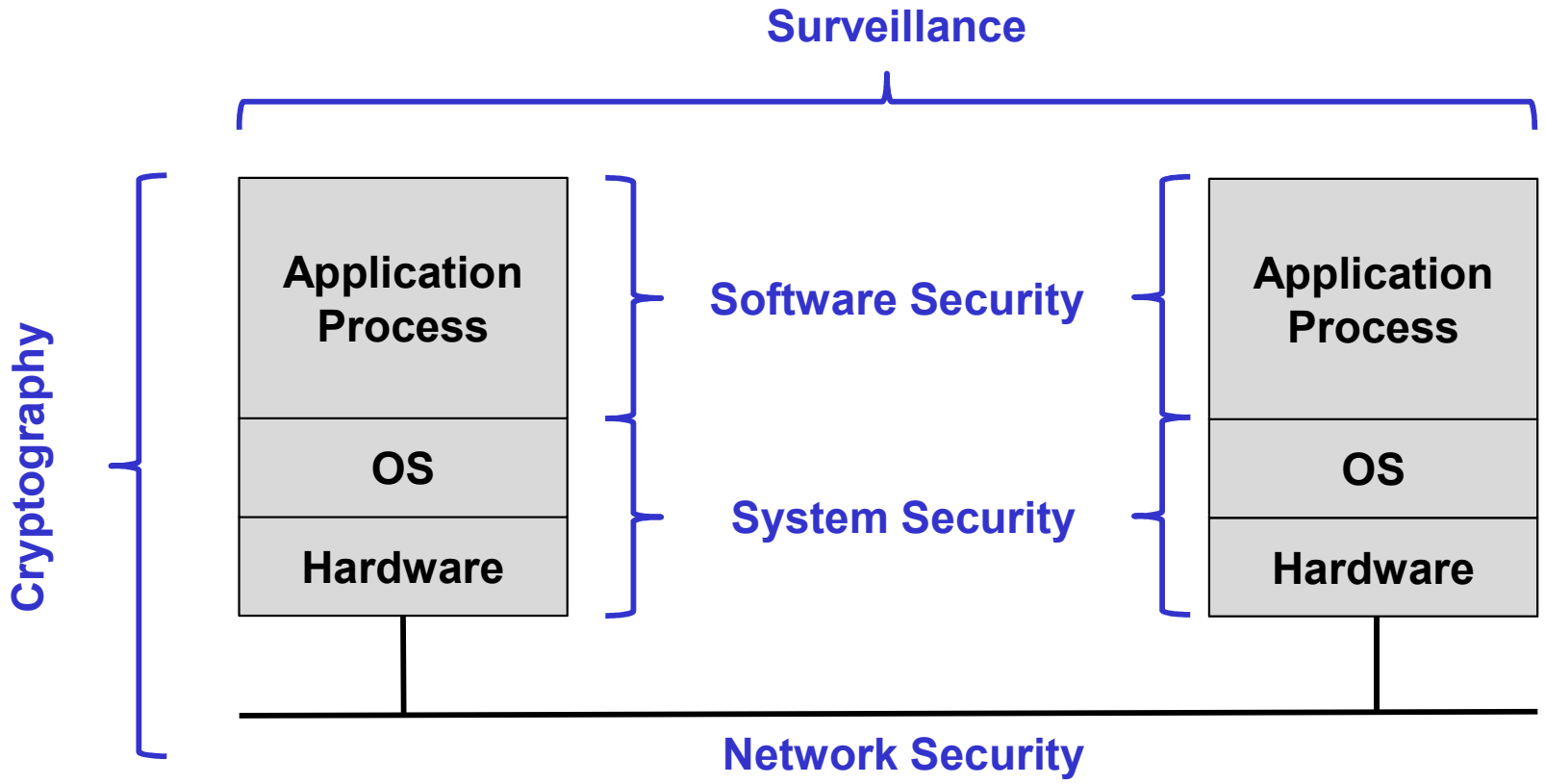
Chap. 16) Security

경희대학교 컴퓨터공학과

조 진 성

Computer Security



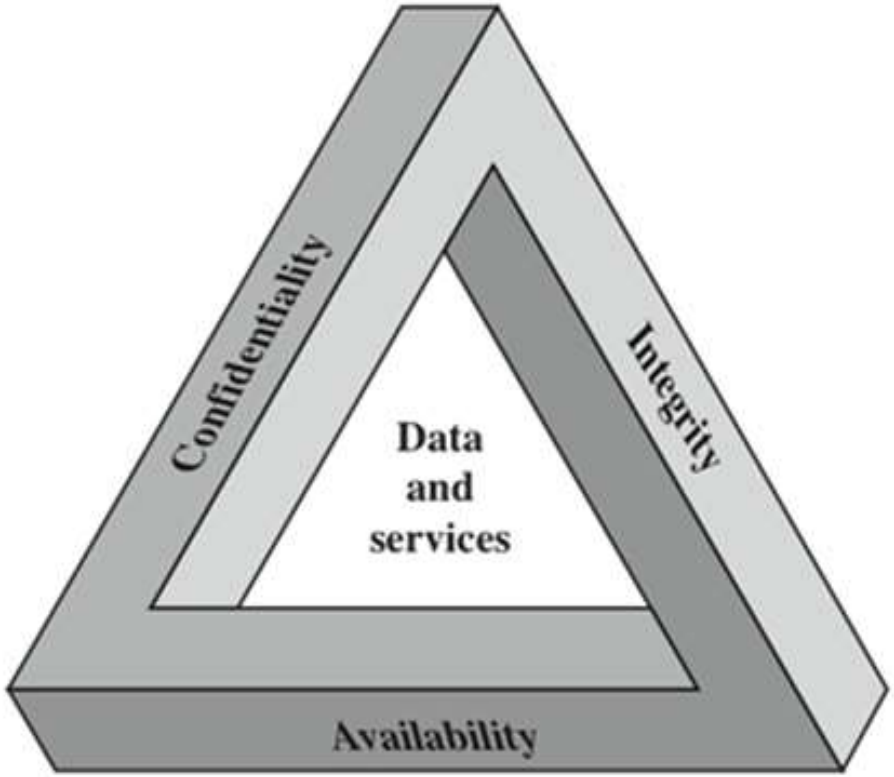
Computer Security Overview

NIST computer security handbook defines **Computer Security** as

- ✓ The protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability and confidentiality of information system resources" (includes hardware, software, firmware, information/data, and telecommunications)

Security requirement triad (CIA Triad)

- ✓ Confidentiality
  - data confidentiality
  - privacy
- ✓ Integrity
  - data integrity
  - system integrity
- ✓ Availability



Security Problem

There is no perfectly secure system!

- ✓ Protection can only increase the effort needed to do something bad. It cannot prevent it
- ✓ Every system has holes, it just depends on what they look like
- ✓ Even assuming a technically perfect system, there are always the four Bs:
  - Burglary: steal it
  - Bribery: find whoever has access to what you want and bribe them
  - Blackmail: or photograph them in a compromising position
  - Bludgeoning: or just beat them until they tell you

Terminology

- ✓ **Vulnerability**: loss of CIA (Confidentiality, Integrity, Availability)
- ✓ **Threat**: capable of exploiting vulnerabilities
- ✓ **Attack**: threats carried out
- ✓ **Adversary**: an entity that attacks a system
- ✓ **Countermeasure**: means to deal with attacks

Security Services

- Confidentiality
- Integrity
- Availability
- Authentication
- Access control
- Nonrepudiation

AUTHENTICATION

The assurance that the communicating entity is the one that it claims to be.

Peer Entity Authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

Data-Origin Authentication
In a connectionless transfer, provides assurance that the source of received data is as claimed.

ACCESS CONTROL

The prevention of unauthorized use of a resource (i.e., 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 do).

DATA CONFIDENTIALITY

The protection of data from unauthorized disclosure.

Connection Confidentiality
The protection of all user data on a connection.

Connectionless Confidentiality
The protection of all user data in a single data block.

Selective-Field Confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

Traffic-Flow Confidentiality
The protection of the information that might be derived from observation of traffic flows.

AVAILABILITY

Ensures that there is no denial of authorized access to network elements, stored information, information flows, services and applications due to events impacting the network. Disaster recovery solutions are included in this category.

DATA INTEGRITY

The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay).

Connection Integrity with Recovery
Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted.

Connection Integrity without Recovery
As above, but provides only detection without recovery.

Selective-Field Connection Integrity
Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed.

Connectionless Integrity
Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided.

Selective-Field Connectionless Integrity
Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified.

NONREPUDIATION

Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication.

Nonrepudiation, Origin
Proof that the message was sent by the specified party.

Nonrepudiation, Destination
Proof that the message was received by the specified party.

Cracker's Basic Steps

Gather information

- ✓ as much information about your site as possible

Use port scanner

- ✓ to gather information about what services are running on hosts
- ✓ Search for weak security services

Get a login account

- ✓ Doesn't matter whose account

Get root privilege

- ✓ Bugs in programs or badly configured systems

Keep root privilege

- ✓ Leave some sort of backdoor for future access

Physical Security

Hardware security

- ✓ Restrict access to equipments
  - Smart card (ID card)
  - Bio-metric access control

BIOS security

- ✓ Set a boot password
- ✓ Prevent booting from CD-ROM or floppy drives

Session security

- ✓ Some shells (e.g. tcsh) provide the automatic logout facility if there is no activity during the specified time period
- ✓ vlock (for locking a virtual terminal) / xlock
- ✓ Screen savers

Account Security

Authentication

- ✓ Make sure we know who we are talking to
- ✓ Usually done with passwords
  - First line of defense and single biggest security hole
- ✓ Problems in passwords:
  - Users who write their password on paper for all to see
  - Type password slowly that others can see
  - Dumb passwords like “password”
  - Passwords should be long and obscure – unfortunately easily forgotten and usually written down
- ✓ Passwords should not be stored in a directly-readable form
  - Use some sort of one-way-transformation (a “secure hash”) and store that

- ✓ *Cf) CHAP (Challenge Handshake Authentication Protocol)*

Account Security

Authentication alternatives

- ✓ Some alternatives
  - Physical keys: badges, smart cards, …
  - Biometric keys: Fingerprints, iris prints, facial profiles, voice prints, hand geometry, signature analysis …
  - Passwords using images
- ✓ Should not be forgeable or copiable
- ✓ Can be stolen, but the owner should know if it is
  - Need to invalidate old one

Account Security

Authorization

- ✓ Determine if x is allowed to do y
  - Can be represented as an “access matrix”
- ✓ Access control lists (ACLs)
  - With each object, indicate which users are allowed to perform which operations
  - Simple and used in almost all file systems
- ✓ Capabilities
  - With each users, indicate which resources may be accessed and in what ways
  - Frequently do both naming and protection: Can only “see” an object if you have a capability for it
  - Used in systems that need to be very secure

File System Security

Setuid/setgid programs

- ✓ Badly written setuid programs may contain a security hole
  - Know of all setuid and setgid programs on your system
  - Setuid programs that are not needed should be deleted
  - Never allow setuid/setgid files in user's home directories
  - Use nosuid option in fstab file for home file system and for NFS-mounted file system
  - Maintain a check on any new setuid programs:
    find / -type f –perm 2000 –o perm 4000 –o perm 6000
  - Never write setuid/setgid shell programs

File System Security

Search paths

- ✓ Many users include the current directory in their search path
- ✓ A cracker could place programs with the same name as standard commands everywhere they have write access in directory hierarchy
  - The fake program may have malicious code, or capture data from the user pretending to be the real application
- ✓ Place current directory last in the path
  - Alternatively use full path names (e.g. /bin/su)
- ✓ Current directory SHOULD NOT be in the search path for root user

File System Security

Other countermeasures

- ✓ Carefully specify default permissions: umask
- ✓ Put a limitation on the file system usage: quota
- ✓ Check file system integrity regularly: find, tripwire, …
  - Files without known owners may indicate unauthorized access: find / -nouser –o –nogroup
  - Files with “other” write permission (o+w) may indicate a problem: find / -type f –perm 2
- ✓ Use encrypted file system
  - CFS (Cryptographic File System)
  - TCFS (Transparent CFS), etc.
- ✓ Backup file system: tar, dd, …
- ✓ Monitor system logs

Network Security

Use secure protocols

- ✓ Don’t let the plain password float around the network
- ✓ Secure shell (ssh) suite of programs encrypts the communications of many of protocols
  - ssh (telnet), slogin (rlogin), sftp (ftp)
- ✓ Use secure http (https) for secure connection
- ✓ Secure Socket Layer (SSL) provides data encryption of all data that passes between clients and server
- ✓ IPsec protocol: encrypt every IP packet
  - Required for IPv6, optional for IPv4

Network Security

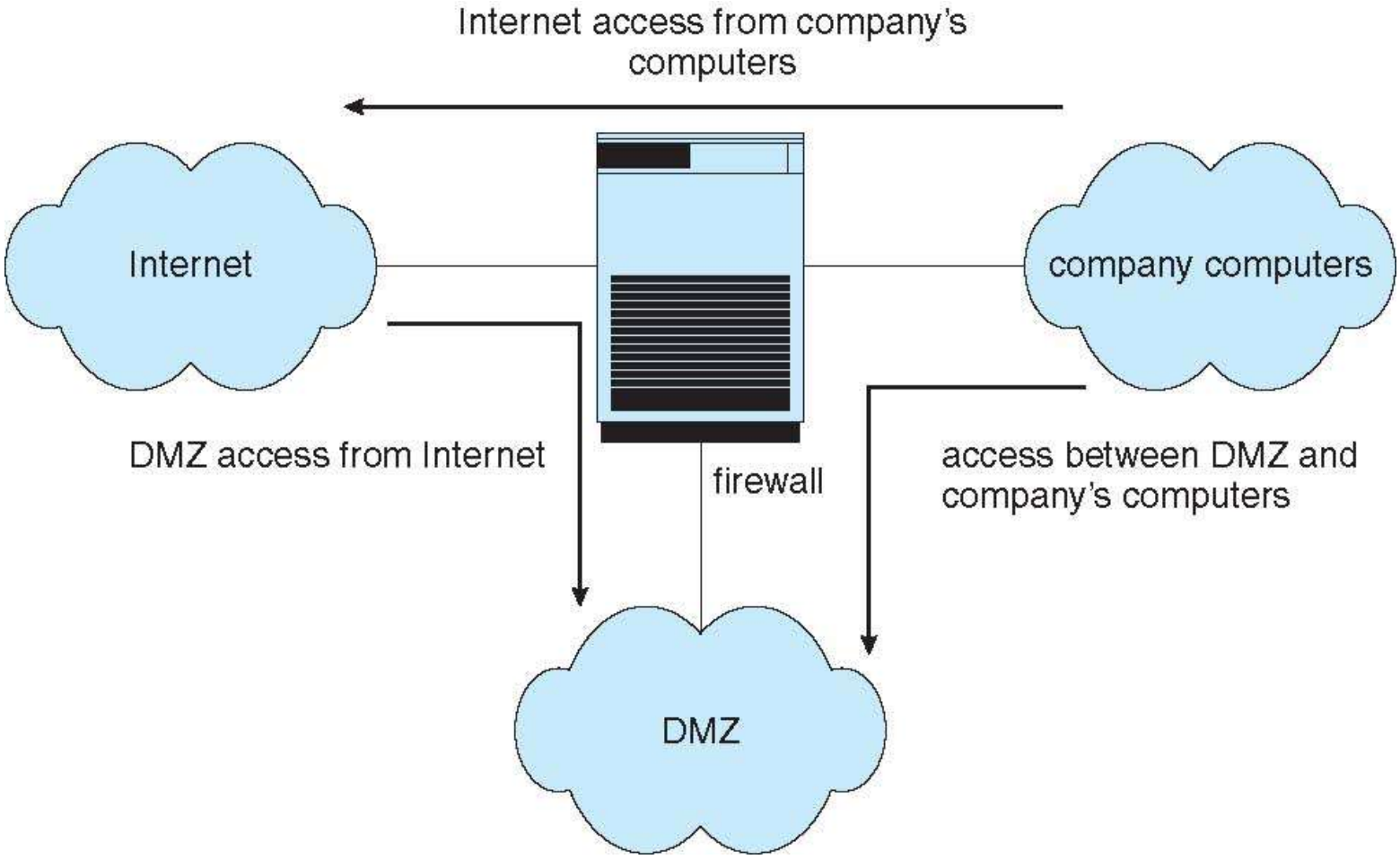
TCP wrappers

- ✓ Monitors/filters Internet services such as telnet, ftp, finger, etc.
- ✓ Similar to Internet super daemon, inetd
- ✓ Before connecting the client to the service program, log the activity and check if it should be permitted
  - /etc/hosts.allow, /etc/hosts.deny
- ✓ You should be able to detect cracking intention or activity from the log

Network Security

A **firewall** is placed between trusted and untrusted hosts

- ✓ Creates a filter or protective layer between an organization's internal networks and any external networks to which they are connected



Network Security

Intrusion Detection / Prevention

- ✓ Detect / Prevent attempts to intrude into computer systems

Firewall vs. IDS vs. IPS

Intrusion Detection System (IDS)

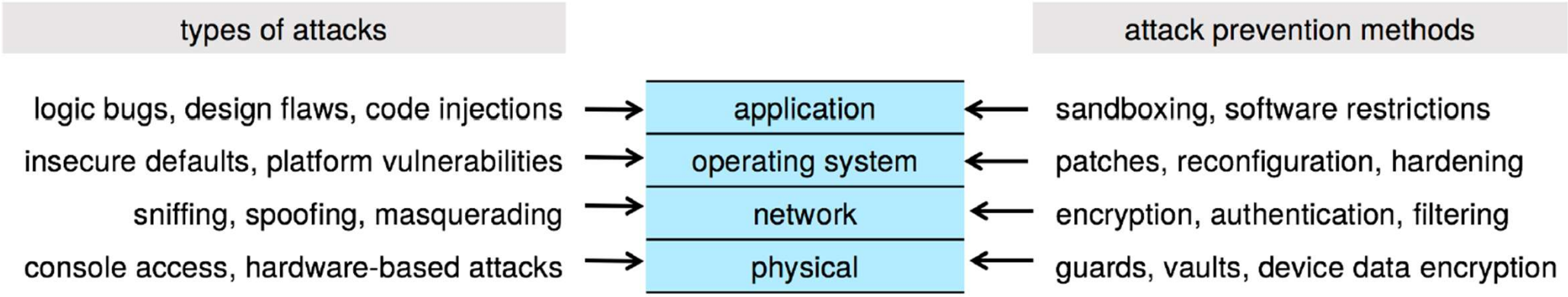
- ✓ Host-based IDS (H-IDS)
- ✓ Network-based IDS (N-IDS)

Intrusion Prevention System (IPS)

- ✓ E.g.) Wireless IPS (WIPS)

Attacks vs. Countermeasures

Four-layered model of security



Security Threats

Physical threats

- ✓ Acts of nature: floods, fire, earthquake, explosion, etc.
- ✓ Intruder takes computers, dig up network cable, or access system consoles

Logical threats

- ✓ Caused by problems with computer software
  - Misuse by people (e.g. easy-to-guess passwords)
  - Bugs in programs or in their interaction with each other

Operational threats

- ✓ No security policy, incomplete enforcement

Denial of service

- ✓ Prevent computer from providing services through
  - wasting resources of computer
  - flooding services on your system, thus preventing them from providing service to legitimate clients

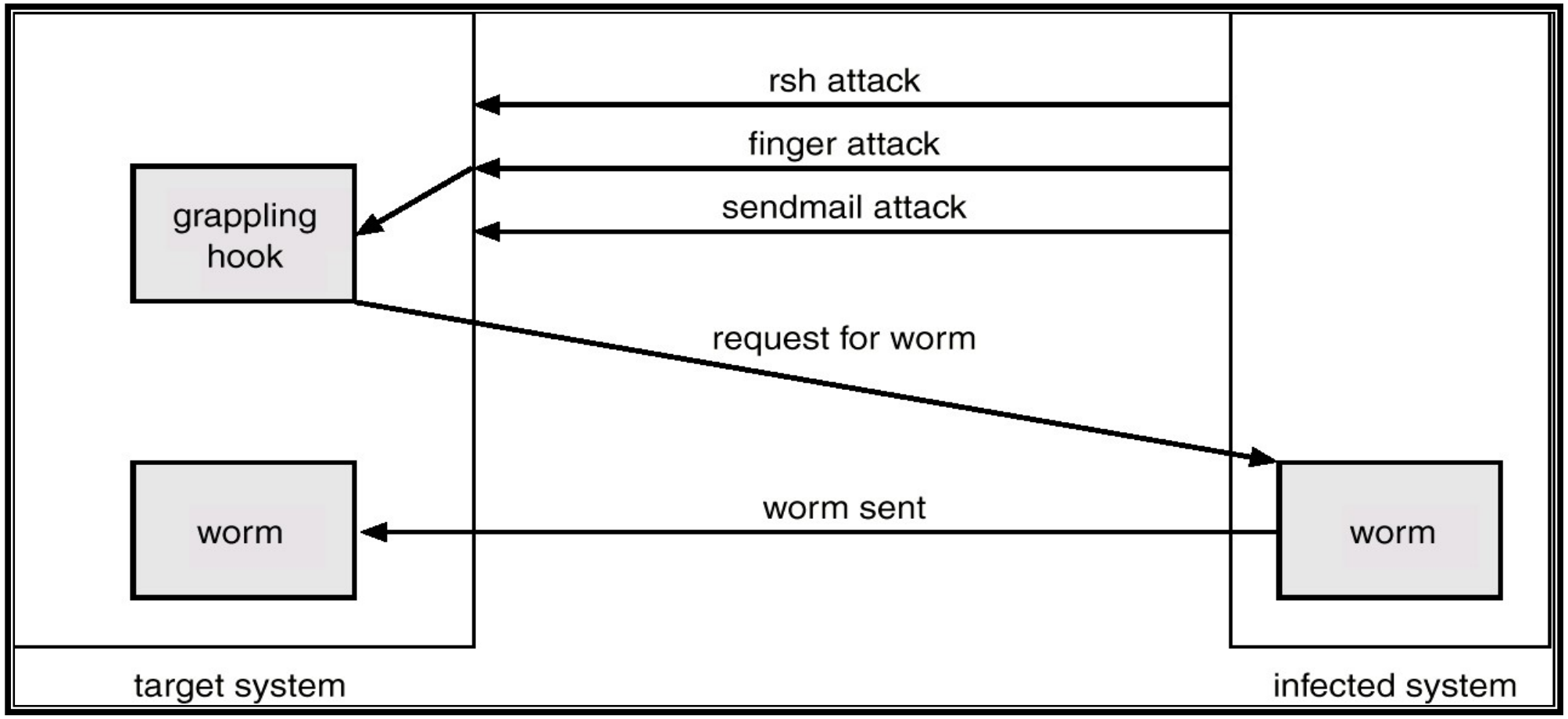
Attacks

Virus / Worm
Trojan horses
Logic bomb
Trap door
Dictionary attacks
Login spoofing

Malware / Spyware / Ransomware
Keystroke logger
Code injection
Packet sniffing / Replay attack / Man-In-The-Middle (MITM) / IP spoofing

DoS / DDoS

The Morris Internet Worm



Attacks

Buffer overflow

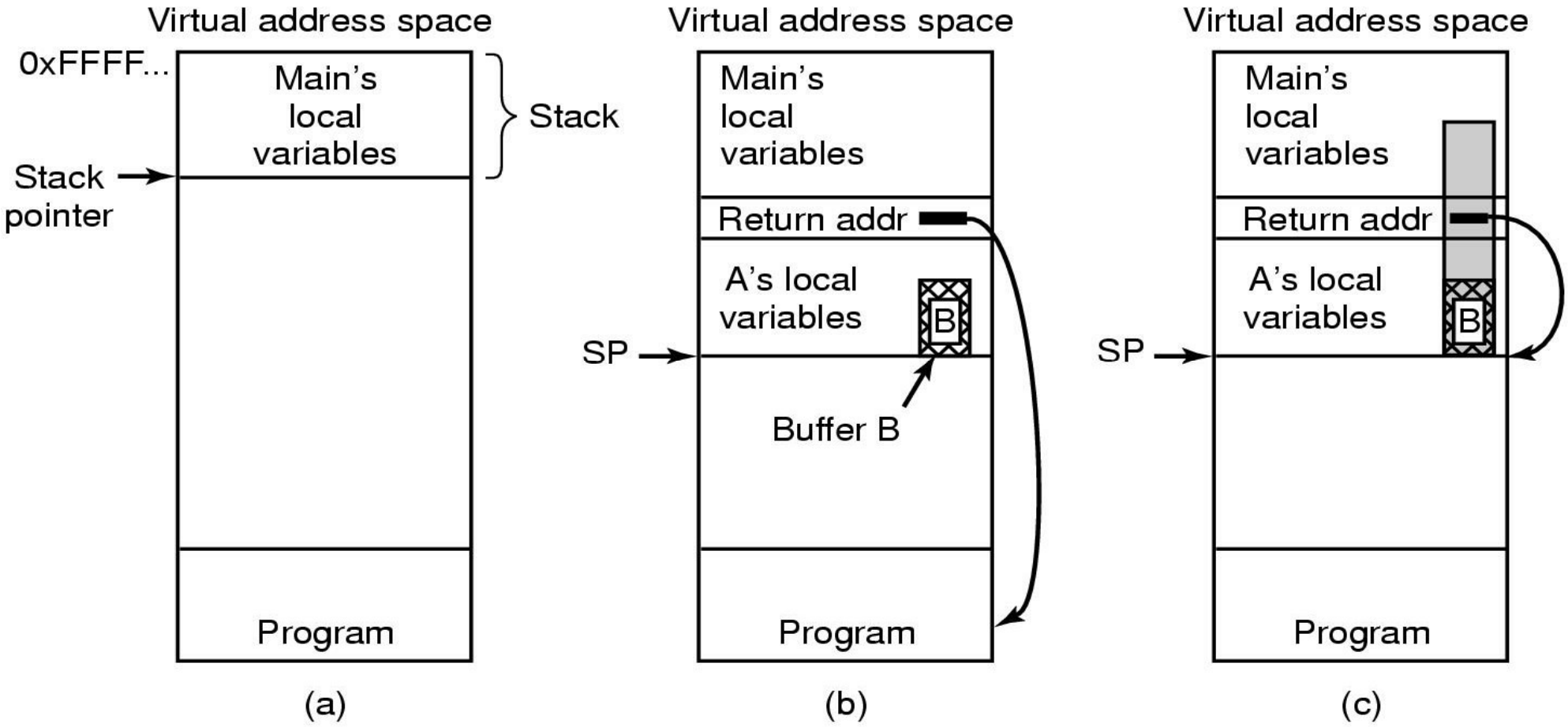
- ✓ What's the problem of the following codes?

```
void A(char *src)
{
    char B[1024];
    strcpy(B, src);
    puts(B); printf("\n");
}
int main(int argc, char *argv[])
{
    if (argc > 1)  {
        A(argv[1]);
    }
    return 0;
}
```

Attacks

Code injection

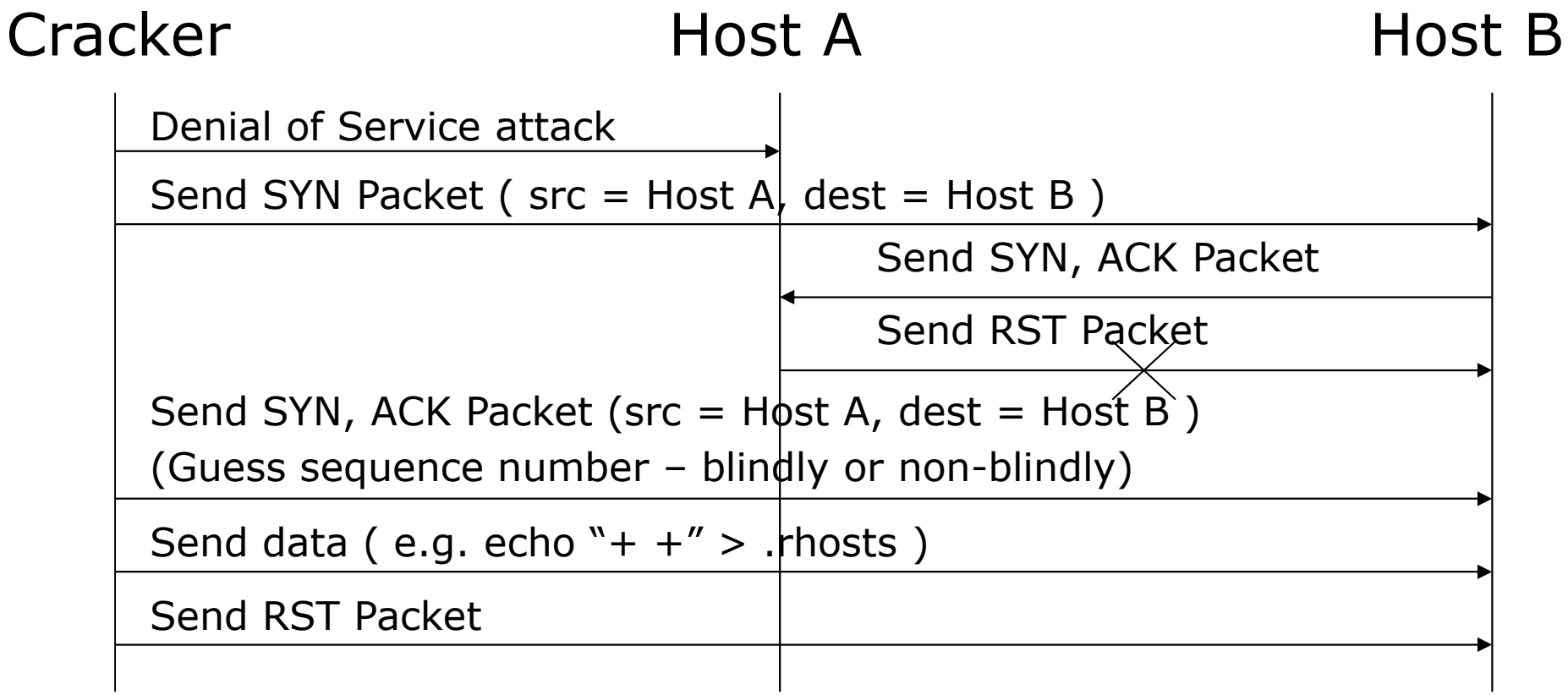
✓ Do array bounds checking! → Secure Coding!



Attacks

IP spoofing

- ✓ Steal an authorized IP and use it



Attacks

Denial of service: internal attacks

- ✓ Use up all resources and make system crash
- ✓ Attacking resources: disk, memory, process, …
- ✓ Examples
  - Shell script: while (1) { mkdir foo; cd foo; }
  - C: while (1) { fork(); ((int *) malloc(100000))[40] = 1; }
- ✓ Done by a local user, and in most cases by accident

Attacks

Denial of service: external attacks

- ✓ Application level
  - Mail bombing
  - Buffer overflow
  - Java Applet attack
- ✓ Protocol level
  - TCP SYN flooding
  - UDP Storming
- ✓ Network level
  - Ping flooding

Distributed DOS (DDOS)

- ✓ Use multiple machines

Basic Concept of Cryptography

What is cryptography

- ✓ The science of obfuscating data
- ✓ Can provide authentication, confidentiality, data integrity and etc.
- ✓ Cryptography algorithm is open, but key MUST be confidential

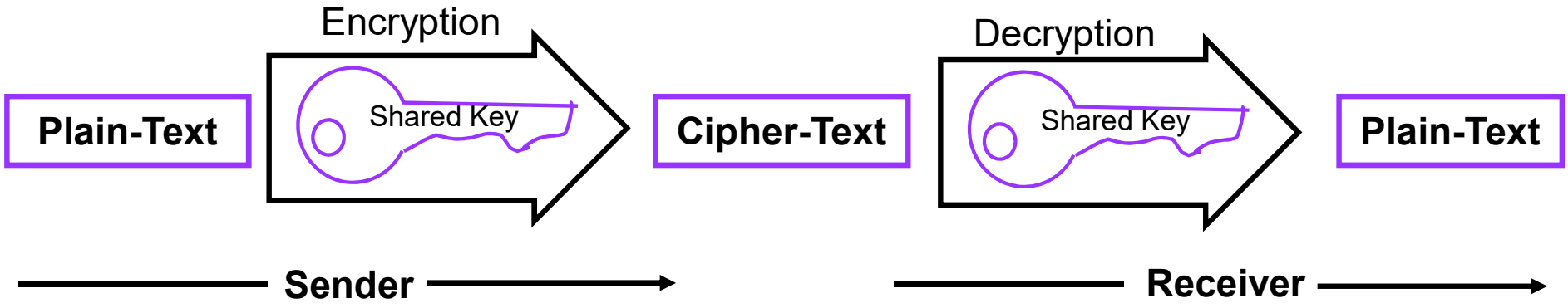
Two kinds of cryptography

- ✓ Shared key cryptography (symmetric cryptography)
- ✓ Public key cryptography (asymmetric cryptography)

Basic Concept of Cryptography

Shared key cryptography

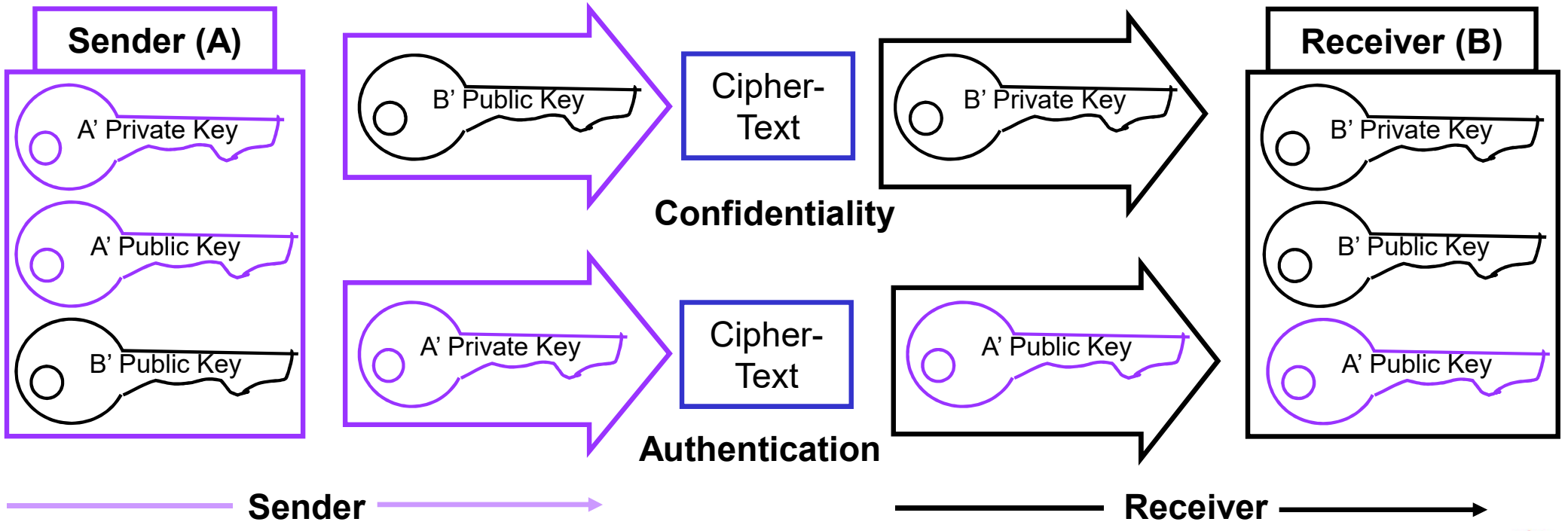
- ✓ Both of peers share the same key
- ✓ DES(Data Encryption Standard) / AES(Advanced Encryption Standard)
  - Bit operation
  - Can provide authentication and confidentiality
  - ***How can distribute the shared key secret and keep it secret*** ?



Basic Concept of Cryptography

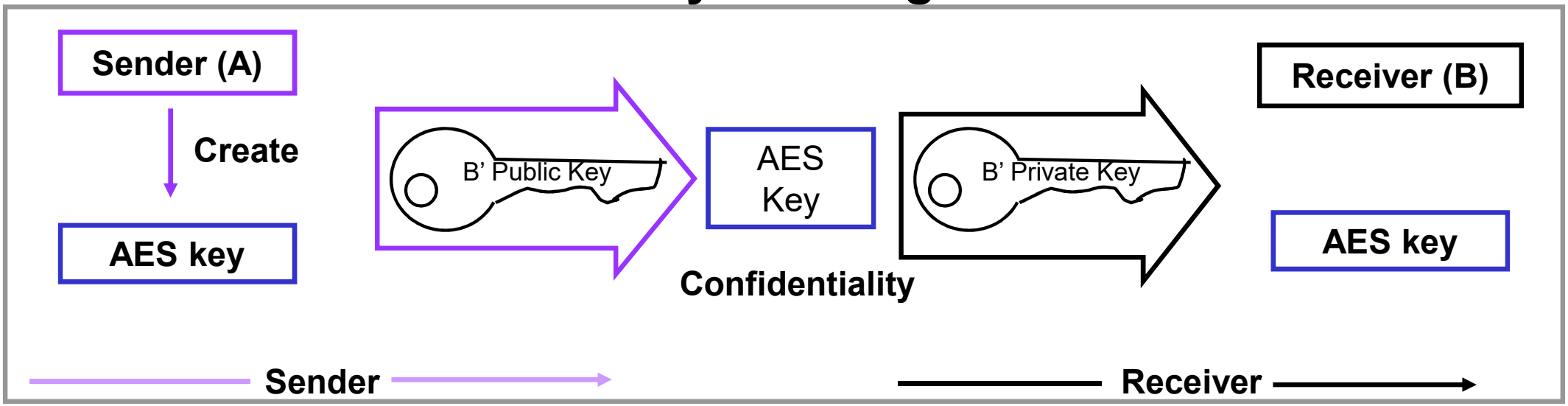
Public key cryptography

- ✓ Both of peers have its own private key and public keys
- ✓ Key pair
  - well known 'Public Key' and secret 'Private Key'
- ✓ Can provide confidentiality and authentication
- ✓ RSA : well known algorithm (Cf. ECC)

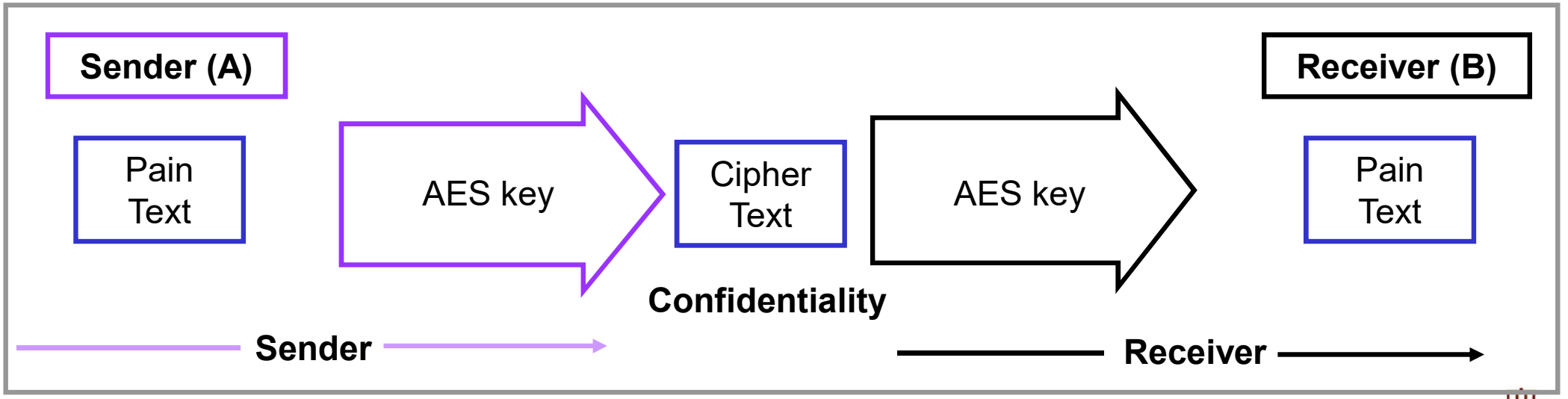


Applied Cryptography for Network (TLS/SSL)

Key exchange



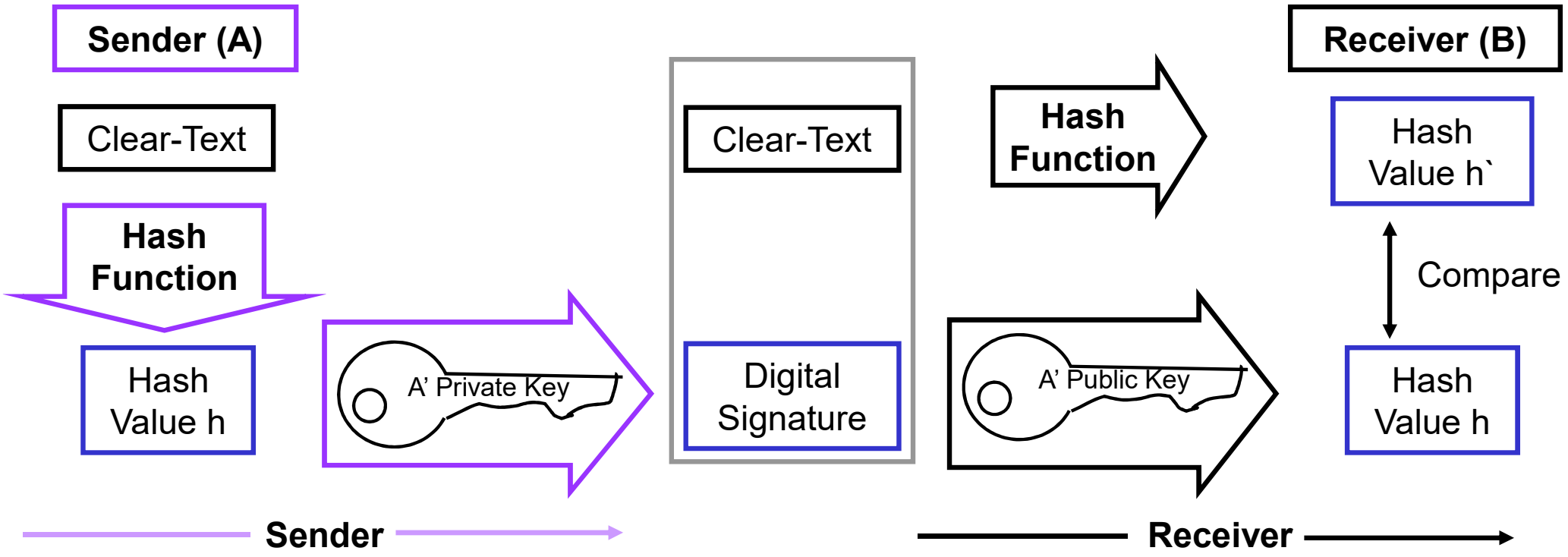
Data transfer



Applied Cryptography for Network

Digital Signature

- ✓ minimize encryption processing
- ✓ for authentication & integrity (not confidentiality)



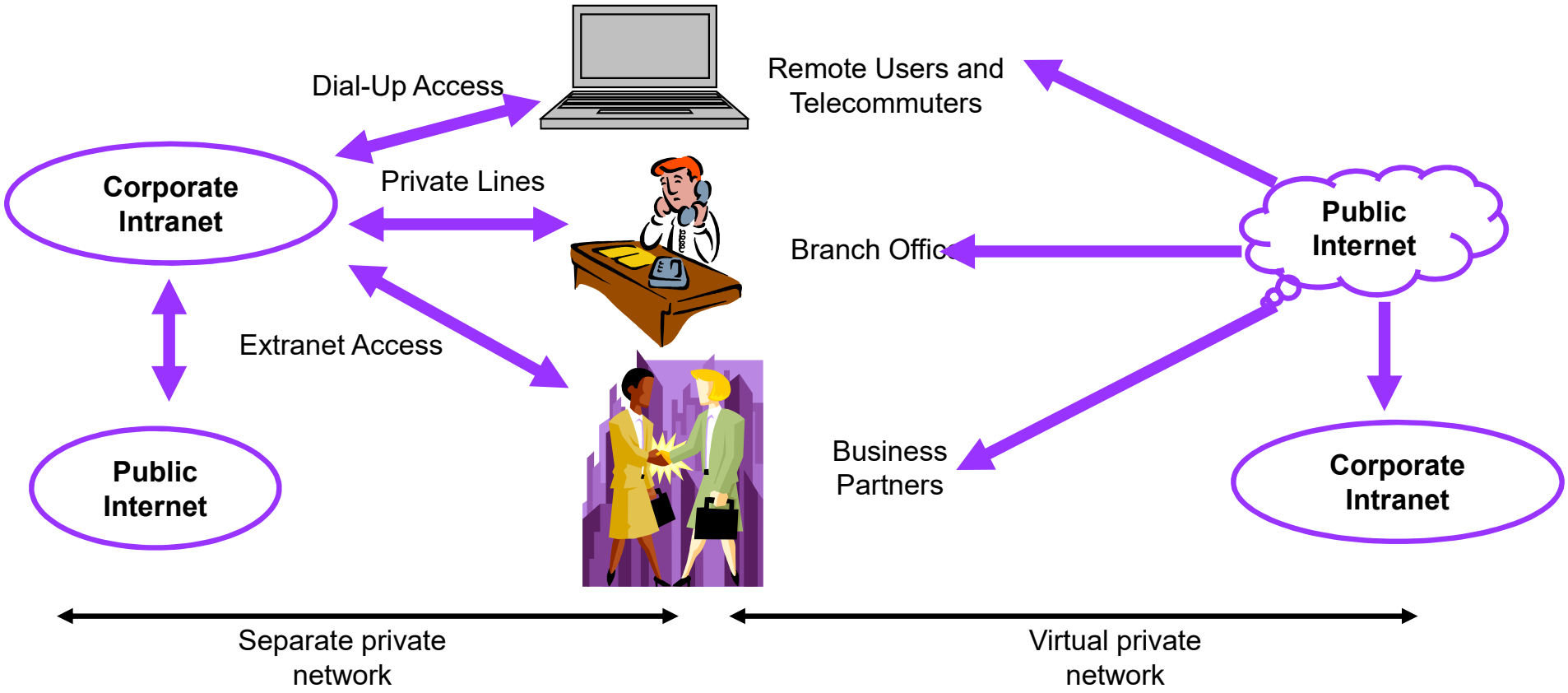
Virtual Private Network (VPN)

Virtual

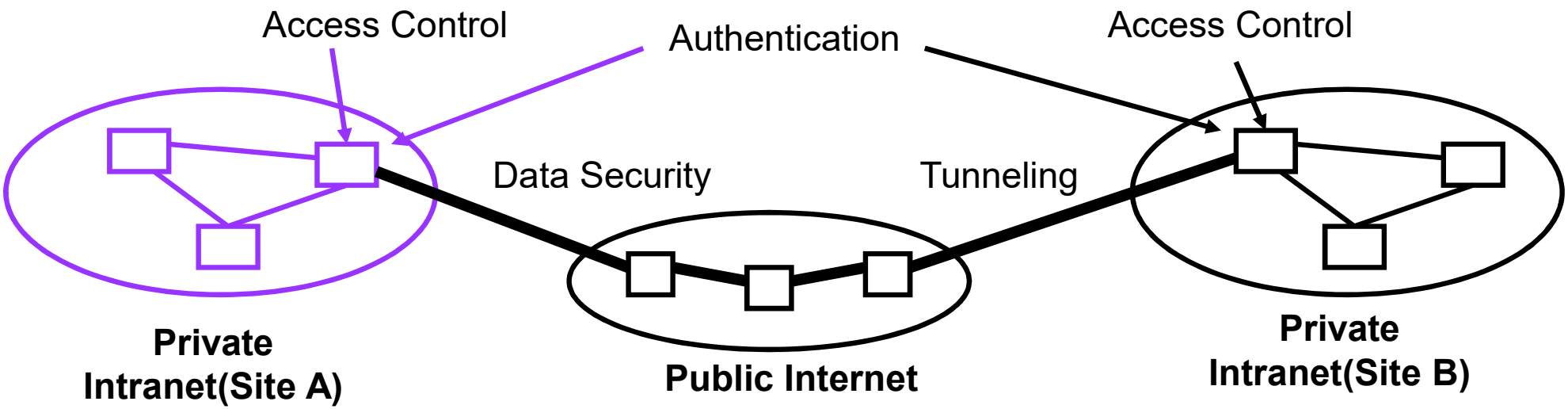
- ✓ ***No*** physical infrastructure ***dedicated*** to the private network

Private

- ✓ Keep data confidential so that it can be received by an intended receiver



VPN Technologies



Tunneling

- ✓ PPTP, L2TP, L2F, MPLS , IPsec and etc.

Authentication

- ✓ Radius, CHAP, PKI and etc.

Access Control

- ✓ PKI and etc.

Data Security

- ✓ IPsec, PKI, SSL, TSL and etc.