Network Security

2008. 3. 21.

Prof. Byoungcheon Lee
Joongbu University
sultan@joongbu.ac.kr

KADO KOREA AGENCY FOR DIGITAL OPPORTUNITY & PROMOTION

Outline

1. Overview of Internet Security
- Internet Security Issues
- Security Threat, Mechanism, Service

2. Attacks and Countermeasures
- Various security attacks and their countermeasures

3. Securing Network with IS Products
- Firewall
- Intrusion Detection System

4. Authentication

5. Communications Security
- VPN
- IPSec
- SSL/TLS

6. Security Management
- Information security industry
- Enterprise security management
- Penetration Testing for Intrusive Attacks

7. Applications Security
- E-commerce in Korea

1. Overview of Internet Security

- What is the Internet?
- Internet Security Issues
- Security Threat, Mechanism, Service
- Internet Security Technologies

What is the Internet?

- Collection of networks that communicate
  - with a common set of standard protocols (TCP/IP)
  - by multilateral agreement
- Collection of networks with
  - no central control
  - no central authority
  - no common legal oversight or regulations
  - no standard acceptable use policy
- Physical network connections not important
  - leased lines, dial-up, wireless
- Logical connectivity
  - everything is connected to everything else

Internet Security Issues (1)

- **Internet Infrastructure is Inherently Insecure**
  - Security was not a design consideration of Internet protocols
  - Unauthenticated routing protocols control Internet reachability
  - Add-on security is hard on users and hard to integrate into applications

- **Increasing Complexity of Network & Applications**
  - Increasing complexity of network connectivity
    - Varying collection of ISPs, Wireless WAN/LAN, Home networking …
    - Dial-up, DSL, Cable modem, Wireless, Satellite, Power line …
  - Increasing complexity of network protocols & applications
    - Peer-to-peer networking protocols, multimedia over IP
  - Internet everywhere: More complexity of management
    - Mobile phones, home appliances ...
  - Complexity is the Worst Enemy of Security & Management

Internet Security Issues (2)

- **More Distributed Networking / Applications Emerging**
  - Distributed file sharing/computing
  - Peer-to-peer networking, Home networking
  - Ubiquitous computing

- **Vulnerable Software Everywhere**
  - Vulnerability in software is inevitable and continues to appear
  - Vulnerable security products deployed

- **Sophistication & Automation of Attack Tools**
  - Attack tools / toolkits are becoming more sophisticated, automated, easy to use & hard to trace back
  - No specific knowledge required to mount attacks
  - Global collaboration is essential

Threats Analysis

- Who is Vulnerable?
  - Financial institutions and banks
  - Internet service providers
  - Government and defense agencies
  - Multinational corporations
  - **ANYONE ON THE NETWORK**

- What do we need to protect
  - Data
  - Resources
  - Reputation

Top Corporate Security Threats

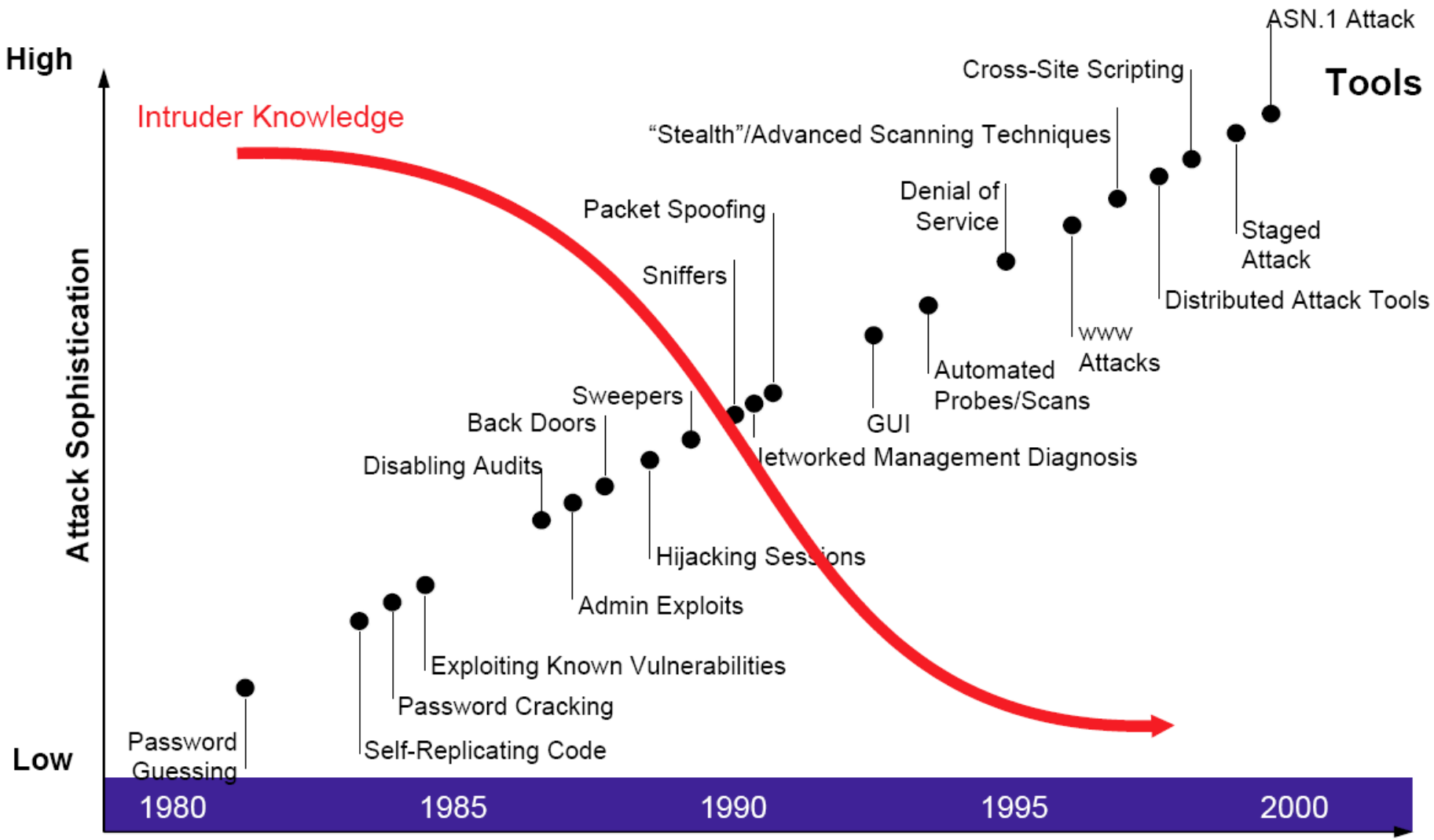
1. External hackers attacking your systems' availability
2. Security defects / vulnerabilities in hardware and software
3. External hackers attacking your corporate information
4. Employee errors in software and computer use
5. Employee actions that are intentionally harmful
6. Natural disasters
7. Theft of physical assets
8. Unauthorized wireless network access
9. Terrorism

Security Attacks

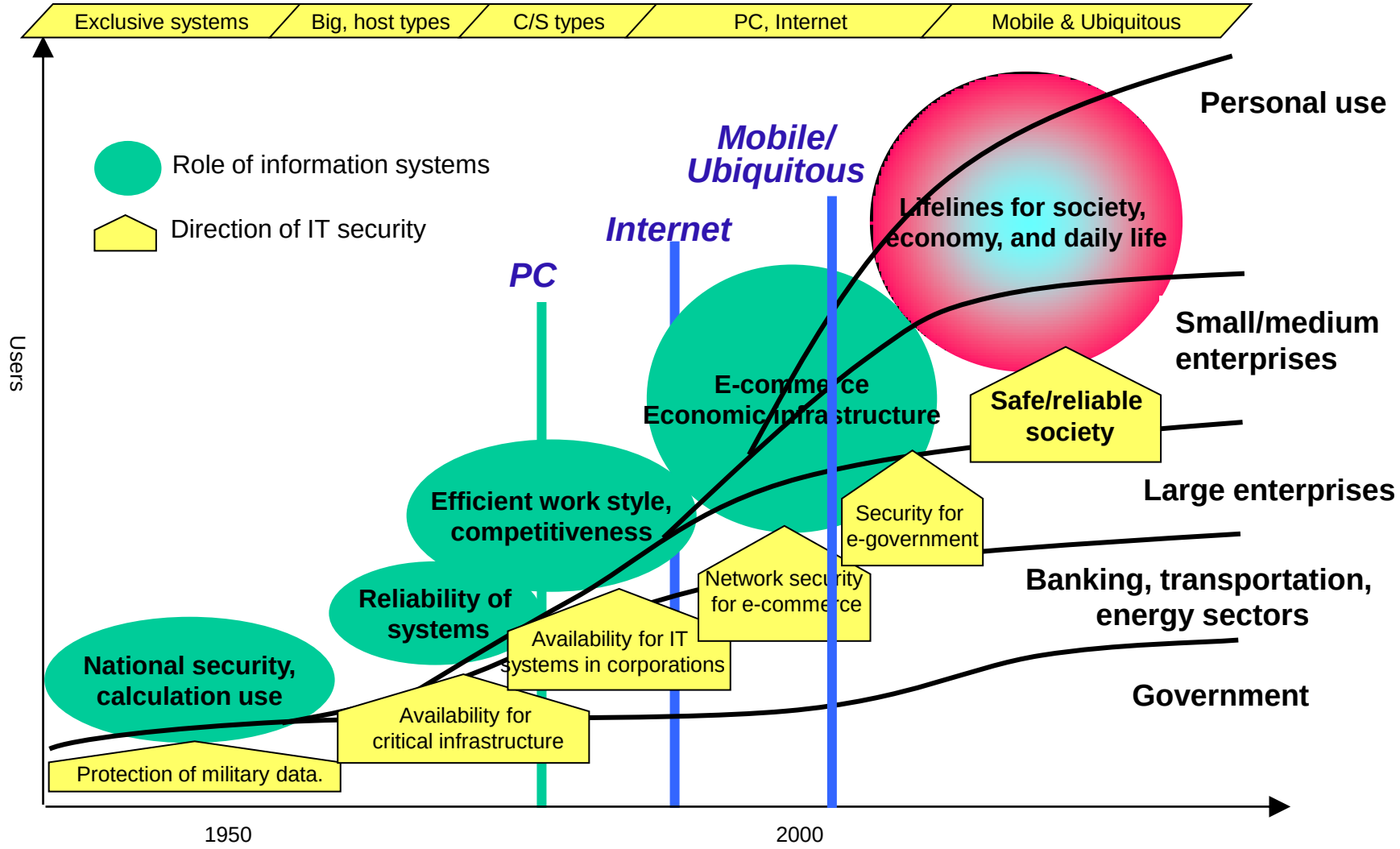
- **Passive (Observing the information from the system)**
  - **Sniffing**
  - **Wiretap**
  - **TEMPEST : detecting information from Transient Electromagnetic Pulse**
  - **Social Engineering**

- **Active (Try to alter system resources or affect their operation)**
  - **Worm : program that replicates itself through network**
  - **Logic bomb : malicious instructions that trigger on some event in the future, such as a particular time occurring**
  - **Trojan horse : program that does something unexpected (and often secretly)**
  - **Trapdoor : an undocumented entry point intentionally written into a program, often for debugging purposes, which can be exploited as a security flaw**
  - **Virus : program fragment that, when executed, attached itself to other programs**

Evolution of Attack

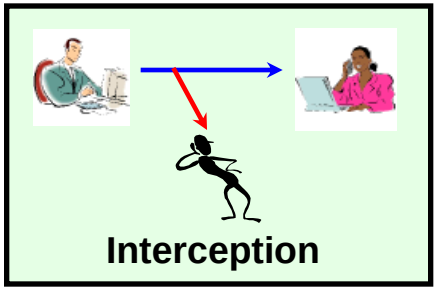


Trends of IT Security



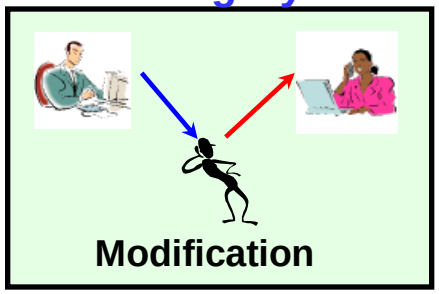
Security Needs for Network Communications

Confidentiality



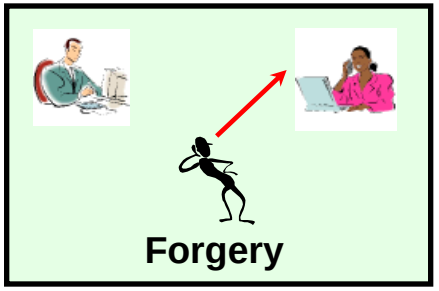
Is Private?

Integrity



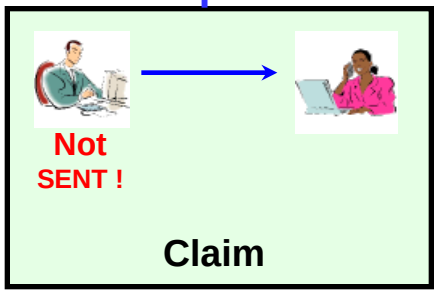
Has been altered?

Authentication



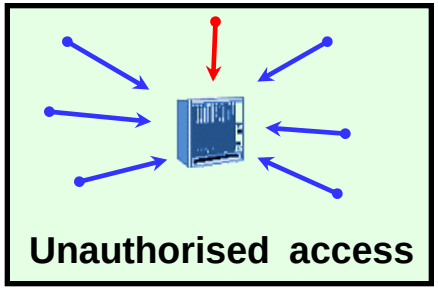
Who am I dealing with?

Non-Repudiation



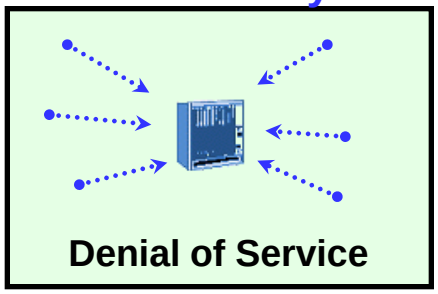
Who sent/received it?

Access Control



Have you privilege?

Availability



Wish to access!!

Authenticity

On the Internet, nobody knows you're a dog

"On the Internet, nobody knows you're a dog."

The OSI Security Architecture

- ITU-T Recommendation X.800, *Security Architecture for OSI* defines

  - **Security attack**
    - **Any action that compromises the security of information**

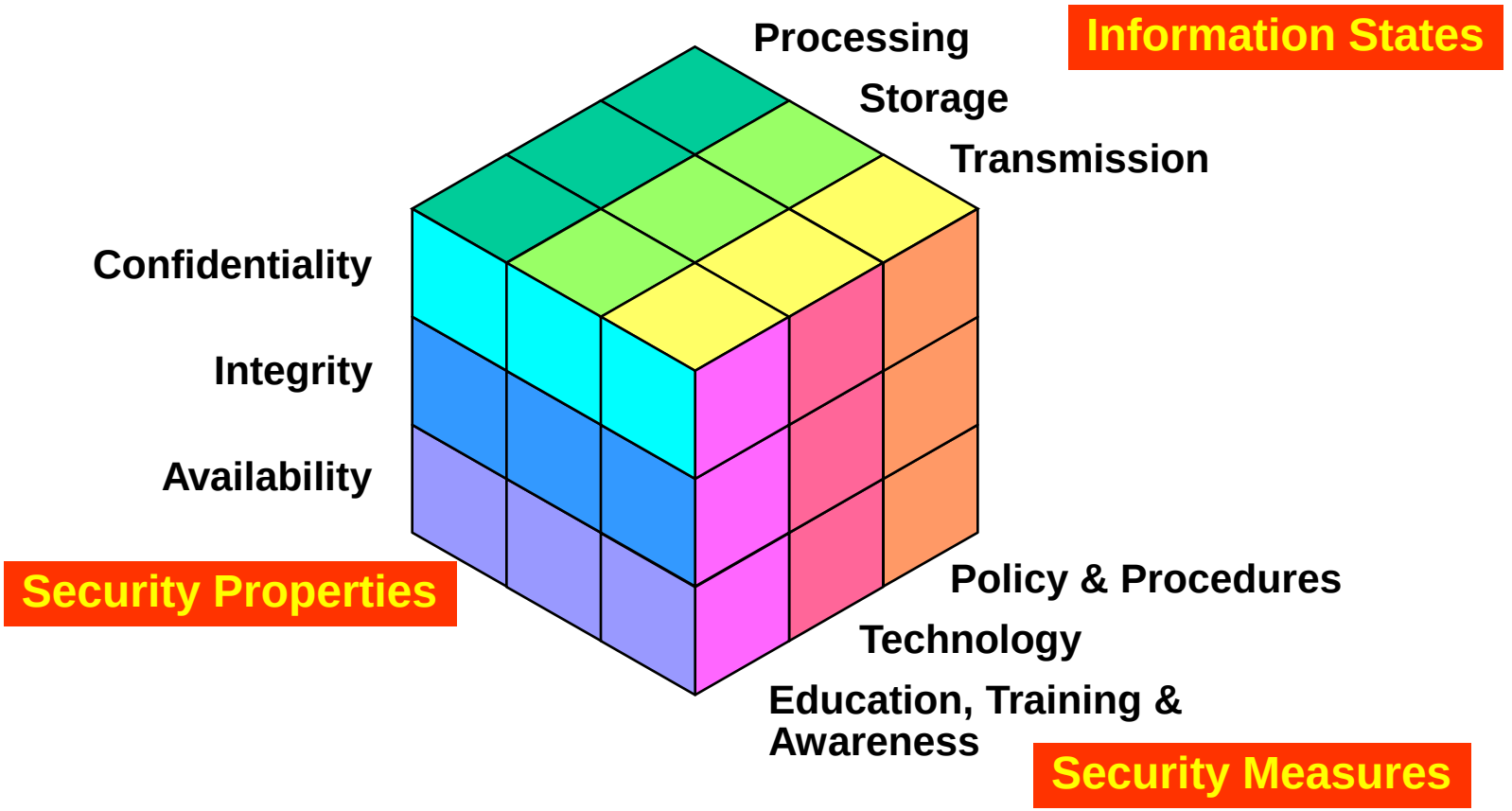
  - **Security mechanism**
    - **A process designed to detect, prevent, or recover from a security attack**

  - **Security service**
    - **A service making use of security mechanisms to counter security attacks.**

The OSI Security Architecture

Security Attacks	Security Mechanisms	Security Services
Interception	Encryption	Confidentiality
Forgery	Authentication	Authentication
Modification	Digital signature	Integrity
Denial of facts	Key exchange	Non-repudiation
Unauthorized access	Access control	Access control
Interruption	Monitoring & Responding	Availability

Information Security



NSTISSI 4011: National Training Standard for Information Systems Security Professionals, 1994

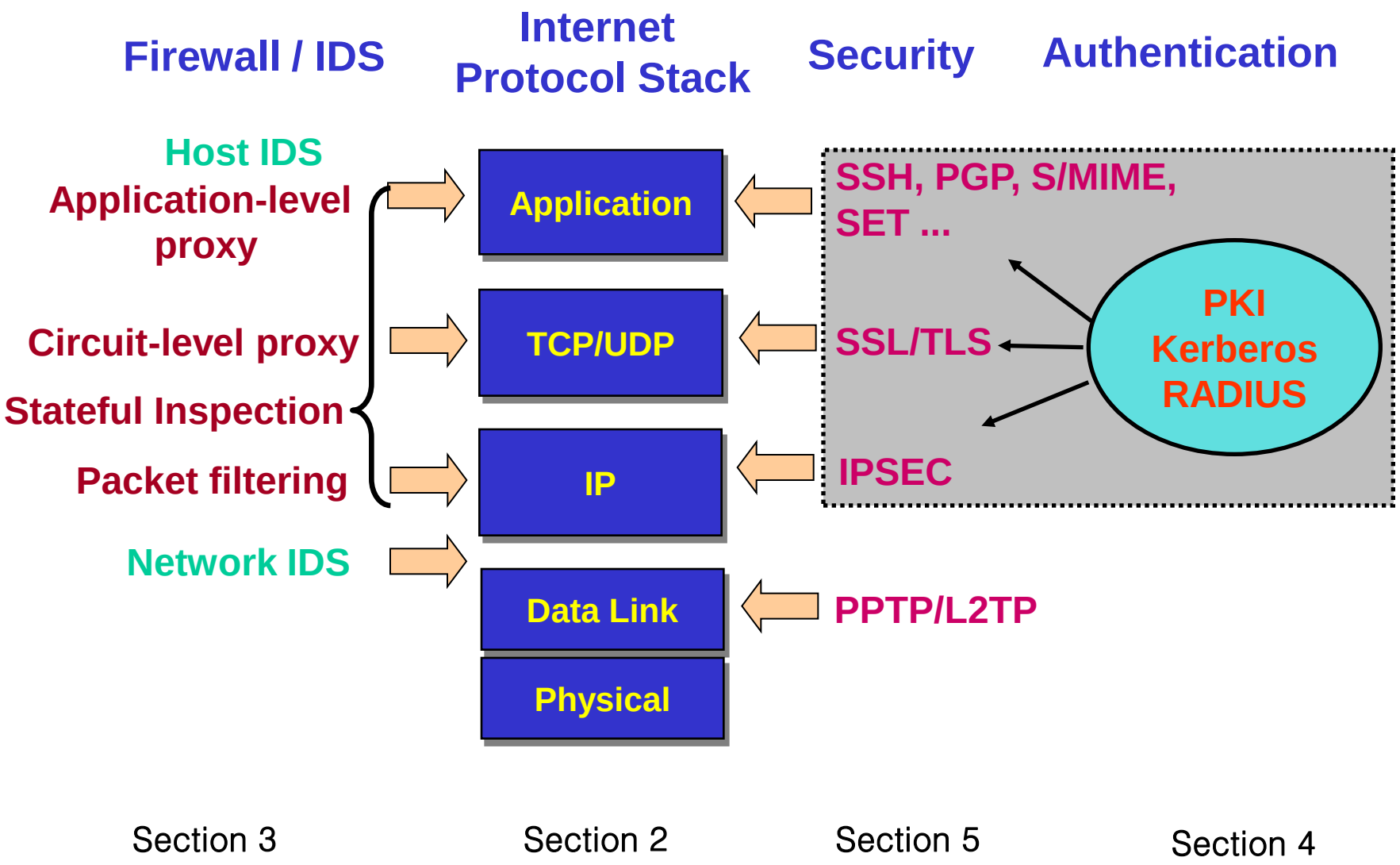
Information Security C.I.A.

- Information Security
  - Discipline that protects the Confidentiality, Integrity & Availability of information, during processing, storage & transmission, through Policies, Technologies & Operations
  - Network/Communication security, Host/Computer security

- C.I.A. of Information Security
  - Confidentiality: Protecting from unauthorized disclosure
  - Integrity: Protecting from unauthorized modification
  - Availability: Making information accessible/available when needed

- How to Achieve Information Security
  - Policies : what should do, what should not do, etc., for information security
  - Technologies: implementing the policies
  - Operations: assessment & improvement on the implemented technologies

Major Internet Security Technologies



2. Attacks and Countermeasures

- TCP/IP attacks
- DOS attack
- Web attacks
- Spyware, Adware
- Phishing
- Social Engineering

Security Vulnerabilities

- Security Problems in the TCP/IP Protocol Suite – Steve Bellovin, 1989

- Attacks on Different Layers
  - IP Attacks
  - ICMP Attacks
  - Routing Attacks
  - TCP Attacks
  - Application Layer Attacks

Security Vulnerabilities - Why?

- TCP/IP was designed for connectivity, not considering security
  - Assumed to have lots of trust

- Host implementation vulnerabilities
  - Software “had/have/will have” bugs
  - Some elements in the specification were left to the implementers

Security Flaws in IP

- The IP addresses are filled in by the originating host
  - Address spoofing
- Using source address for authentication
  - r-utilities (rlogin, rsh, rhosts, etc..)
- IP fragmentation attack
  - End hosts need to keep the fragments till all the fragments arrive

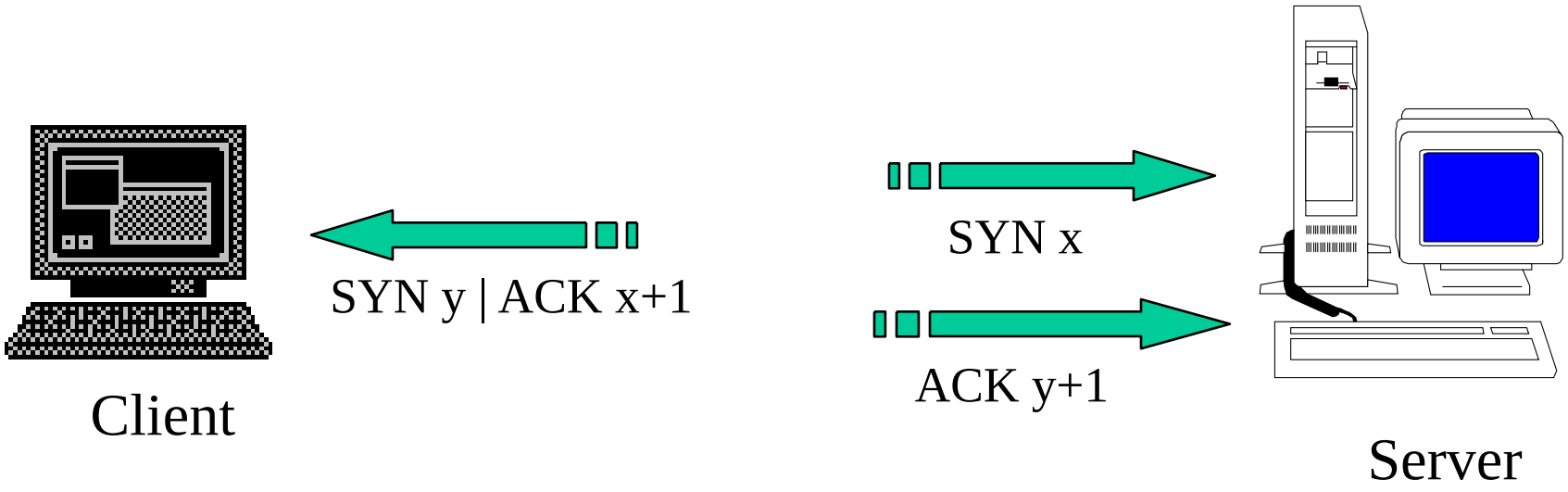
Packet Sniffing

- Packet Sniffing
  - Recall that Ethernet is a broadcast-based communication
  - Sniff other's packet: promiscuous NIC reads all packets passing by
  - Can read all unencrypted data (e.g. passwords)
- Countermeasures
  - run software that checks periodically whether host interface is in promiscuous mode.
  - Use encryption
    - **SSH, not Telnet**
    - **HTTP over SSL**
    - **SFTP, not FTP**
    - **IPSec**

ICMP Attacks

- No authentication in ICMP
- ICMP redirect message
  - Can cause the host to switch gateways
  - Benefit of doing this?
    - **Man in the middle attack, sniffing**
- ICMP destination unreachable
  - Can cause the host to drop connection
- ICMP echo request/reply
  - Can collect useful information

TCP Attacks



Issues?

- Server needs to keep waiting for ACK y+1
- Server recognizes Client based on IP address/port and y+1

TCP Attacks

- TCP Session Hijacking
  - When is a TCP packet valid?
    - Address/Port/Sequence Number in window
  - How to get sequence number?
    - Sniff traffic
    - Guess it: Many earlier systems had predictable ISN
  - If an attacker learns the associated TCP state for the connection, then the connection can be hijacked!
  - Attacker can insert malicious data into the TCP stream, and the recipient will believe it came from the original source
- TCP Session Poisoning
  - Send RST packet
    - Will tear down connection

Preventing TCP Attacks

- Use IPSec
  - Provides **source authentication**, so Mr. Big Ears cannot pretend to be Alice
  - **Encrypts data** before transport, so Mr. Big Ears cannot talk to Bob without knowing what the session key is

Application Layer Attacks

- Applications which DO NOT authenticate properly
- Authentication information in clear
  - FTP, Telnet, POP
- DNS insecurity
  - DNS poisoning
  - DNS zone transfer

Denial of Service (DoS)

- Objective: make a network service unusable, usually by overloading the server or network
- Consume host resources
  - TCP SYN floods
  - SMURF - ICMP ECHO (ping) floods
- Consume bandwidth
  - UDP floods
  - ICMP floods
- Crashing the victim
  - Ping-of-Death
  - TCP options (unused, or used incorrectly)

SYN Flooding Attack

- Send SYN packets with bogus source address
  - Server responds with SYN ACK and keeps state about TCP half-open connection
  - Eventually, server memory is exhausted with this state

- Solution: use “SYN cookies”
  - In response to a SYN, create a special “cookie” for the connection, and forget everything else
  - Then, can recreate the forgotten information when the ACK comes in from a legitimate connection

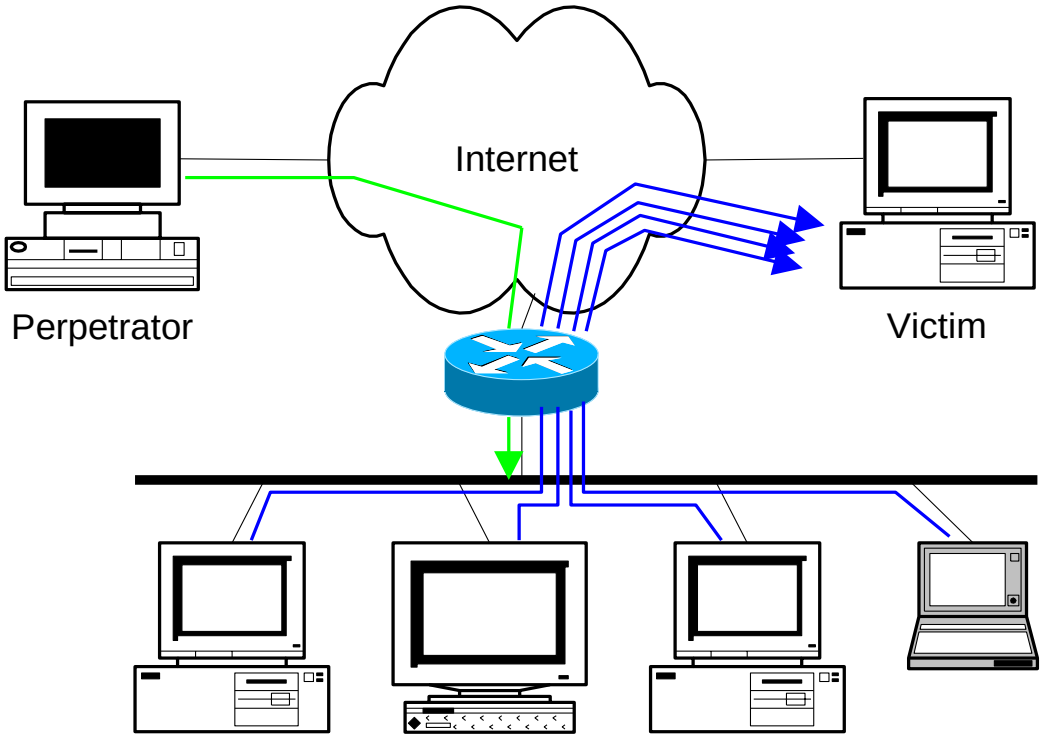
SMURF Attack

- SMURF
  - A way of generating a lot of computer network traffic to a victim site
  - Source IP address of a broadcast ping is forged, then large number of machines respond back to victim, overloading it

SMURF Attack

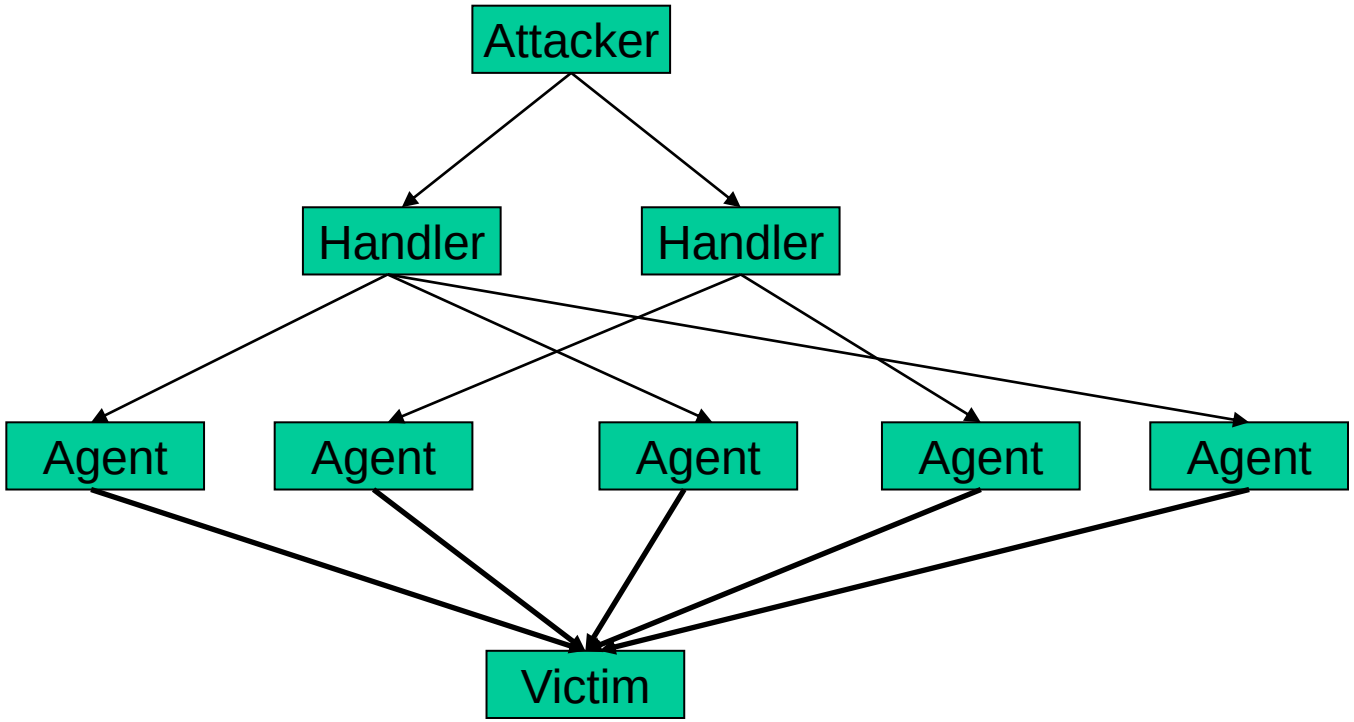
ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

ICMP echo reply



Distributed DoS

- Distributed Denial of Service
  - Same techniques as regular DoS, but on a much larger scale
  - Very difficult to track down the attacker



Case Study – CodeRed

- CodeRed
  - July 19, 2001: over 359,000 computers infected with Code-Red in less than 14 hours
  - Used a recently known buffer exploit in Microsoft IIS
  - Damages estimated in excess of $2.6 billion

Protect against DoS

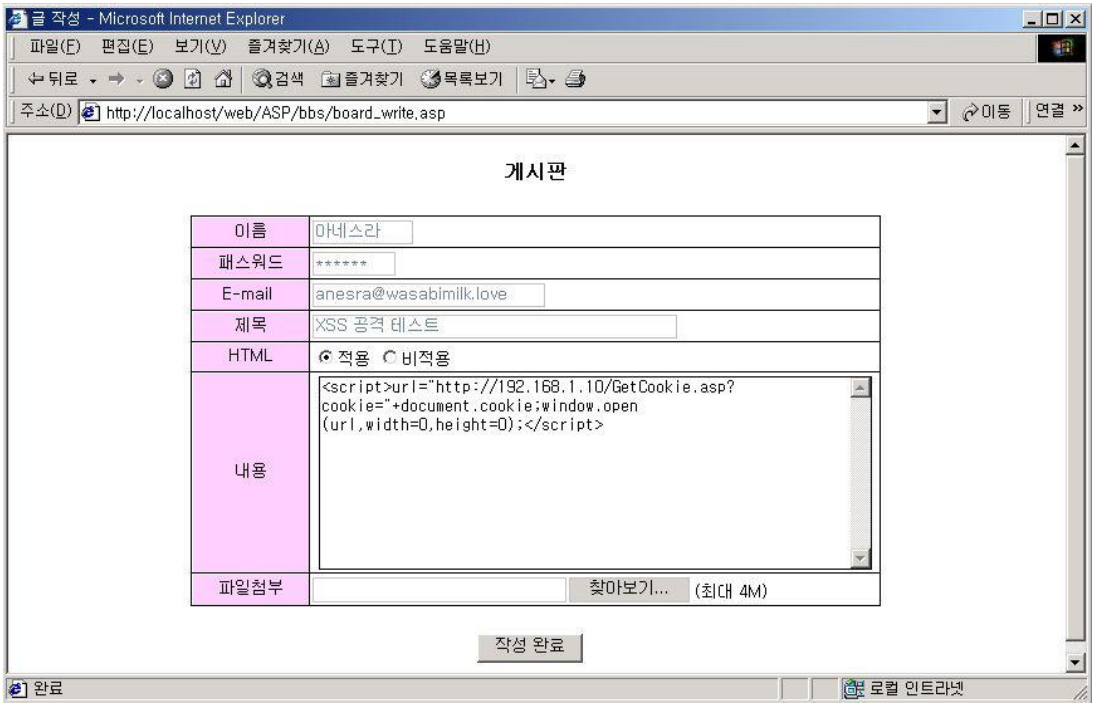
- How can we protect ourselves?
  - Ingress filtering
    - **A technique used to make sure that incoming packets are actually from the networks that they claim to be from**
    - **If the source IP of a packet comes in on an interface which does not have a route to that packet, then drop it**
    - **RFC 2267 has more information about this**
  - Stay on top of CERT advisories and the latest security patches
    - **A fix for the IIS buffer overflow was released** sixteen days before **CodeRed had been deployed!**

Web Services Threats

- SQL Injections
  - Special characters in queries
- Capture and Replay Attacks
  - Man in the middle attacks
- DoS (resulting from a large load)
  - Blow up application from inside
- Improper Error Handling
  - Dump of stack trace etc
- Broken Access Control
  - Take over earlier sessions tokens etc

Web Hacking

- Web hacking
  - File upload
  - Directory traversal
  - Directory listing
  - Skipping authentication
  - SQL injection
  - XSS



Spyware and Adware

- Spyware
  - Any technology that aids in gathering information about a person or organization without their knowledge. On the Internet (where it is sometimes called a *spybot* or *tracking software*), spyware is programming that is put in someone's computer to secretly gather information about the user and relay it to advertisers or other interested parties.
- Adware
  - Any software application in which advertising banners are displayed while the program is running. The authors of these applications include additional code that delivers the ads, which can be viewed through pop-up windows or through a bar that appears on a computer screen

Phishing Example

From: Microsoft Corporation Technical Bulletin [ljseedwnge-oswojtfbv@confidence.com] **Sent:** Thu 9/18/2003 3:32 PM
To: MS Customer
Cc:
Subject: Network Critical Patch

Microsoft

All Products | Support | Search | Microsoft.com Guide

Microsoft Home

Microsoft Customer

This is the latest version of security update, the 'September 2003, Cumulative Patch' update which resolves all known security vulnerabilities affecting MS Internet Explorer, MS Outlook and MS Outlook Express as well as three new vulnerabilities. Install now to help maintain the security of your computer from these vulnerabilities. This update includes the functionality of all previously released patches.

Phishing Example

Dear Citibank Customer

We were unable to process the recent transactions on your account. To ensure that your account is not suspended, please update your information by clicking here.

If you have recently updated your information, please disregard this message as we are processing the changes you have made.

Citibank Customer Service
Citibank Alerting Service
Citibank [alert@citibank.com]

Links to http://82.90.165.65/citi

Phishing Basics (1)

- Scam to **steal valuable information** such as credit cards, social security numbers, user IDs and passwords.
- Also known as "brand spoofing"
- Official-looking e-mail sent to potential victims
  - Pretends to be from their ISP, retail store, etc.,
  - Due to internal accounting errors or some other pretext, certain information must be updated to continue the service.

Phishing Basics (2)

- Link in e-mail message directs the user to a Web page
  - Asks for financial information
  - Page looks genuine
    - **Easy to fake valid Web site**
    - **Any HTML page on the real Web can be copied and modified**
- E-mails sent to people on selected lists or to any list
  - Some % will actually have account
- “Phishing kit"
  - Set of software tools
  - Help novice phisher imitate target Web site
  - Make mass mailings
  - May include lists of e-mail addresses

Possible Solutions

- Strong authentication
  - Strong Website authentication,
  - Mail server authentication
  - Digitally-signed e-mail with desktop verification
  - Digitally-signed e-mail with gateway verification
- Public Education
  - Use digitally-signed documents ONLY
    - **Don’t release unsigned documents**
    - **Get consumers used to idea that an unsigned document is an untrustworthy document**
  - Use public education campaigns
    - **“No one will ever ask you to confirm your password”**

Social Engineering

- Social Engineering
  - A collection of techniques used to manipulate people into performing actions or divulging confidential information
- People can be just as dangerous as unprotected computer systems
  - People can be lied to, manipulated, bribed, threatened, harmed, tortured, etc. to give up valuable information
- There aren't always solutions to all of these problems
  - Educating them may help a little here, but, depending on how bad you want the information, there are a lot of bad things you can do to get it
  - So, the best that can be done is to implement a wide variety of solutions and more closely monitor who has access to what network resources and information

Security Attacks and Their Countermeasures

- Finding a way into the network
  - Firewalls
- Exploiting software bugs, buffer overflows
  - Intrusion Detection Systems
- Denial of Service
  - Ingress filtering, IDS
- TCP hijacking
  - IPSec
- Packet sniffing
  - Encryption (SSH, SSL, HTTPS)
- Social problems
  - Education

3. Securing Networks with IS Products

- Firewall
- Intrusion Detection System
- Intrusion Prevention System
- Anti-virus, Anti-spyware

Firewall and IDS

Firewall – Security Guard

IDS – Security monitor and alarm

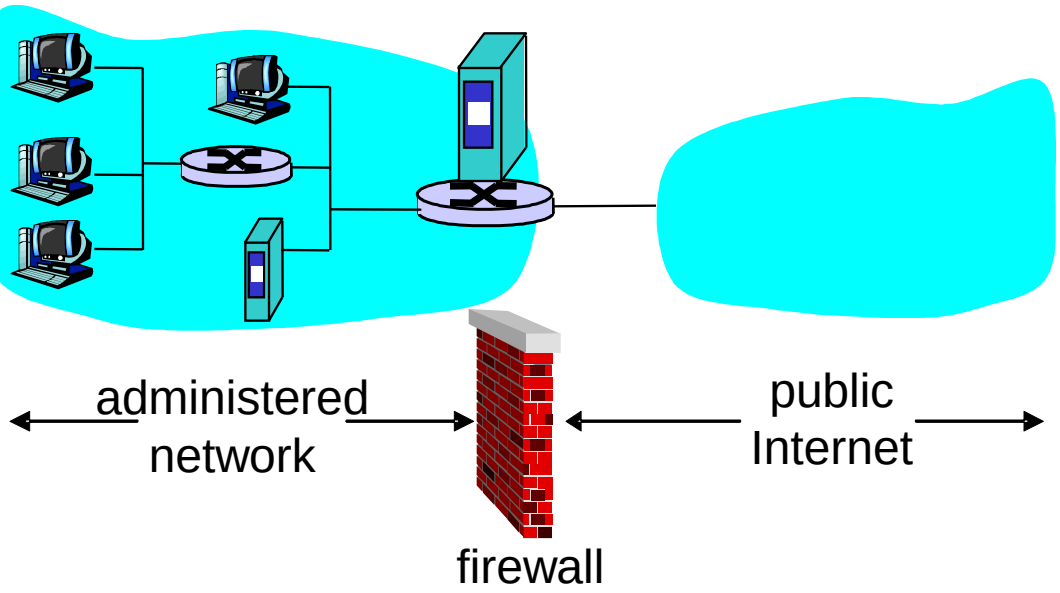
Firewalls

- Basic problem – many network applications and protocols have security problems that are fixed over time
  - Difficult for users to keep up with changes and keep host secure
  - Solution
    - **Administrators limit access to end hosts by using a firewall**
    - **Firewall is kept up-to-date by administrators**

Firewalls

Firewall

isolates organization's internal network from larger Internet, allowing some packets to pass, blocking others.



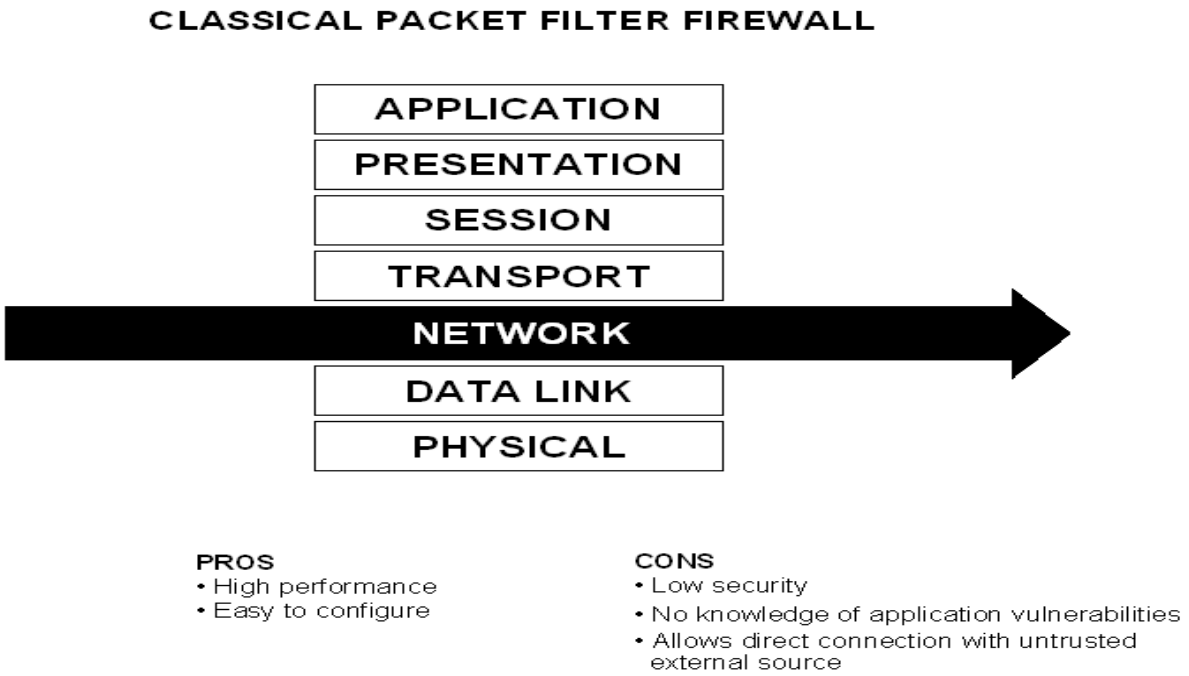
Firewalls

- Firewall inspects traffic through it
  - Allows traffic specified in the policy
  - Drops everything else

- Two Types
  - Packet Filters
  - Application Proxies

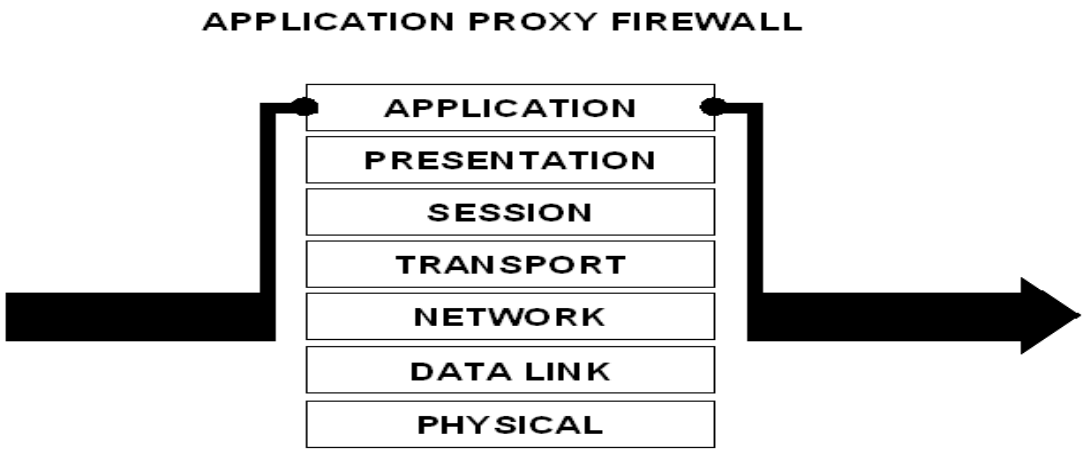
Packet Filter Firewalls

- Packet Filter Firewalls
  - Looks at the header of each packet and compares the IP address and port of the source and destination against its rule base.



Application Proxy Firewalls

- Application Proxy Firewall
  - Full application-level awareness of attempted connections.

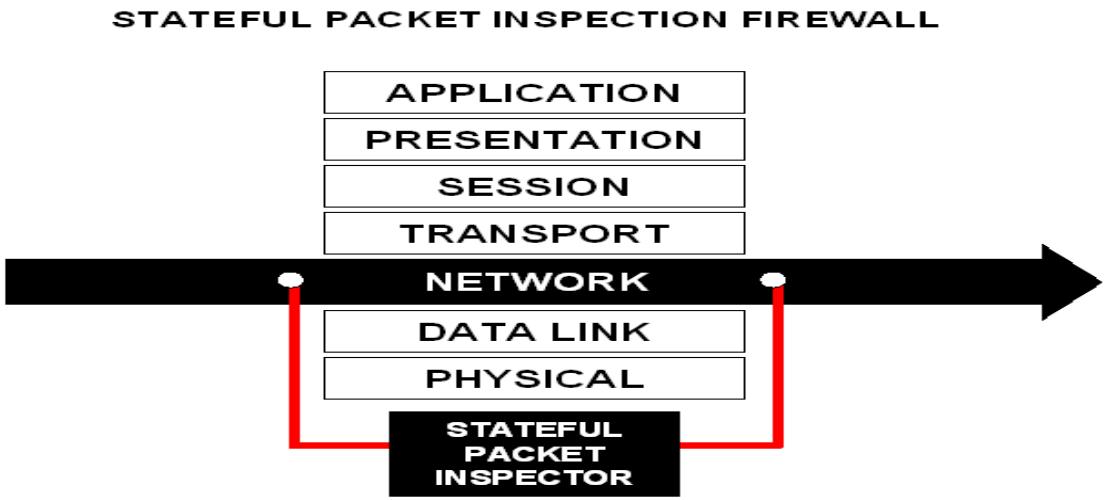


PROS
- Strongest security available
- Full knowledge of vulnerabilities at highest layer of data stack
- Access limited to finite set of clearly identifiable tasks in proxy itself
- Firewall "proxies" connection, never allowing direct contact between trusted and untrusted systems

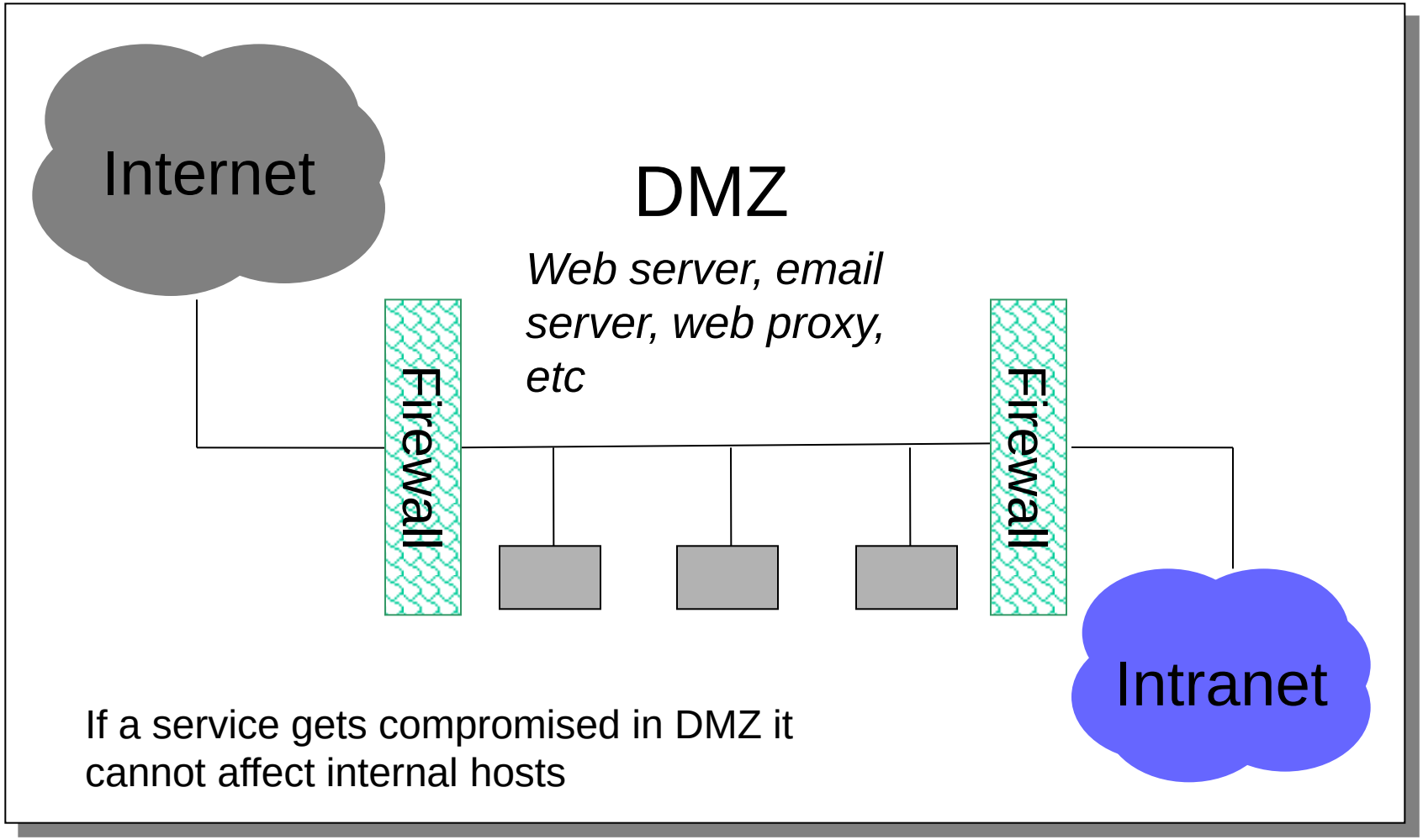
CONS
- Added security can negatively impact performance

Stateful Packet Inspection

- Stateful Packet Inspection
  - State-related information is examined in this inspection module, then maintained in dynamic state tables for evaluating subsequent connection attempts.



Firewalls and DMZ



Intrusion Detection System

- Firewall problems
  - Firewalls allow traffic only to legitimate hosts and services
  - Traffic to the legitimate hosts/services can have attacks (CodeReds on IIS)

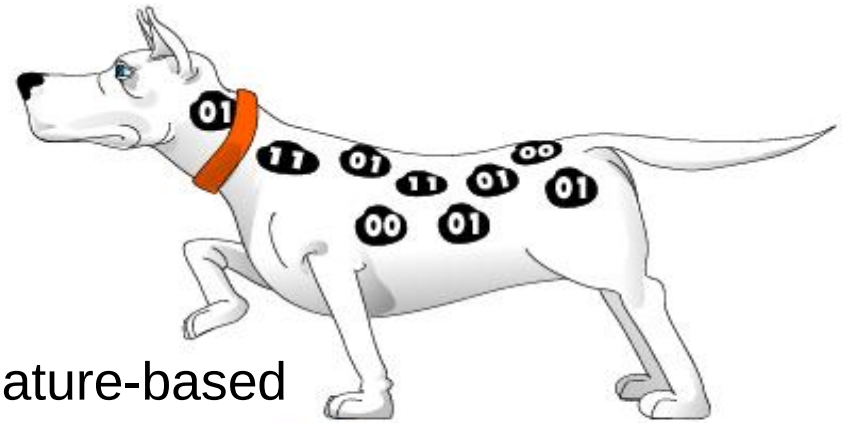
- Solution?
  - Intrusion Detection Systems
  - Monitor data and behavior
  - Report when identify attacks

Intrusion Detection System

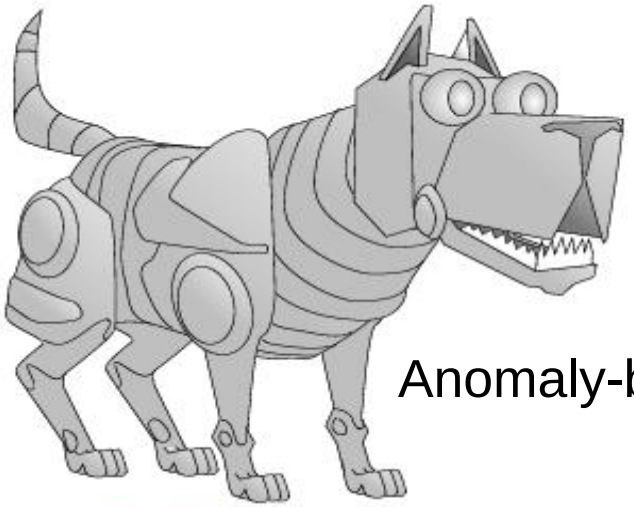
- Used to monitor for “suspicious activity” on a network
  - Can protect against known software exploits, like buffer overflows
- Uses “intrusion signatures” (Well known patterns of behavior)
  - Ping sweeps, port scanning, web server indexing, OS fingerprinting, DoS attempts, etc.

Types of IDS

What kind of Watchdog?

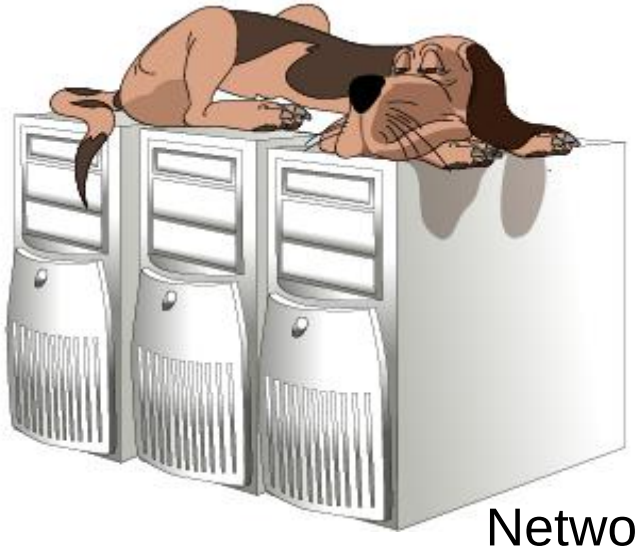


Signature-based



Anomaly-based

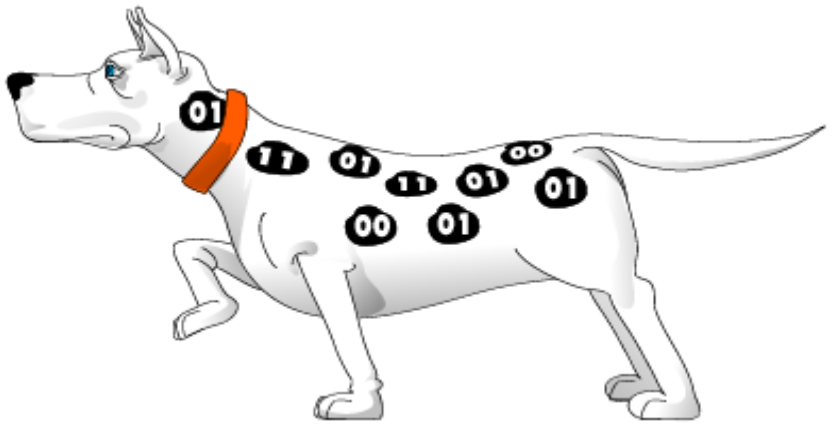
Host-based



Network-based

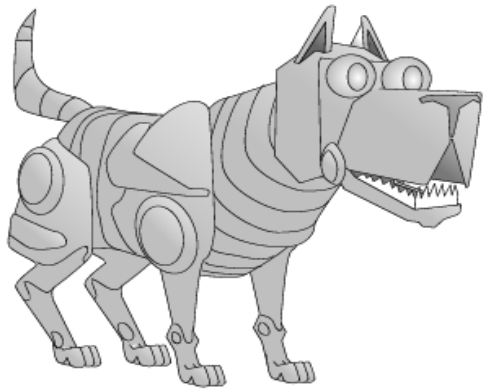
Signature-based IDS

- Characteristics
  - Uses known pattern matching to signify attack
- Advantages?
  - Widely available
  - Fairly fast
  - Easy to implement
  - Easy to update
- Disadvantages?
  - Cannot detect attacks for which it has no signature



Anomaly-based IDS

- Characteristics
  - Uses statistical model or machine learning engine to characterize normal usage behaviors
  - Recognizes departures from normal as potential intrusions
- Advantages?
  - Can detect attempts to exploit new and unforeseen vulnerabilities
  - Can recognize authorized usage that falls outside the normal pattern
- Disadvantages?
  - Generally slower, more resource intensive compared to signature-based IDS
  - Greater complexity, difficult to configure
  - Higher percentages of false alerts

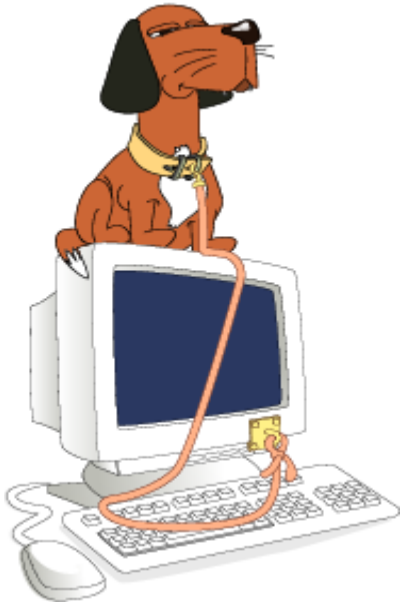


Network-based IDS

- Characteristics
  - NIDS examine raw packets in the network passively and triggers alerts
- Advantages?
  - Easy deployment
  - Unobtrusive
  - Difficult to evade if done at low level of network operation
- Disadvantages?
  - Fail Open
  - Different hosts process packets differently
  - NIDS needs to create traffic seen at the end host
  - Need to have the complete network topology and complete host behavior

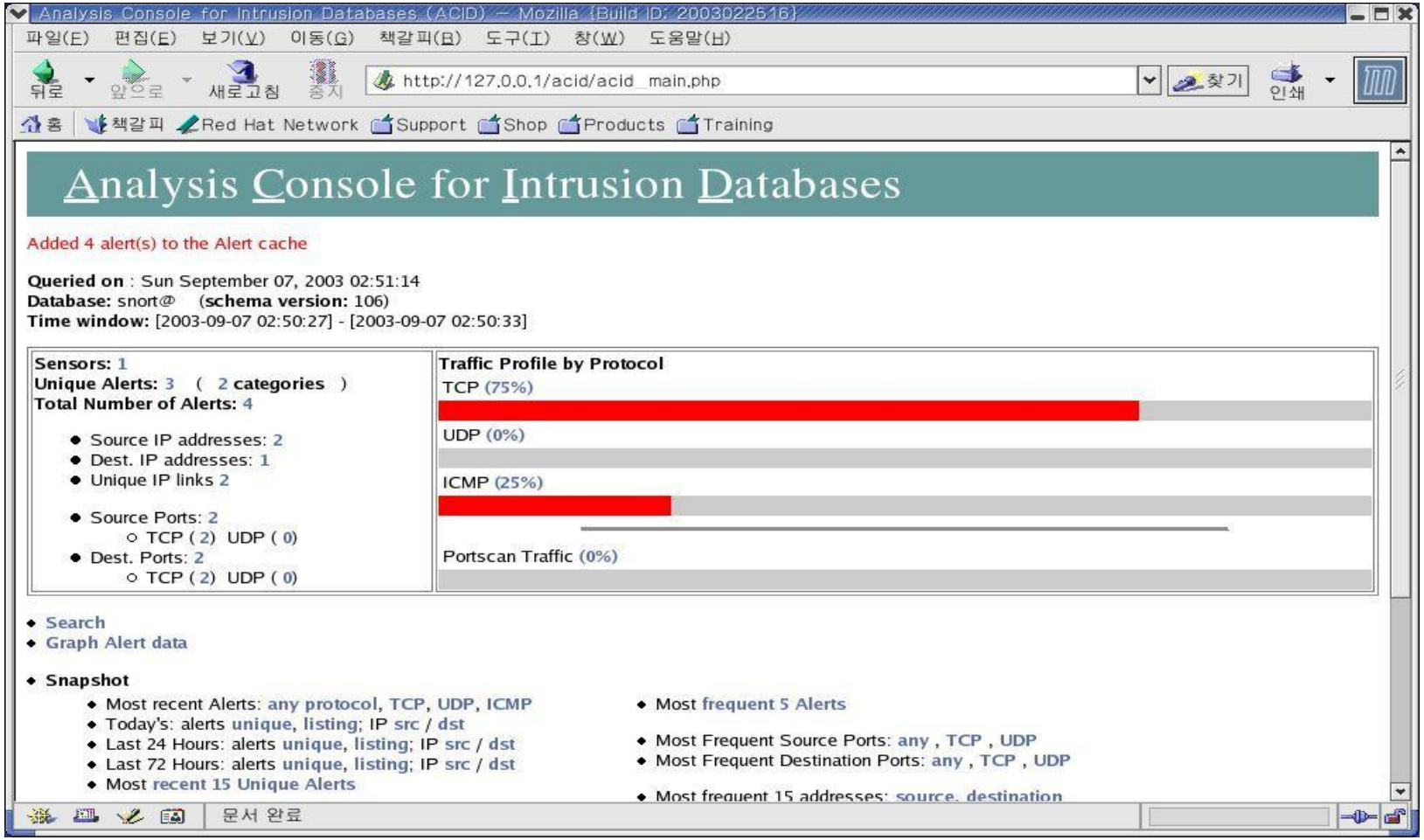
Host-based IDS

- Characteristics
  - Runs on single host
  - Can analyze audit-trails, logs, integrity of files and directories, etc.
- Advantages
  - More accurate than NIDS
  - Less volume of traffic so less overhead
- Disadvantages
  - Deployment is expensive
  - What happens when host get compromised?



SNORT

- Open Source IDS: Snort, www.snort.org



Intrusion Prevention System

- Intrusion Prevention System
  - A system located on the network that monitors the network for issues like security threats and policy violations, then takes corrective action.
  - Combine the roles of firewall and IDS

- IPS can detect and block:
  - OS, Web and database attacks
  - Spyware / Malware
  - Instant Messenger
  - Peer to Peer (P2P)
  - Worm propagation
  - Critical outbound data loss (data leakage)

4. Authentication

Authentication

- Entity Authentication (Identification)
  - Over the communication network, one party, Alice, shows to another party, Bob, that she is the real Alice.
  - Authenticate an entity by presenting some identification information
  - Should be secure against various attacks
  - Through an interactive protocols using secret information

- Message Authentication
  - Show that a message was generated by an entity
  - Using digital signature or MAC

3 Approaches for Identification

- Using Something Known
  - Password, PIN
- Using Something Possessed
  - IC card, Hardware token
- Using Something Inherent
  - Biometrics

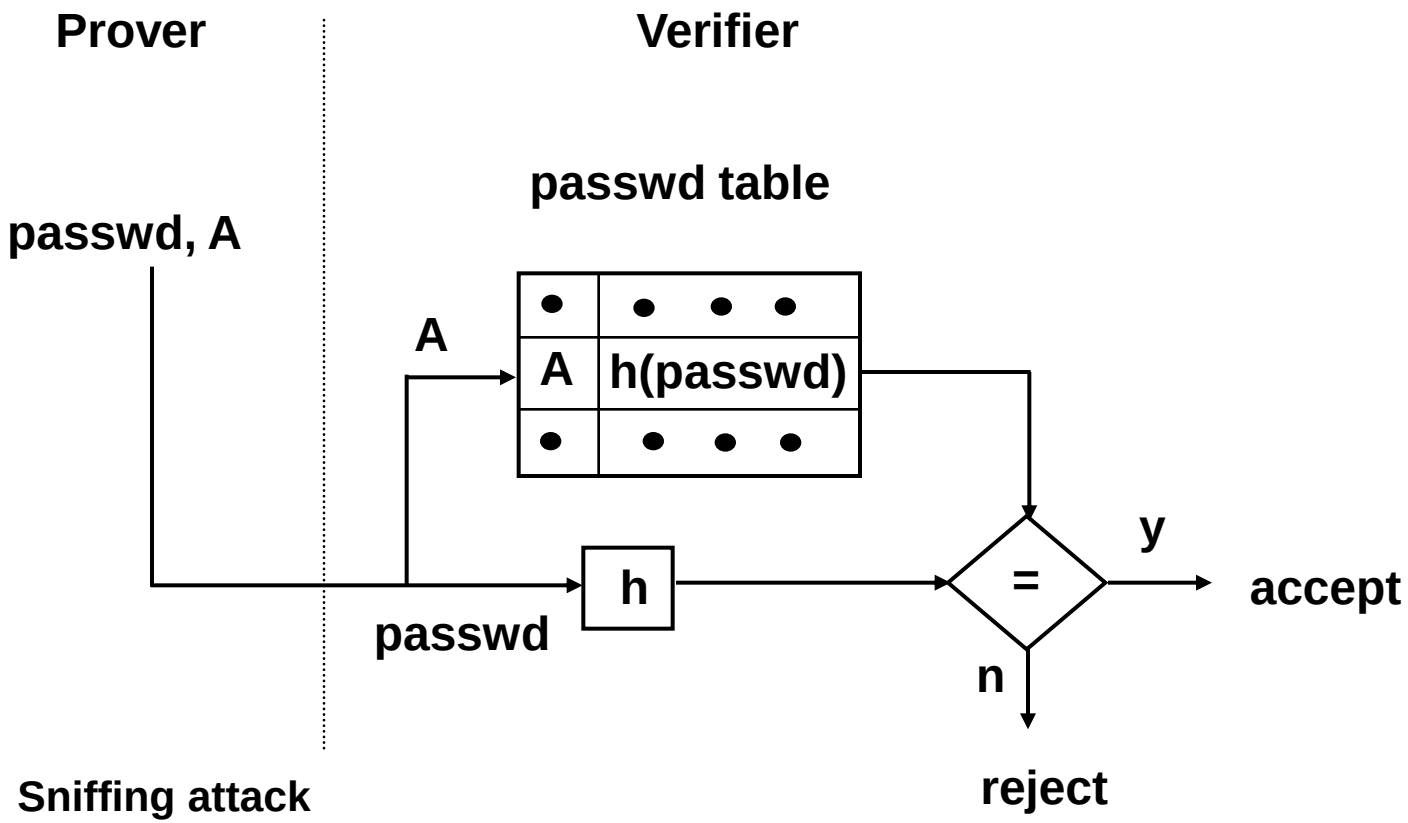
RSA SecurID

Two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator)

Identification Schemes

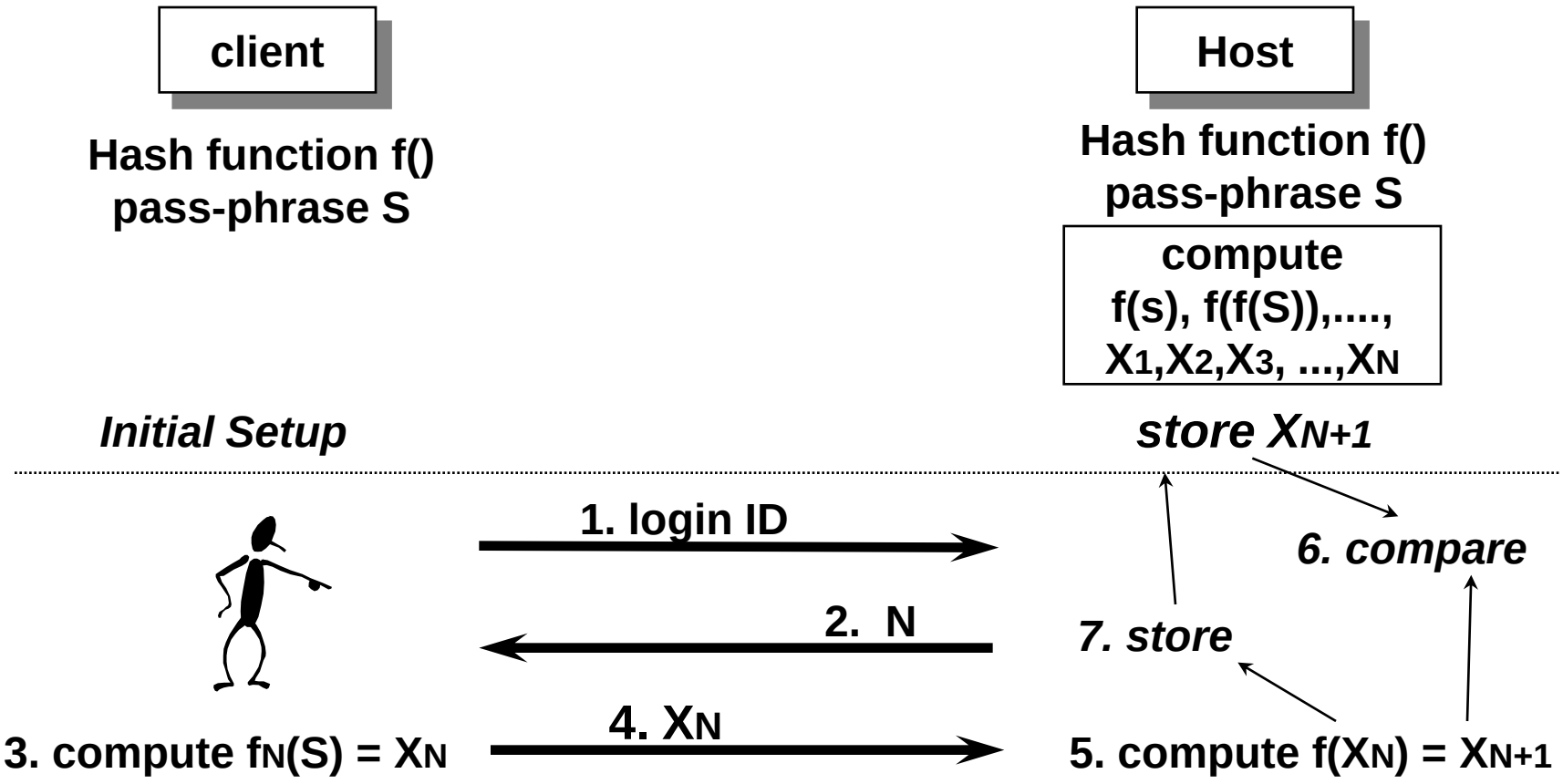
- Password-based scheme (weak authentication)
  - crypt *passwd* under UNIX
  - one-time password
- Challenge-Response scheme (strong authentication)
  - Symmetric cryptosystem
  - MAC (keyed-hash) function
  - Asymmetric cryptosystem
- Using Cryptographic Protocols
  - Fiat-Shamir identification protocol
  - Schnorr identification protocol, *etc*

Identification by Password



Sniffing attack
Replay attack - Static password

S/Key (One-Time Password System)



Schnorr Identification

$$x = \log_g Y \bmod p, \qquad (Y = g^x \bmod p)$$

Prover | **Verifier**

$t \in_R Z_q^*$

$R = g^t \bmod p$

R **Commitment** →

$u \in_R Z_q^*$

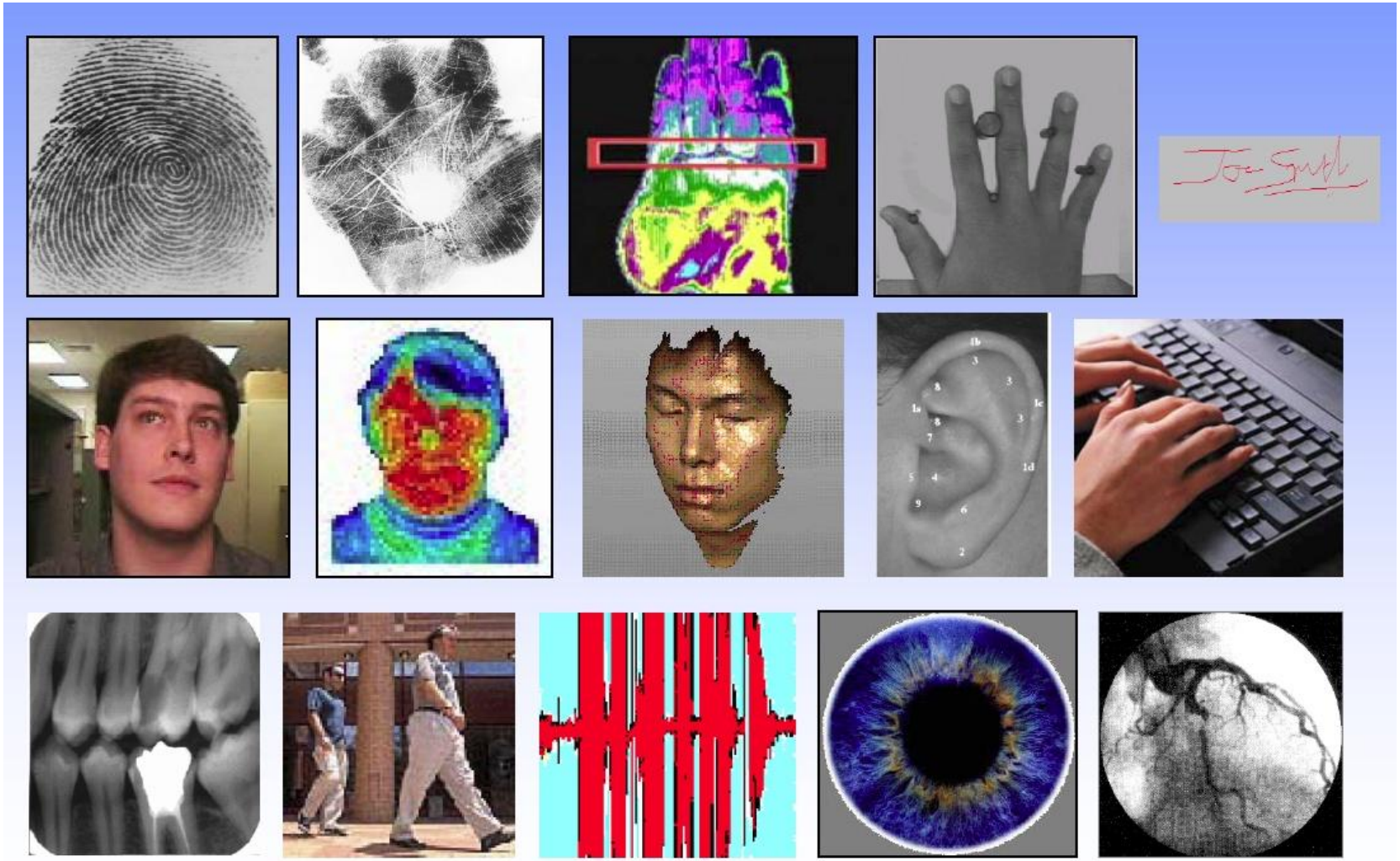
← u **Challenge**

$w = t - ux \bmod q$

w **Response** →

$R \overset{?}{=} g^w Y^u \bmod p$

Identification using Biometric Trails



Certificate-based Authentication

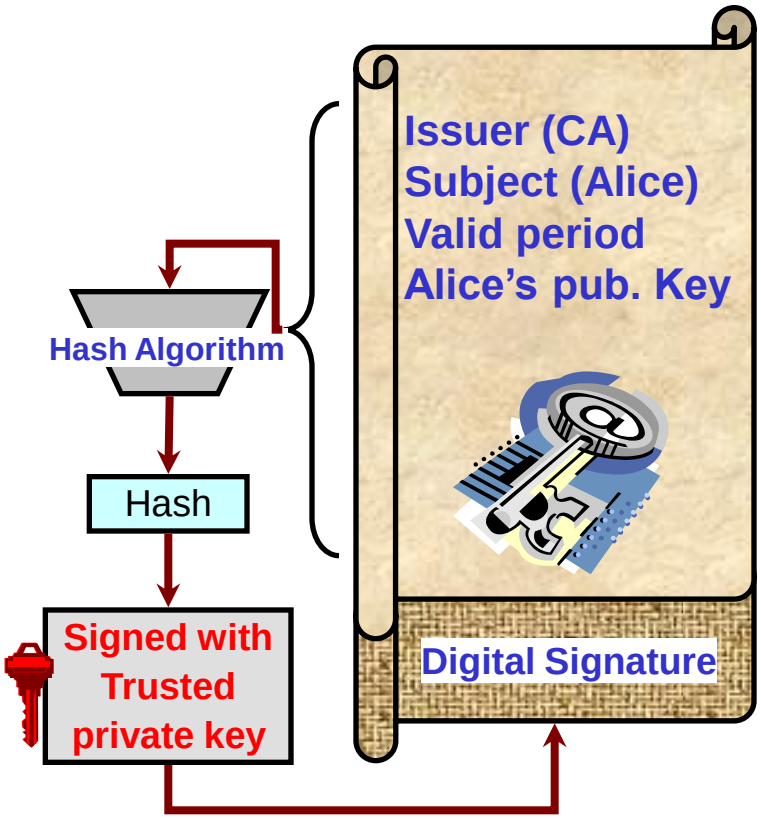
What is a Digital Certificate?

❖ **Digital Certificate**

- ✓ A file containing Identification information (CA's name (Issuer), Alice's name (Subject), valid period, Alice's public key, etc) and digital signature signed by trusted third party (CA) to guarantee its authenticity & integrity

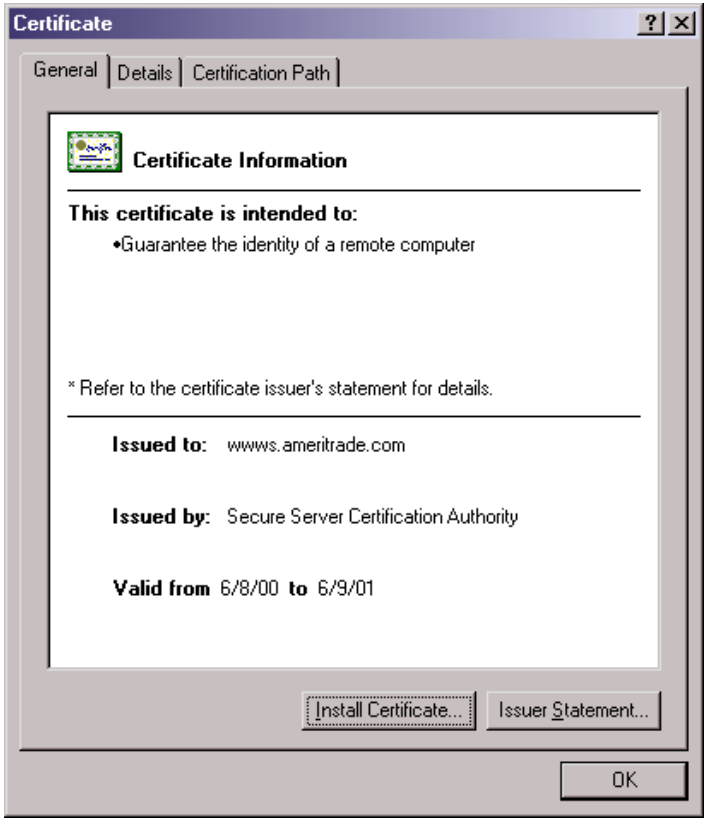
❖ **Certificate Authority (CA)**

- ✓ Trusted third party like a government for passports
- ✓ CA authenticates that the public key belongs to Alice
- ✓ CA creates Alice's a Digital Certificate



72

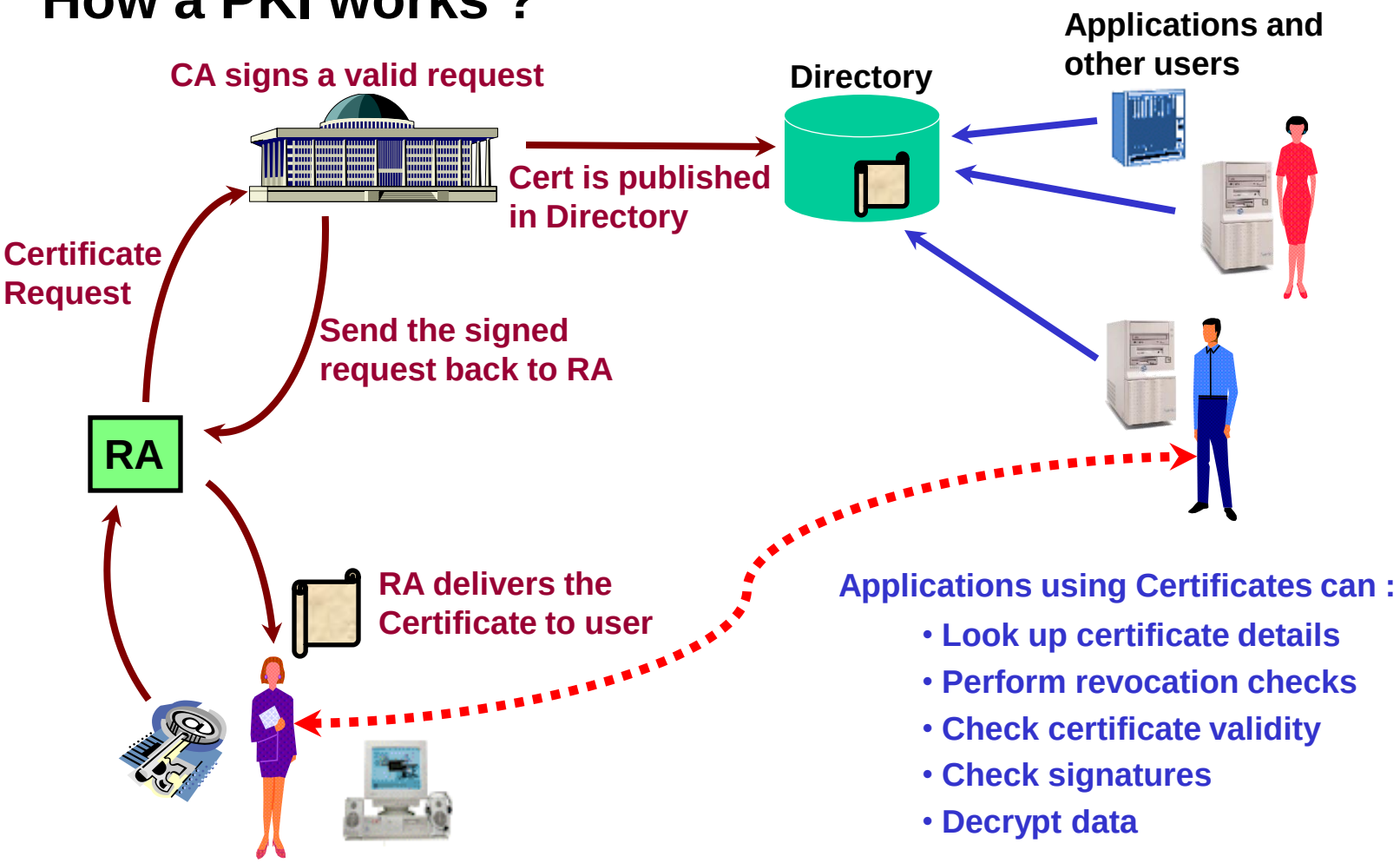
Certificate



Data encrypted using secret key exchanged using some public key associated with some certificate.

Public Key Infrastructure

How a PKI works ?

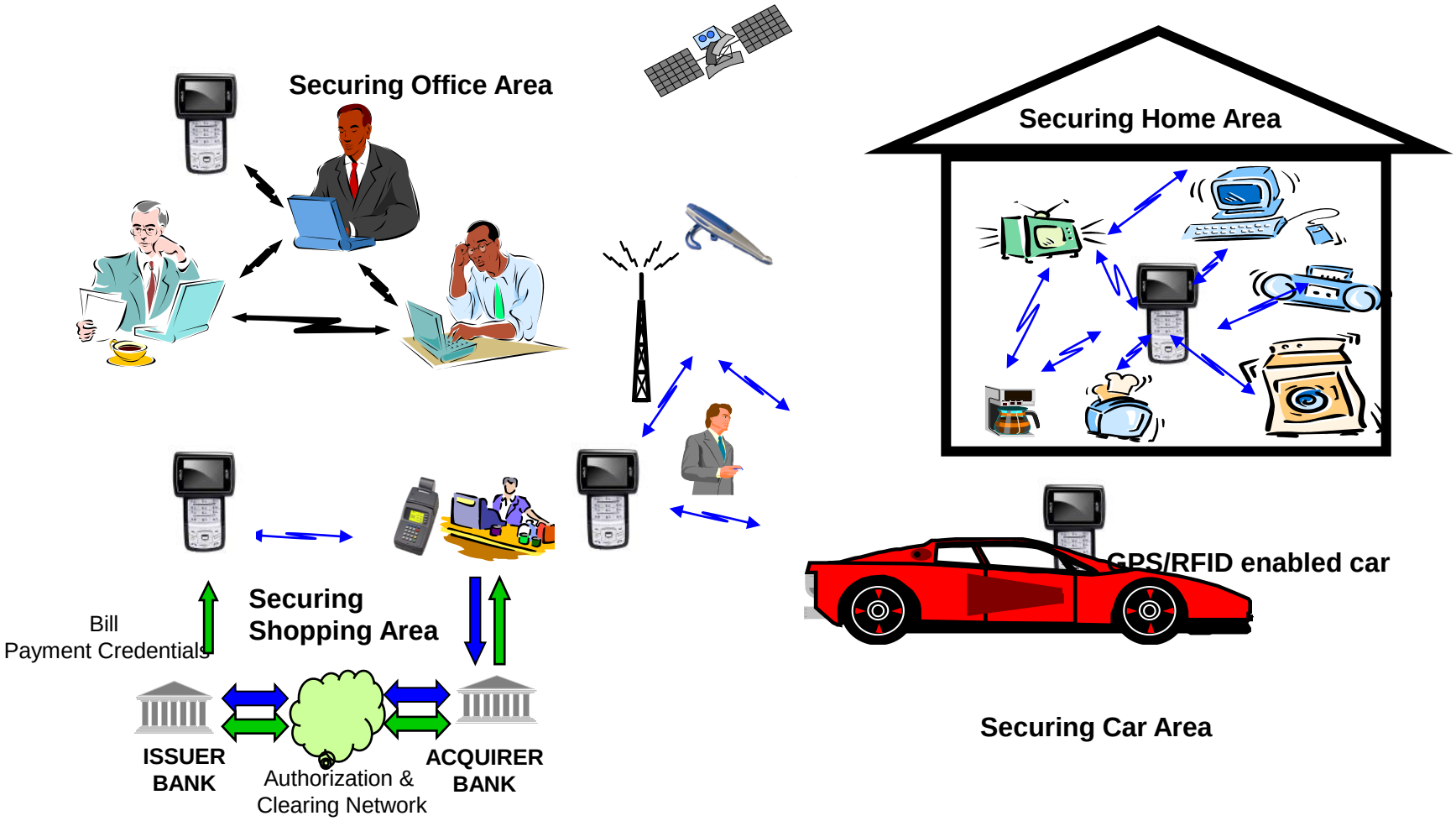


74

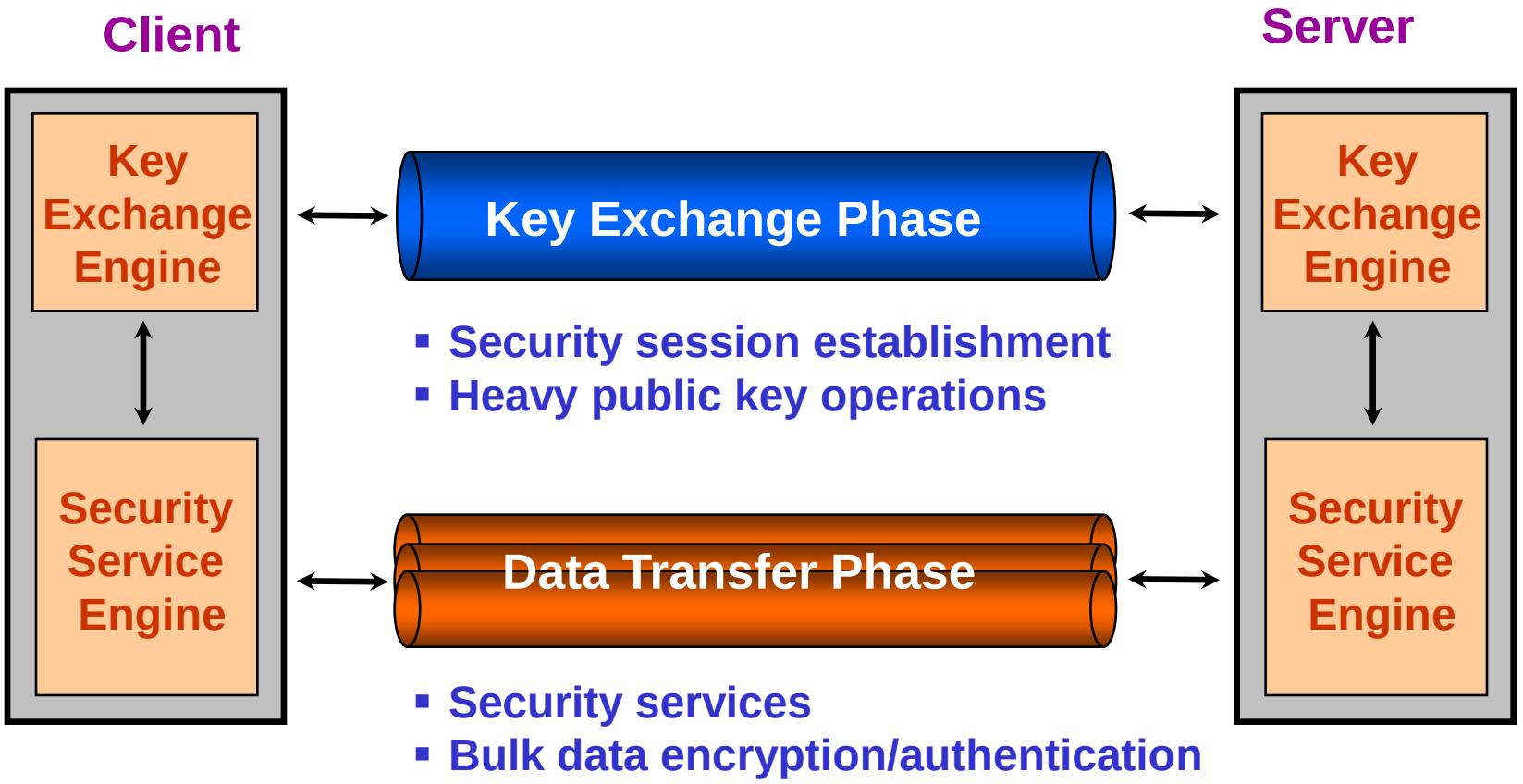
5. Communications Security

- VPN
- IPSec
- SSL/TLS

Lots of Non-F2F Communications

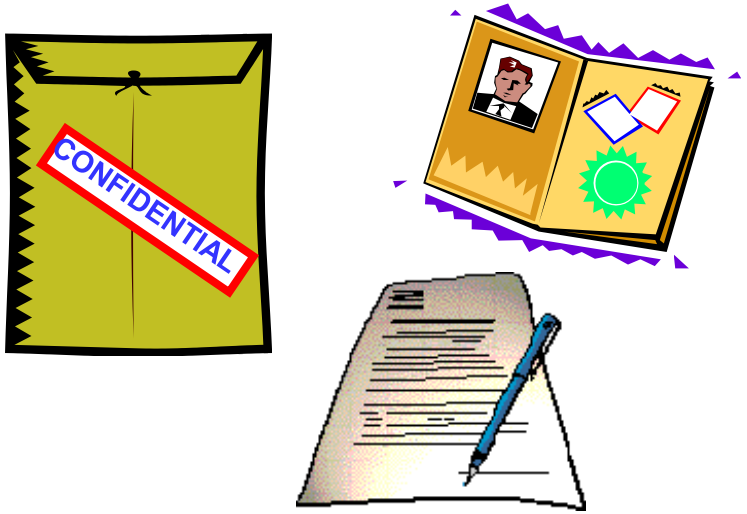


Communications Security Protocols



❖ Examples: IPSec, SSL/TLS/WTLS, SSH …

Solutions for Security Needs



Physical Solutions

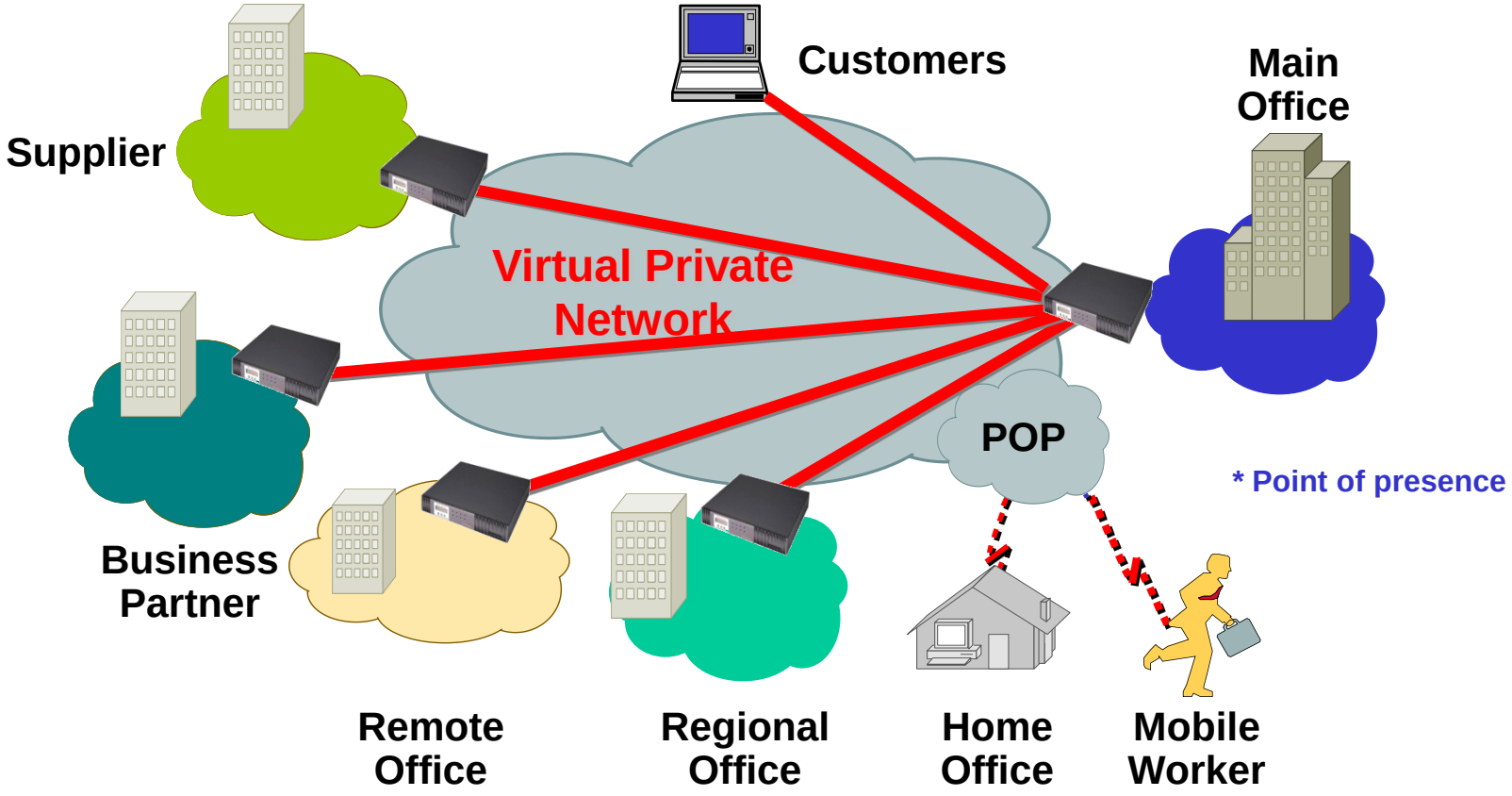
- Temper-evident sealed envelope
- ID-card, Passport, Drivers license
- Signature

Cryptographic Solutions (for communications over open network)

- Encryption with MAC : Confidentiality, Authentication, Integrity Protection
- Digital Certificate : Identification
- Digital Signature : Authentication, Integrity Protection, Non-Repudiation
- Security mechanisms are combined to provide a security service
  - ✓ Virtual Private Network(VPN), Firewall, IDS, etc.

Virtual Private Network (VPN)

Secure connectivity deployed on a shared communication infrastructure with the same security policies and performance as a private network

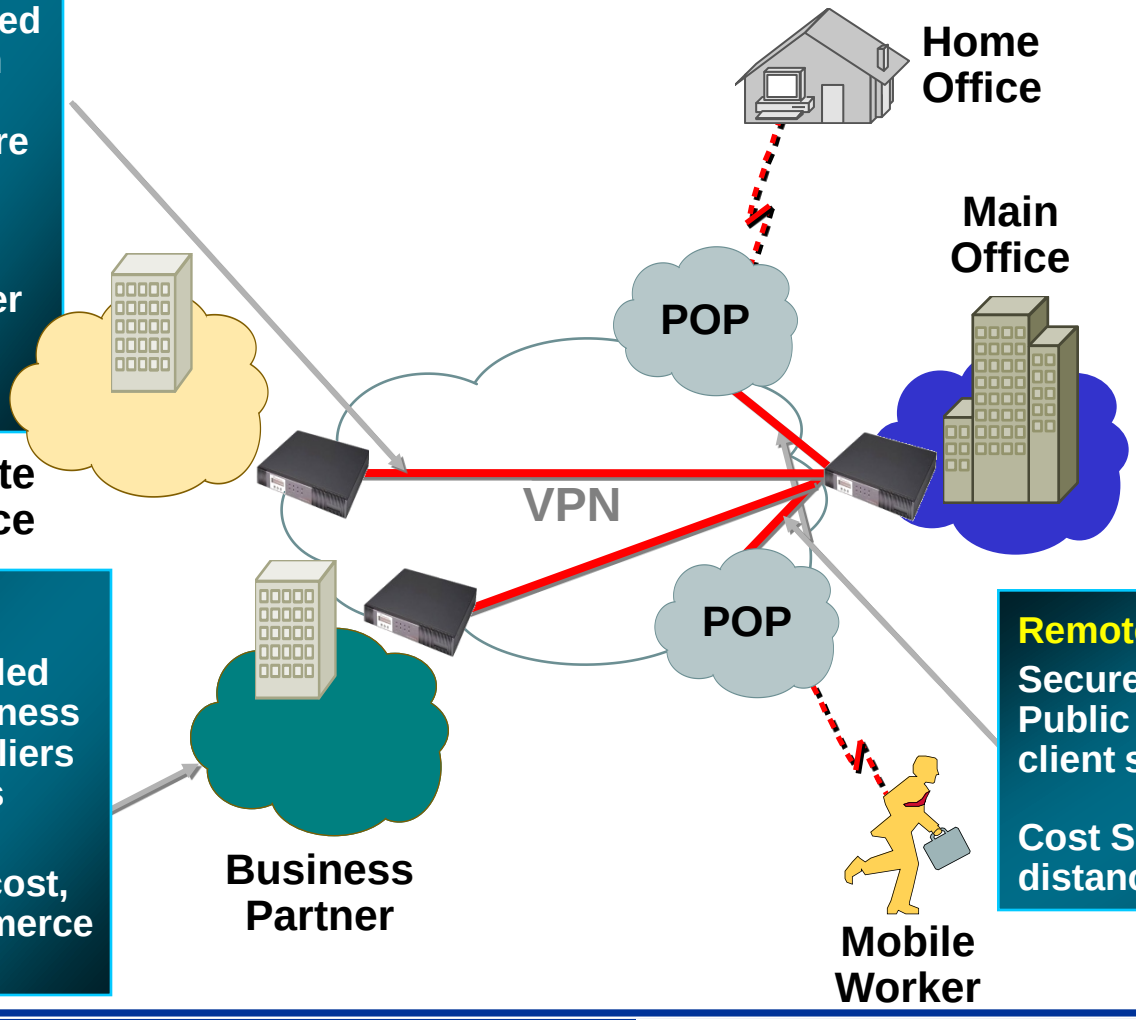


VPN Business Applications

Intranet VPN

Low Cost, tunneled connections with IPSec encryption and QoS to ensure security and reliability

Cost Savings over Frame Relay and Leased Lines



Extranet VPN

Allows controlled access to business partners, suppliers and customers

Provides low-cost, secure E-commerce infrastructure

Remote Access VPN

Secure tunnels across a Public Network with VPN client software

Cost Savings over long distance calls

VPN Benefits

- Build secure business infrastructure
  - Integrate dispersed business environments using secure, controlled connectivity over shared networks
  - Implement once for multiple applications
  - Centrally-controlled access policy
  - Enable multi-level, layered approach to security
- Use internet for remote access
  - Mobile users use internet accounts to gain access and tunnel to offices
- Create internal security
  - Protect sensitive internal traffic/systems from others
- Can also make private networks more private
- Can be used to back-up existing private networks

- VPN issues
  - Security
  - Quality of Service
  - Scalability / Reliability
  - Manageability

VPN Key Components

- **Tunneling**
  - PPTP, L2TP; MPLS; IPSEC, GRE, IP-in-IP; SSL/TLS
- **Security**
  - IPSEC vs. Virtual path(VC, PVC, LSP, etc.)
  - Encrypted tunnel vs. traffic separation
- **Access control**
  - Remote user authentication
  - Membership management
- **Policy Management**
  - Centralized policy control
  - Policy configuration, distribution & update
- **Quality of Service (QoS)**
  - Traffic classification, marking, policing & shaping
  - SLA: Latency, throughput, jitter, packet loss…
- **High Availability**
  - Transparent session fail-over
  - Load balancing, IP clustering

Generic Routing Encapsulation (GRE)
Multi-Protocol Label Switching (MPLS)
Quality of Service (QoS)
Service Level Agreements (SLA)
Point-to-Point Tunneling Protocol (PPTP)
Layer 2 Tunneling Protocol (L2TP)
Secure Socket Layer (SSL)
Internet Protocol Security (IPSEC)
Virtual Circuit (VC)
Permanent Virtual Circuit (PVC)
Label Switched Path (LSP)

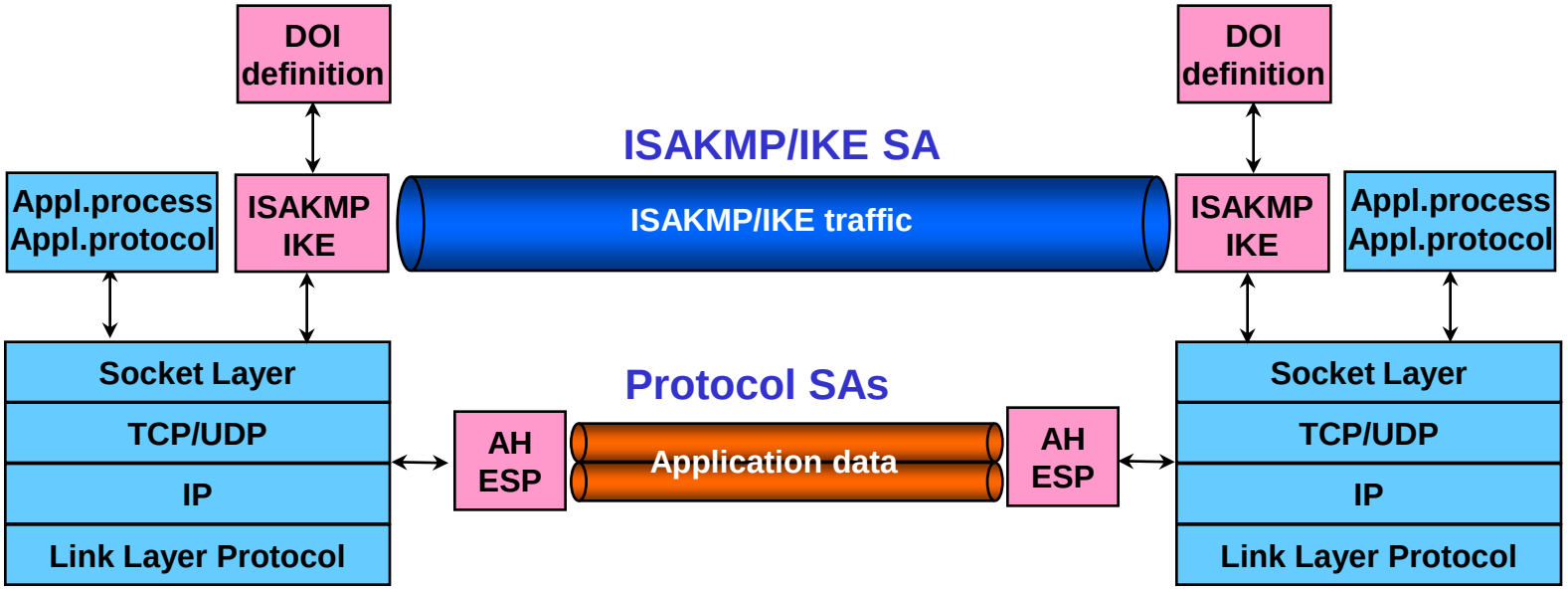
IPSec: IP-layer Security Protocol

- **Two Security Protocols**
  - **AH primarily for authentication and optional anti-replay service**
    - ✓ **Mandatory-to-implement algorithms: HMAC-MD5, HMAC-SHA1**
  - **ESP primarily for confidentiality and optionally AH functionality (with limited protection range)**
    - ✓ **Mandatory-to-implement algorithms:**
      - **DES-CBC (de facto: 3DES-CBC), NULL Encryption algorithm**
      - **HMAC-MD5, HMAC-SHA1, NULL Authentication algorithm**
  - **AH & ESP are vehicles for access control**

- **Key Management**
  - **ISAKMP defines procedures and payload formats for security association (SA) / key management**
  - **Default automated SA/key management protocol for IPSEC:**
    - **IKE (Internet Key Exchange) under IPSEC DOI**

- **Two Modes of Operations**
  - **Transport mode protects primarily upper layer protocols**
  - **Tunnel mode protects primarily tunneled IP packets**

Operations of IPSec



Phase I (ISAKMP SA) : SA negotiation between two ISAKMP servers

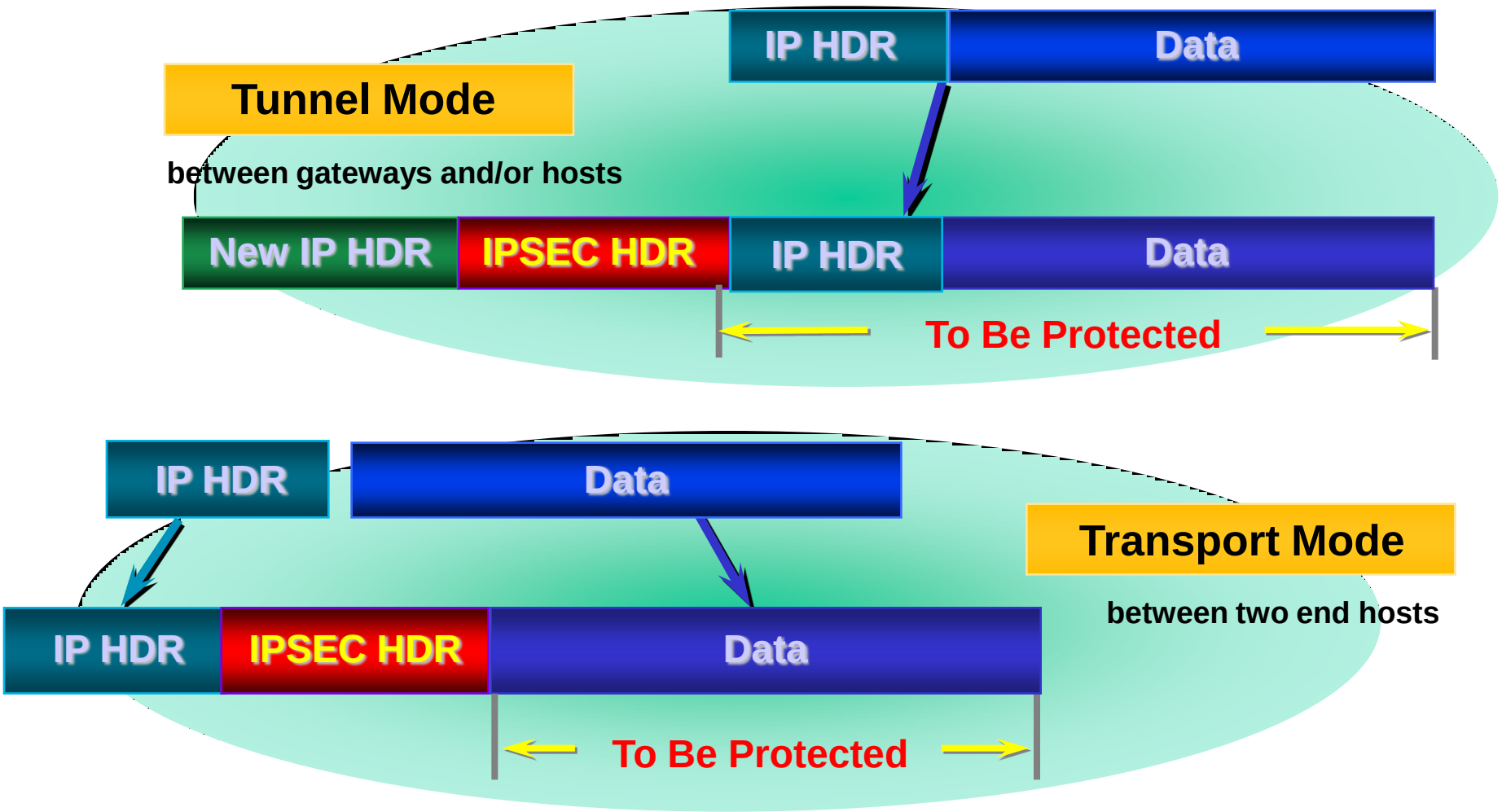
Phase II (Protocol SA) : SA negotiation for other security protocols (e.g., IPSEC AH) under the protection of ISAKMP SA

Security Association (SA) & SPI

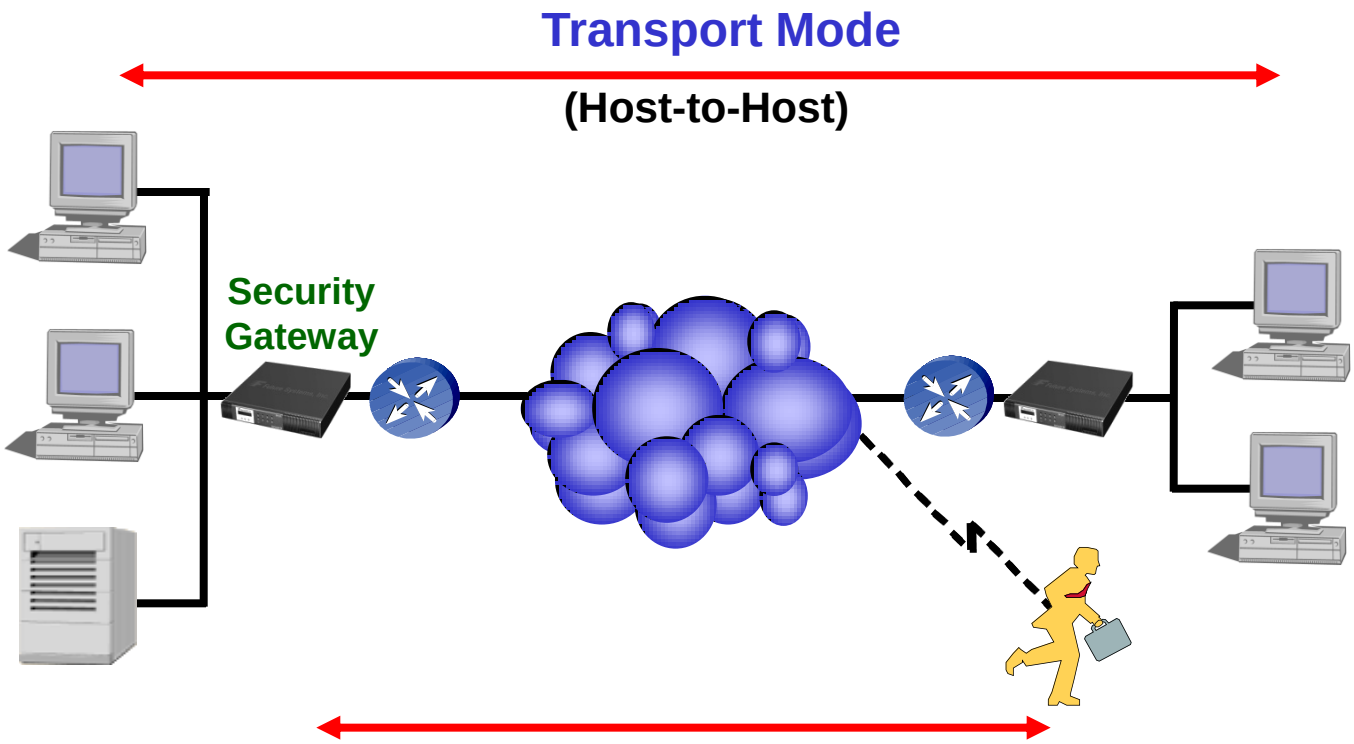
- **Security Association (SA)**
  - A set of security parameters that completely defines the security services and mechanisms to be provided by the security protocol (IKE, AH or ESP).
  - E.g., authentication/encryption algorithm, algorithm mode and secret keys, etc.
  - uniquely identified by a triple (SPI, Destination IP addr., Security protocol).
  - receiver-oriented: the SPI is selected by the destination.
  - ISAKMP/IKE SA : bidirectional (identified by a pair of (I-Cookie, R-Cookie))
  - Protocol SA : unidirectional - one for inbound and one for outbound.

- **Security Parameters Index (SPI)**
  - An identifier for a SA relative to some security protocol (IPSEC: 32 bits)
  - Each security protocol has its own “SPI-space”, and Initiator and Responder each select and exchange their own SPI during the security protocol negotiation.

IPSec Mode of Operations



Transport Mode vs. Tunnel Mode

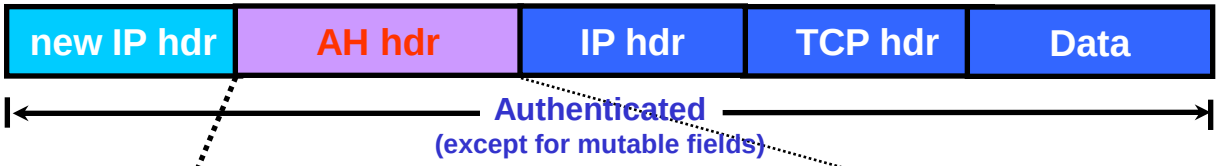


Authentication Header(AH)

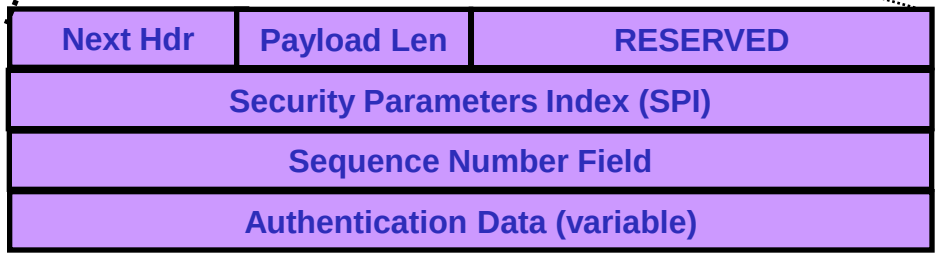
Original IP Packet

AH Transport Mode Protected Packet

AH Tunnel Mode Protected Packet

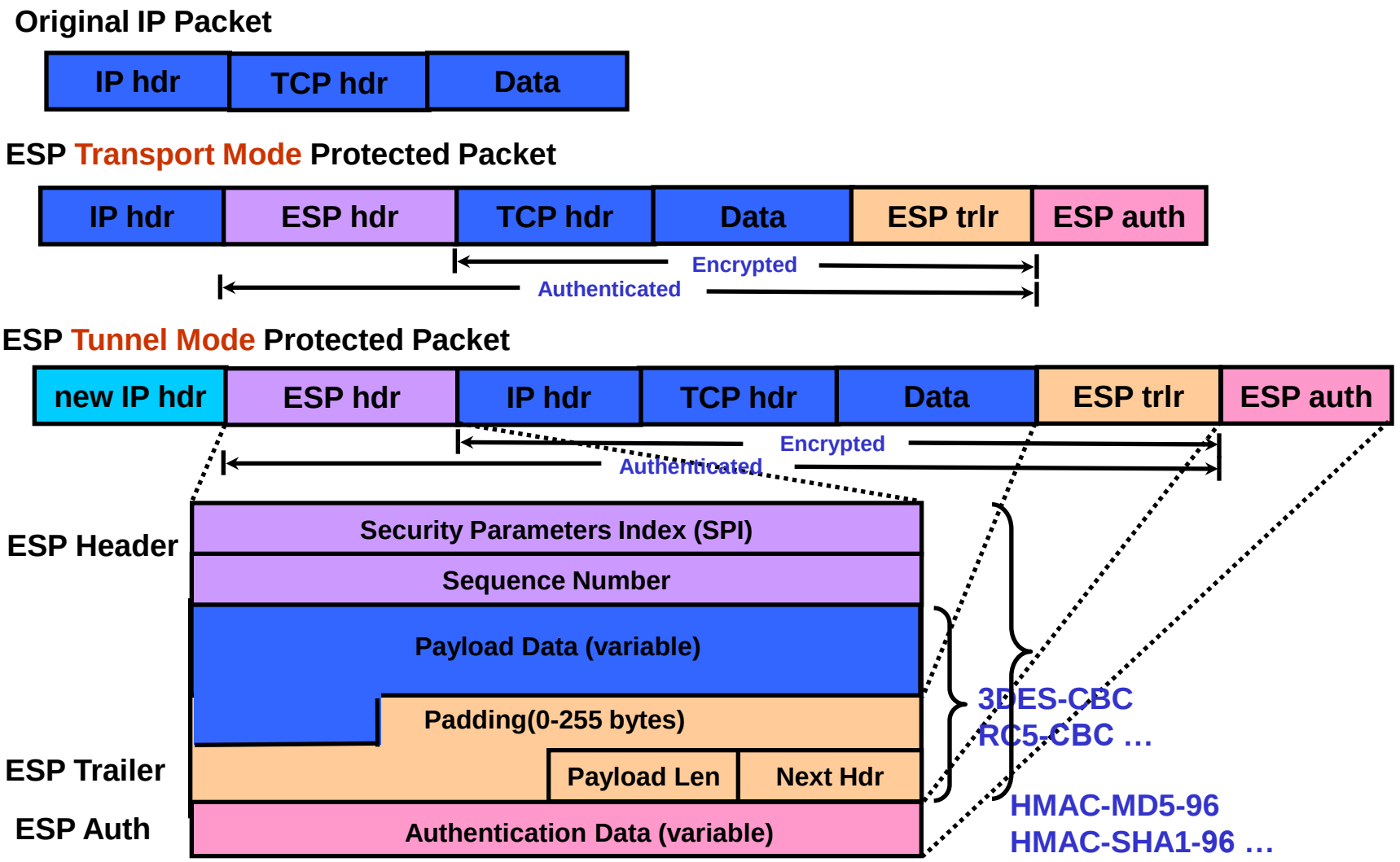


AH Header



HMAC-MD5-96
HMAC-SHA1-96

Encapsulating Security Payload(ESP)

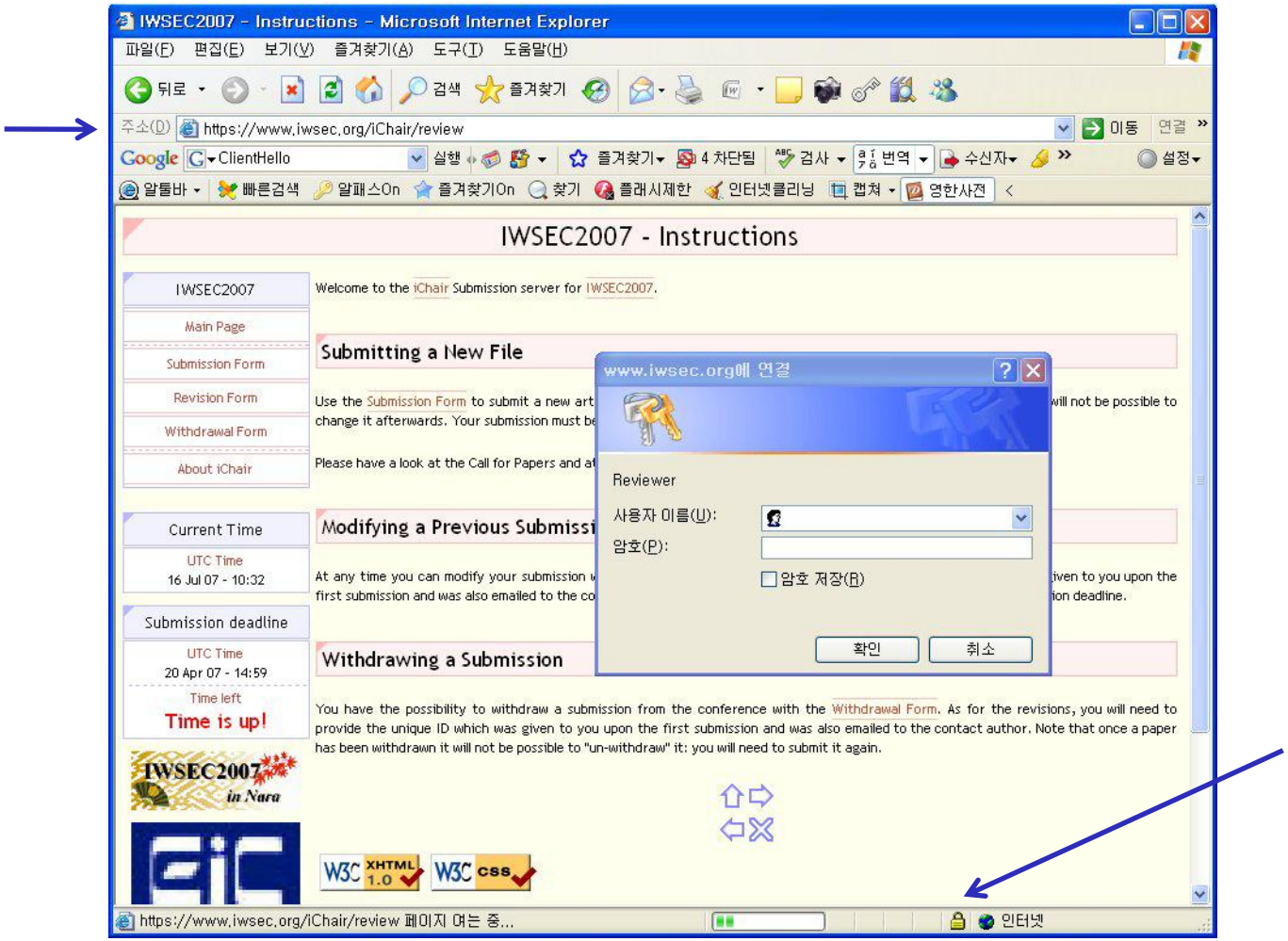


ISAKMP & IKE

- **ISAKMP:**
  - **A general framework for establishing and managing SAs and keys**
  - **Header and payload definitions**
  - **Exchanges types for payload exchanges**
  - **General processing guidelines**

- **IKE:**
  - **A hybrid protocol to negotiate keys and SAs in an authenticated and protected manner**
  - **An authenticated key exchange algorithm based on Diffie-Hellman, with added authentication and security features from Oakley and SKEME techniques**
  - **Authentication methods supported**
    - **Pre-shared secret**
    - **Digital signature**
    - **Public key encryption**
  - **Exchange types defined**
    - **Aggressive mode**
    - **Main mode**

TLS: Transport Layer Security

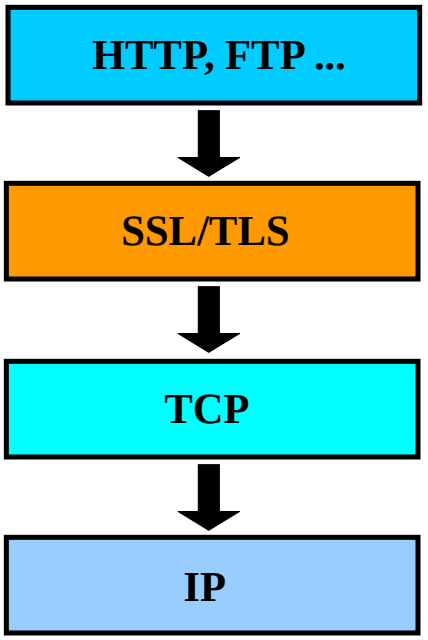


Secure Sockets Layer (SSL)

- Transport layer security to any TCP-based app. using SSL services.
  - used between Web browsers and Web servers for e-commerce (https).
- Security services:
  - server authentication
  - data encryption
  - client authentication (optional)
- Server authentication:
  - SSL-enabled browser includes public keys for trusted CAs.
  - Browser requests server certificate, issued by trusted CA.
  - Browser uses CA′s public key to extract server′s public key from certificate.

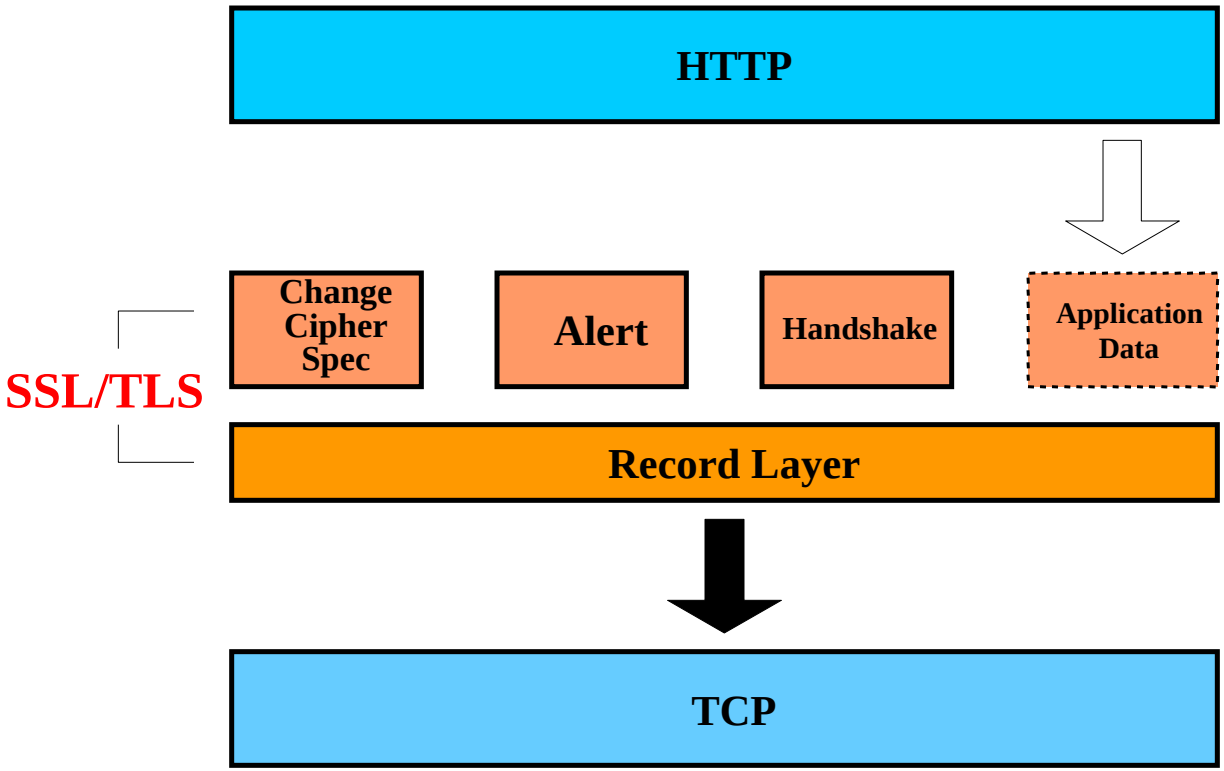
Transport Layer Security (TLS) Protocol

- **SSL/TLS**
  - Layered on top of reliable transport protocols, e.g., TCP
  - Application protocol independent
  - Record Protocol & Handshake Protocol
- **Record Protocol**
  - Encapsulation of higher level protocols
  - Data encryption using CBC block ciphers or stream ciphers
  - Data integrity using HMAC
- **Handshake Protocol**
  - Security parameter negotiation: keys & algorithms
  - Entity authentication using public key cryptography (RSA, DSS; static DH)
  - Key exchange & verification (RSA key transport, DH key exchange)

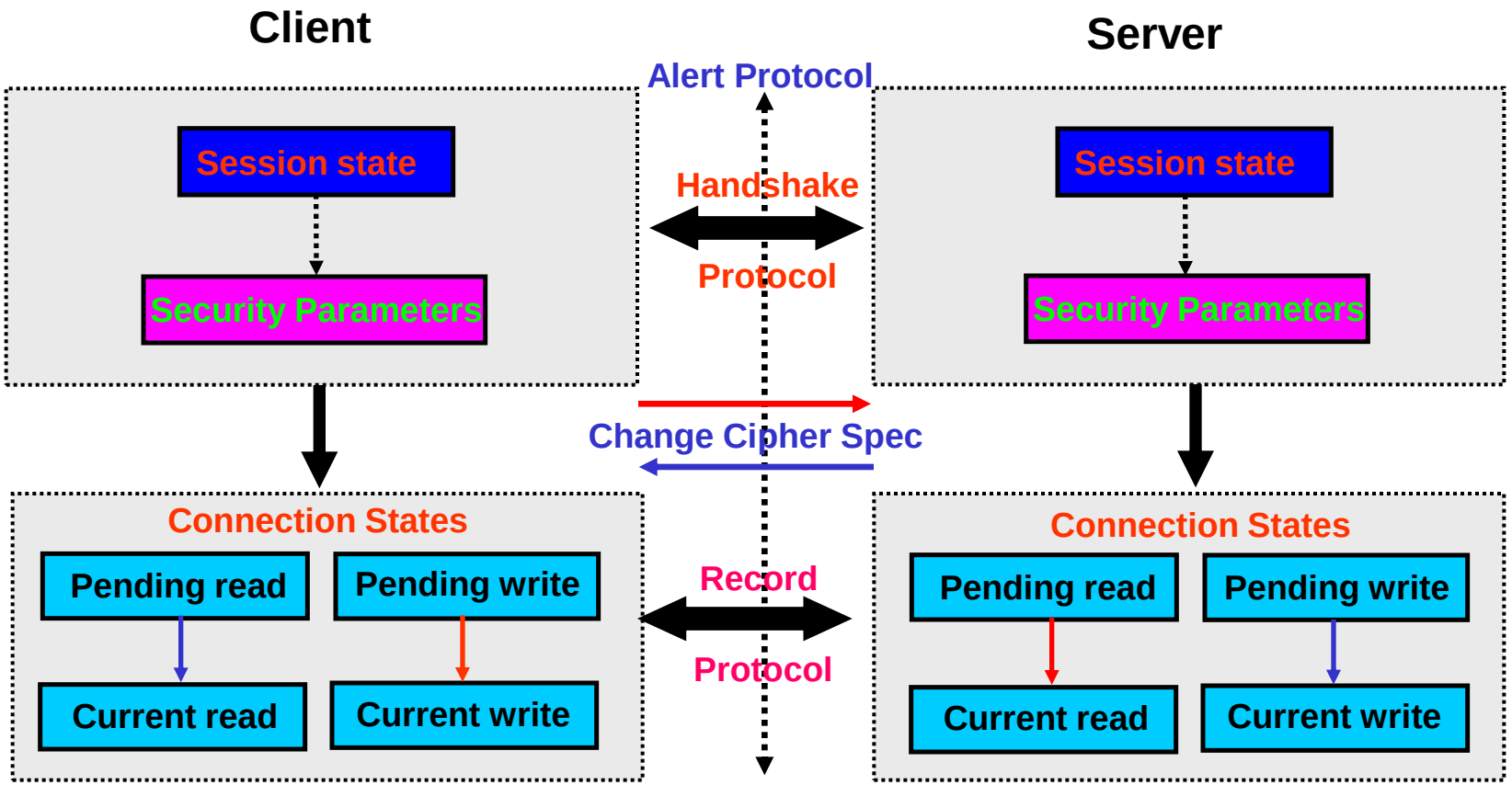


5 bytes

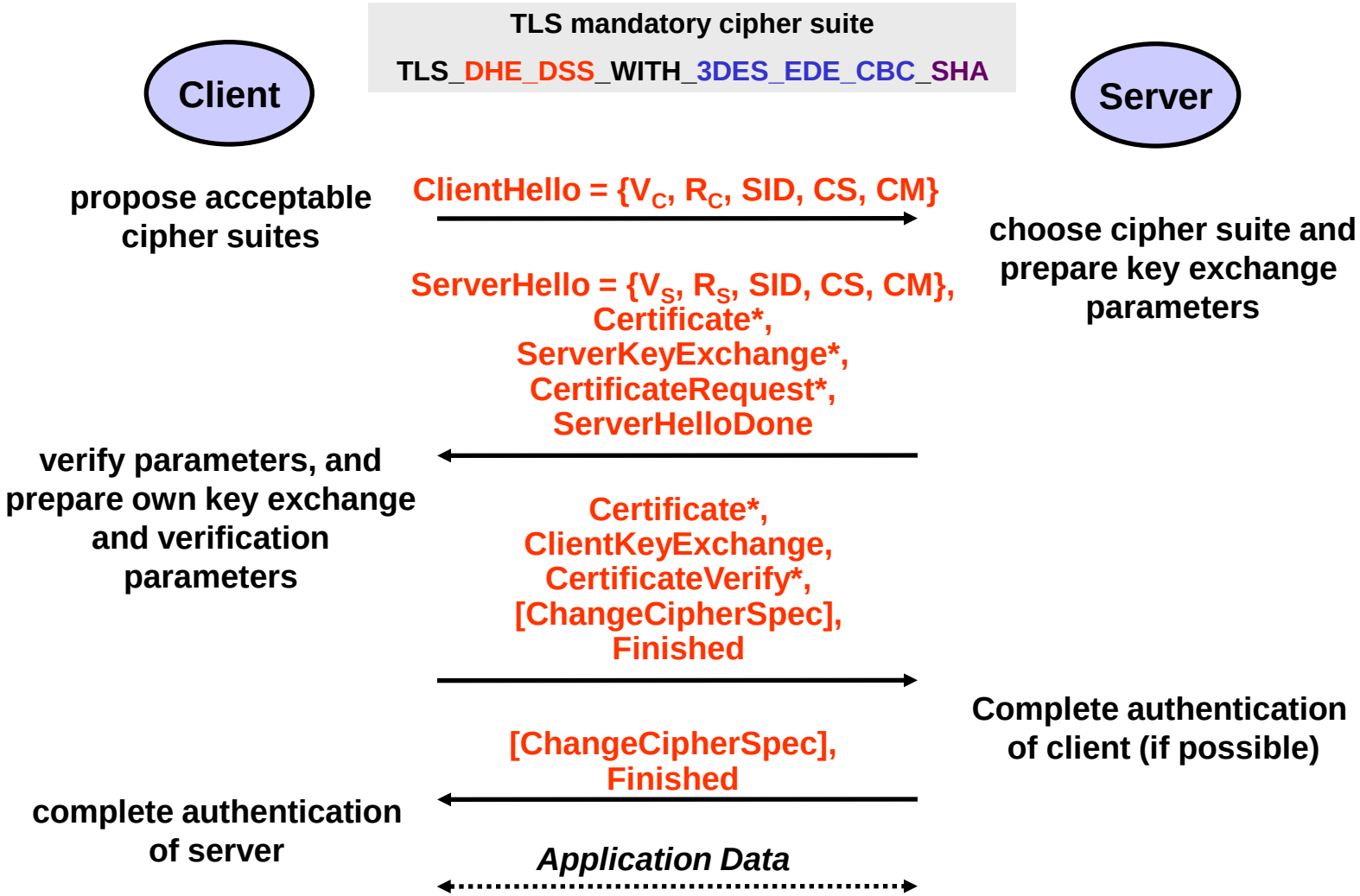
SSL/TLS Layering



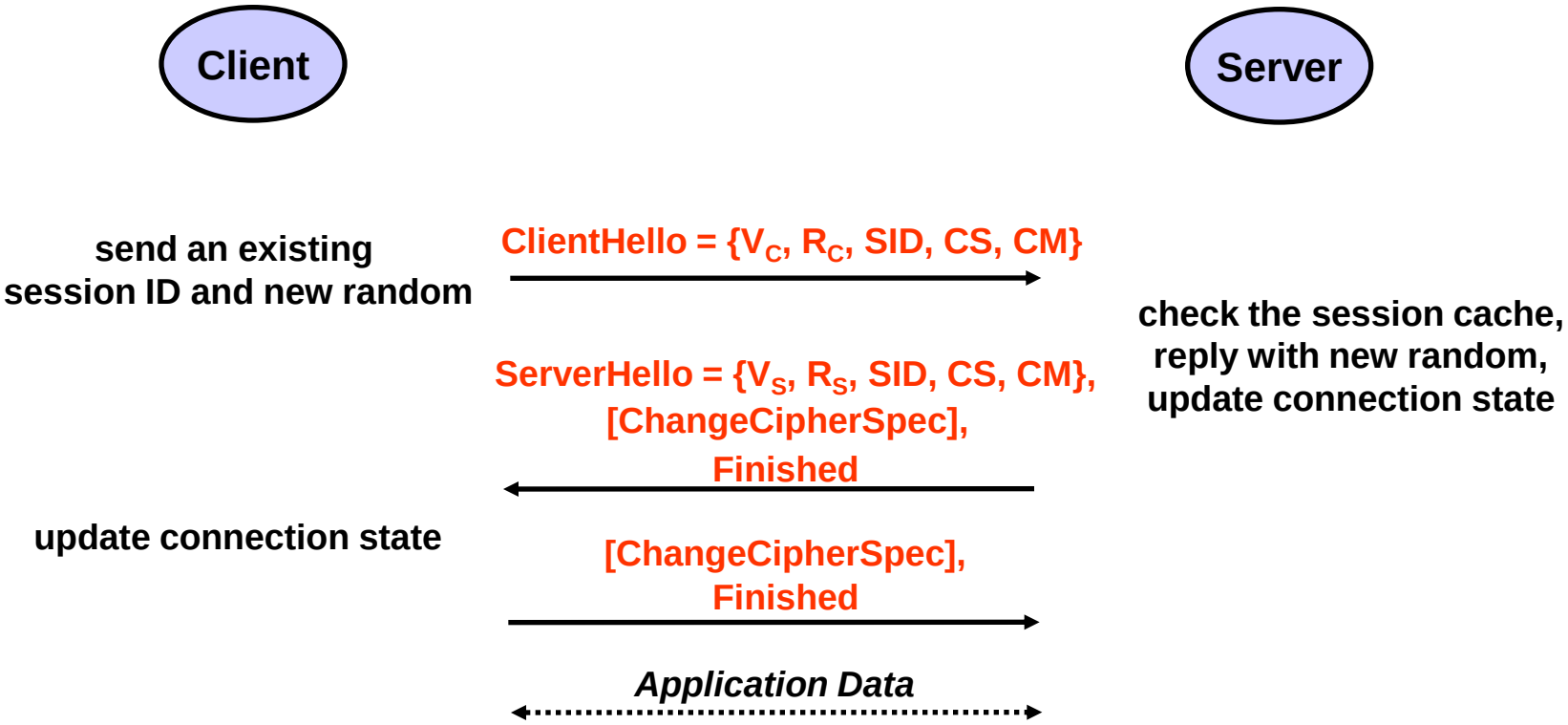
SSL/TLS Operations Overview



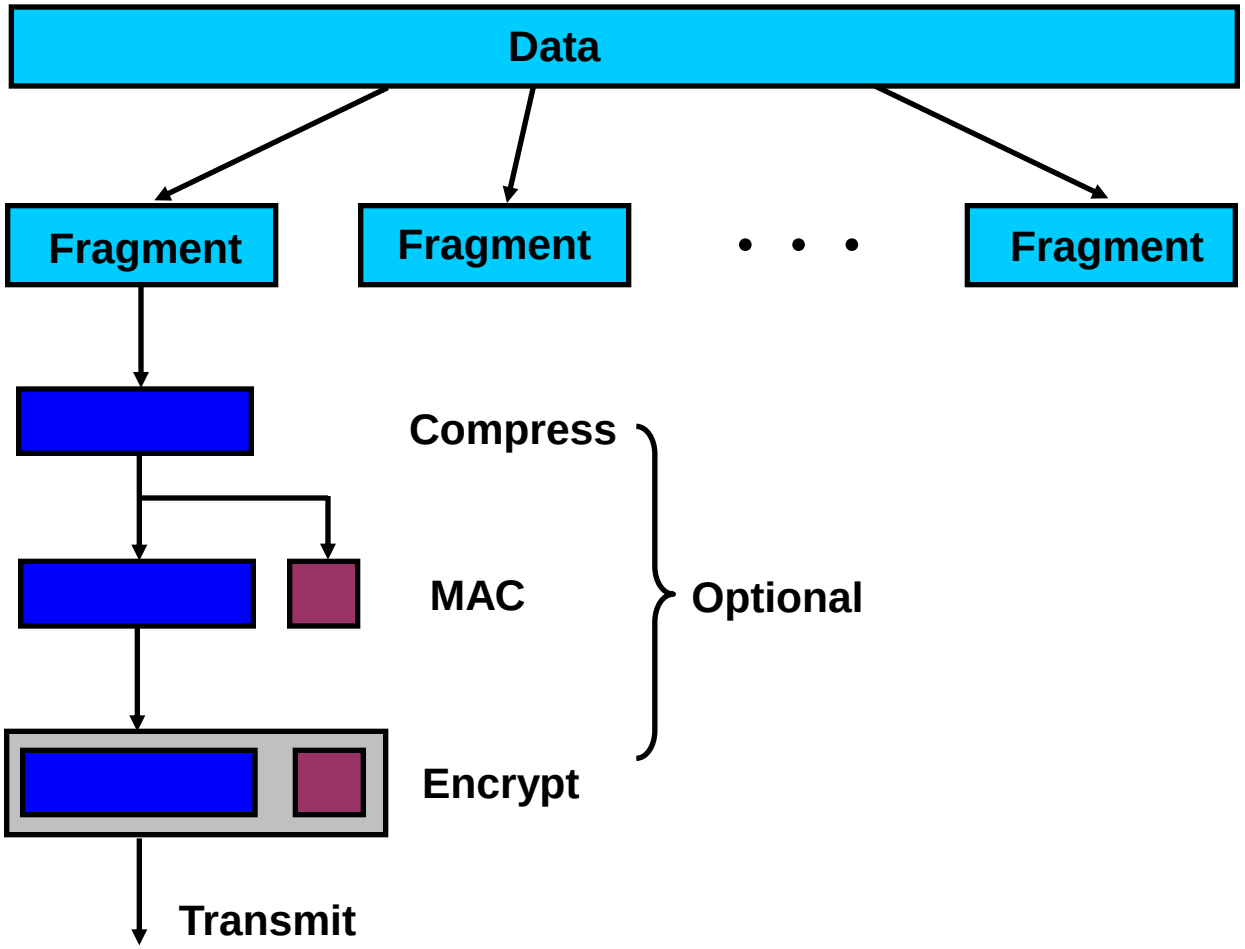
TLS Full Handshake



TLS Abbreviated Handshake



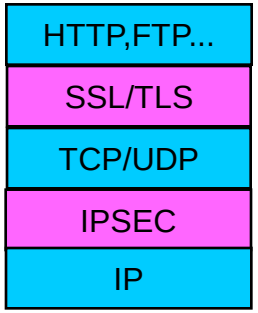
TLS Record Protocol



IPSec vs. SSL/TLS

IPSec

- Network layer security protocol
- Confidentiality, Integrity, Authentication, Access control, Auditing
- Transport protocol independent
- No change to applications (application/user transparency)
- Peer-to-Peer model: Host-to-Server, Host-to-Subnet, Subnet-to-Subnet
- More secure; too complex, special client SW
- IPv4 (optional), IPv6 (mandatory)

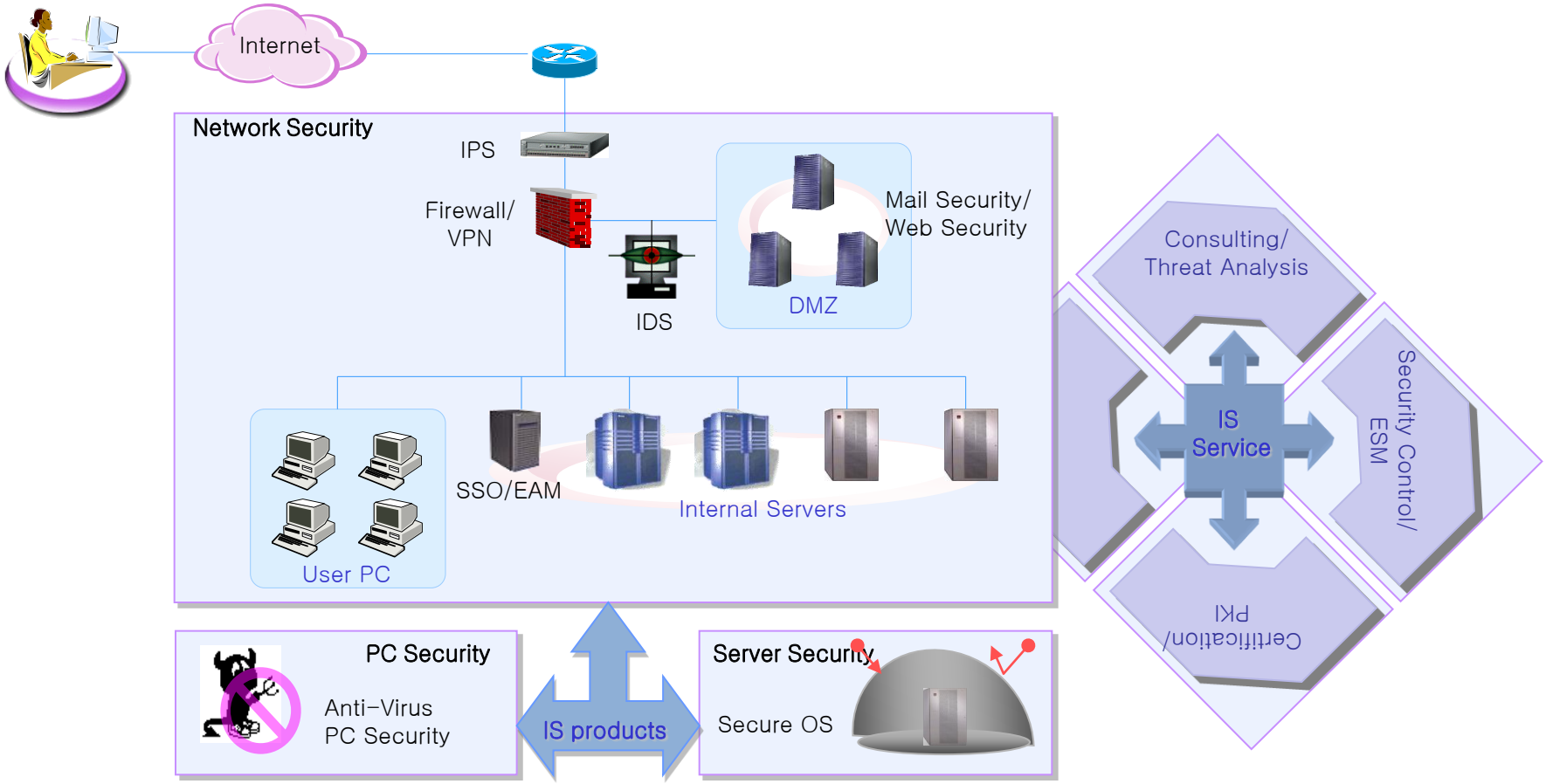


SSL/TLS

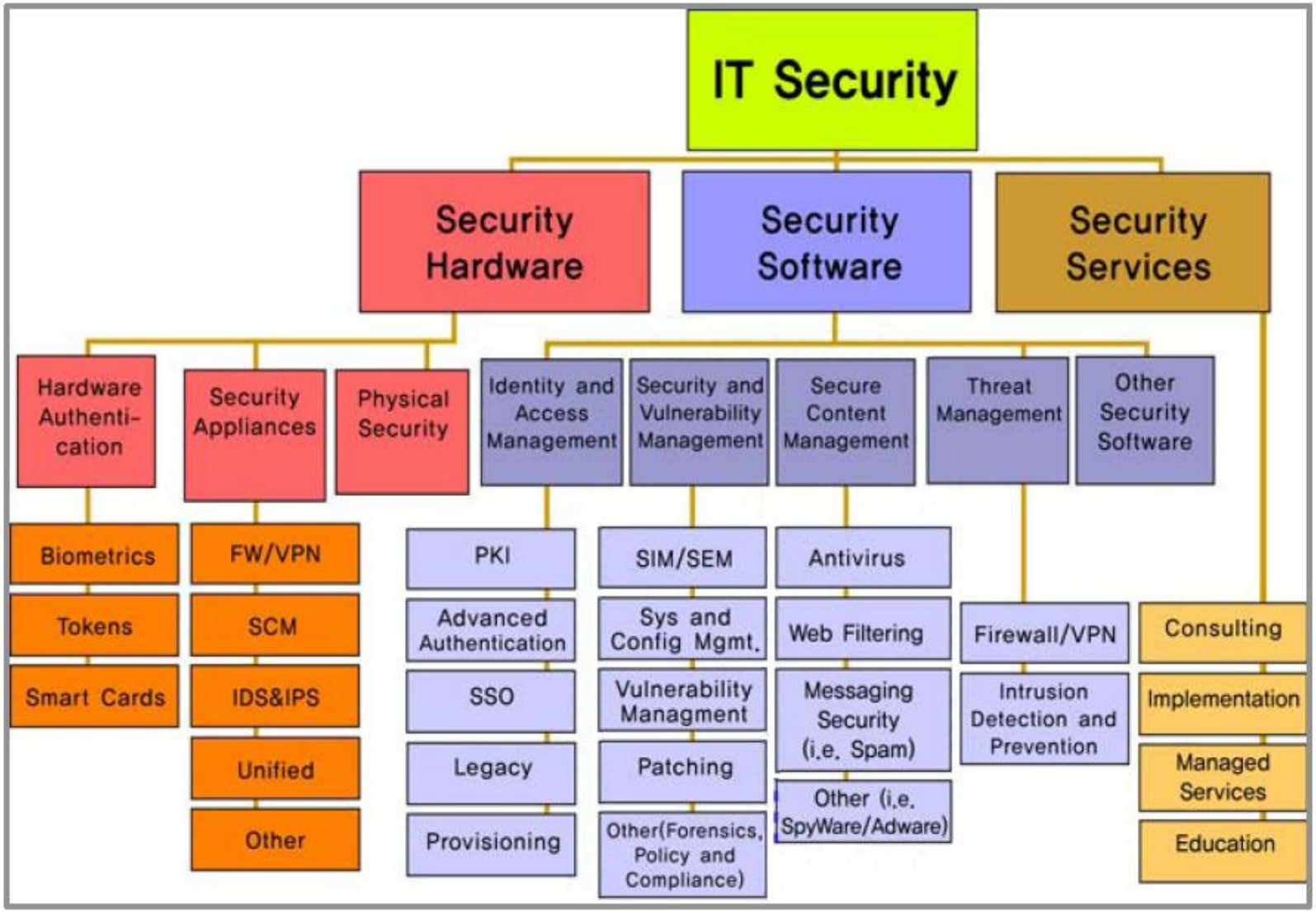
- Transport layer security protocol
- Confidentiality, Integrity, Authentication (usually client-to-server only)
- Works only with TCP (not UDP): HTTP, SMTP, POP3, NNTP, FTP, LDAP…
- Minimal changes to applications
- Client-Server model: Host-to-Server (secure Web transactions)
- Free : built in to nearly all browsers and Web servers

6. Security Management

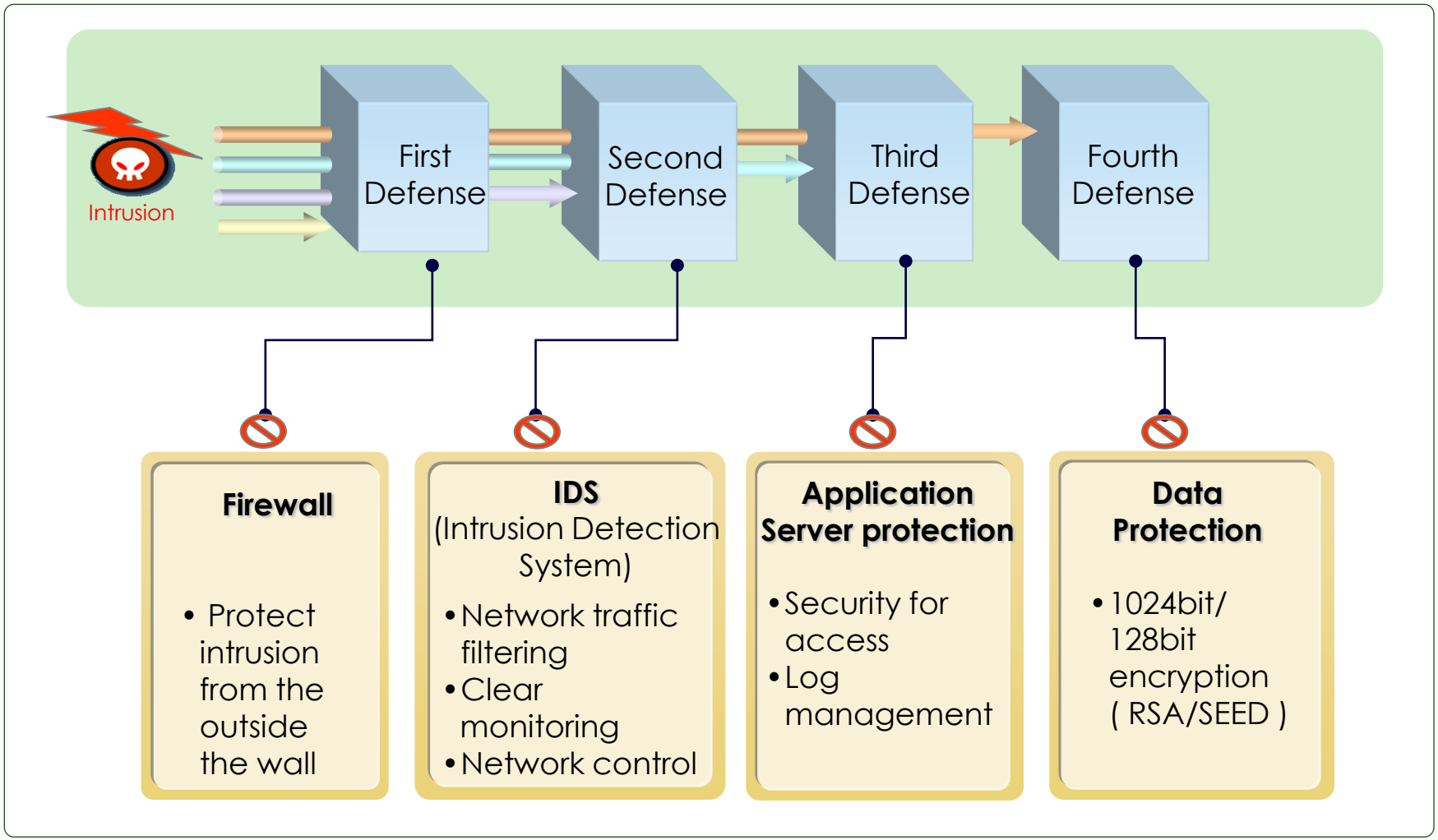
Corporate Information Security



Information Security Industry



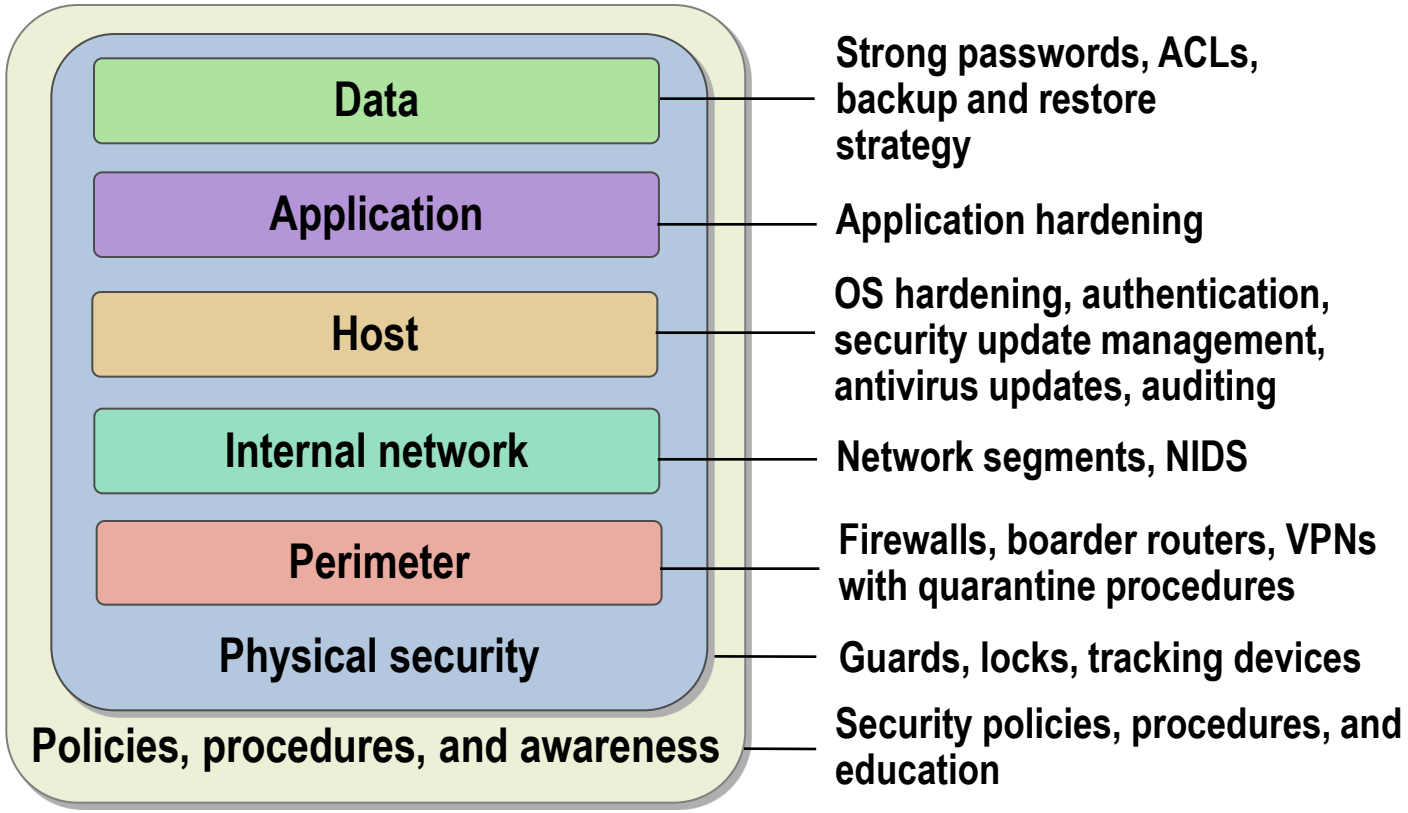
Simplified Security Diagram



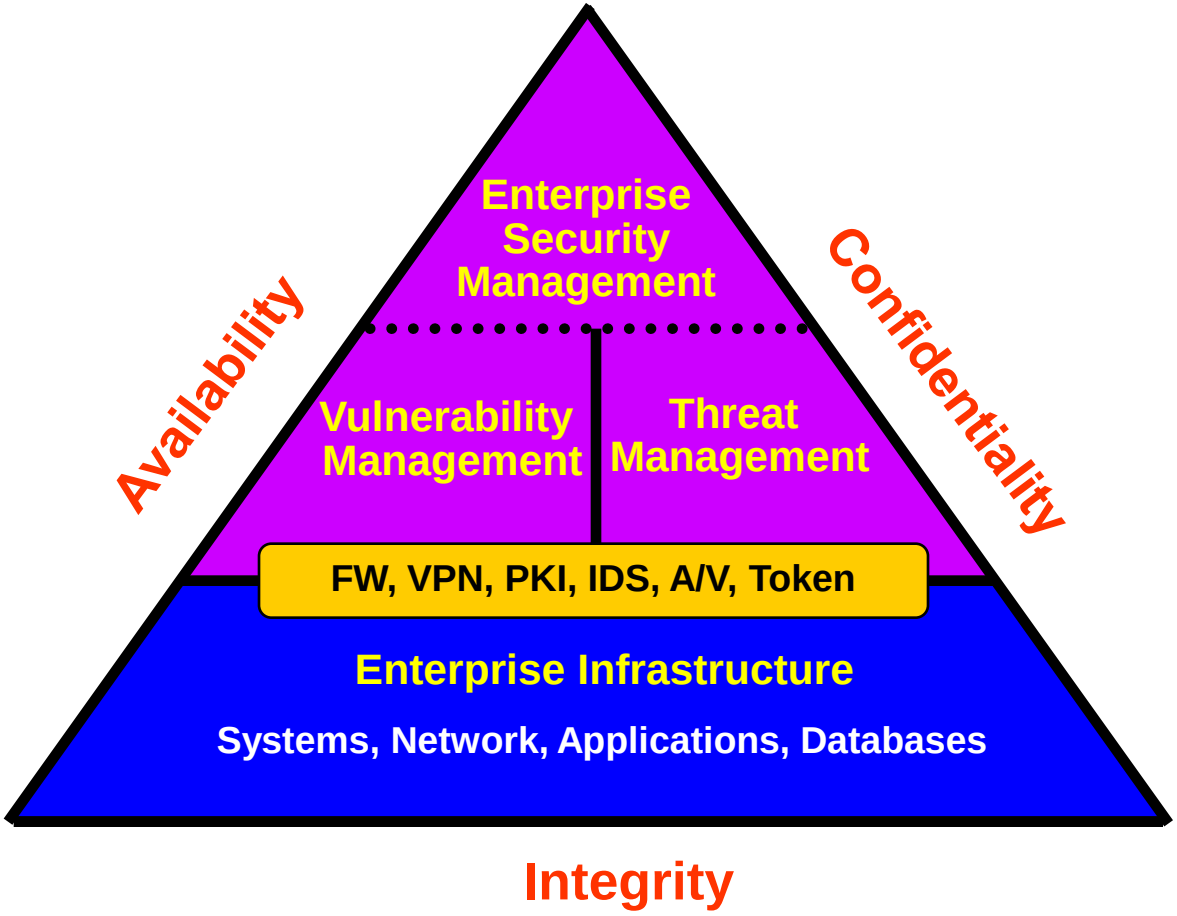
Understanding Defense-in-Depth

Using a layered approach:

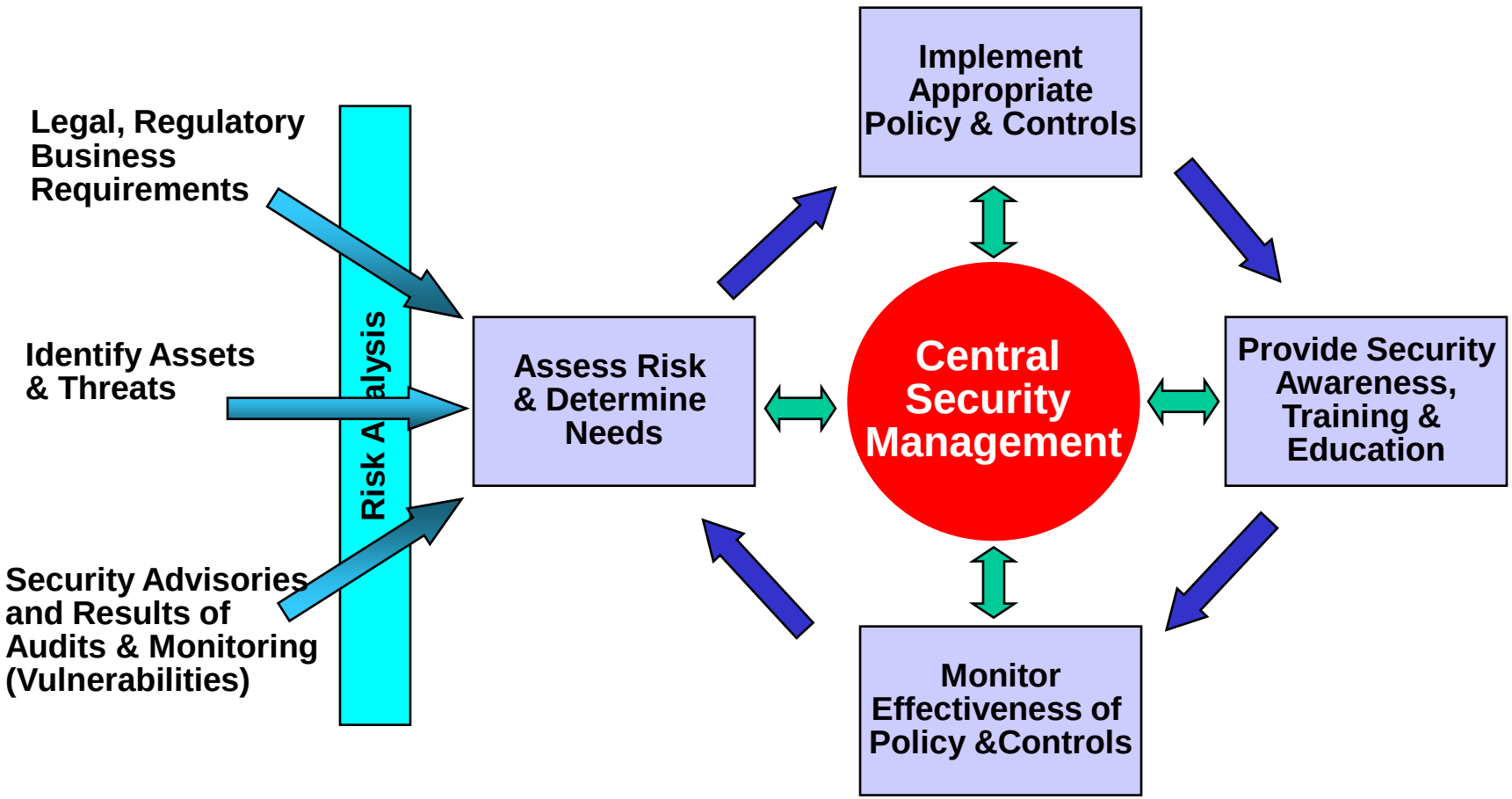
- Increases an attacker's risk of detection
- Reduces an attacker's chance of success



Enterprise Security Management



Managing Security



Security Plan

1. Describe the assets you want to protect
   - data
   - hardware and software
   - services
2. Describe how you will protect the assets
   - access restrictions and authentication
   - redundancy
   - Encryption
3. Describe disaster recovery plans
   - physical disasters
   - equipment failures
   - intrusions
   - employee or customer mistakes
4. Regularly test your security plan
5. Update plan based on results of testing

Penetration Testing for Intrusive Attacks

- **Intrusive attack:** Performing specific tasks that result in a compromise of system information, stability, or availability

- **Examples of penetration testing for intrusive attack methods include:**
  - Automated vulnerability scanning
  - Password attacks
  - Denial-of-service attacks
  - Application and database attacks
  - Network sniffing

Network Vulnerability Scanning

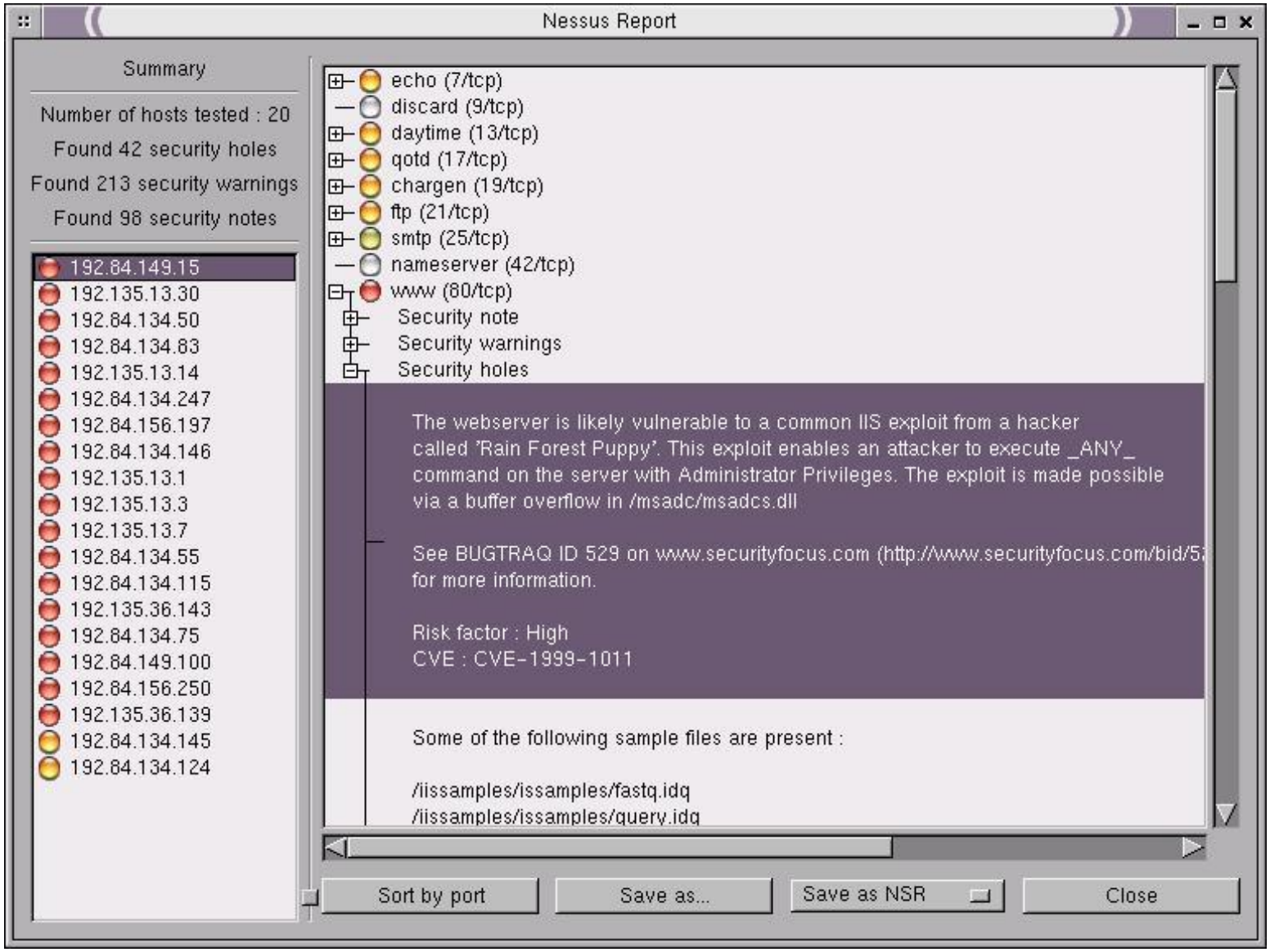
- Nmap: *insecure.org/nmap*

  - Nmap (“network mapper”) is designed to rapidly scan networks to determine what hosts and services are currently available.

- Nessus: *www.nessus.org*

  - Nessus, voted the #1 Network Security tool is a comprehensive network vulnerability scanner used in more then 75,000 organizations world-wide.

Nessus


Nessus Report
Summary
Number of hosts tested : 20
Found 42 security holes
Found 213 security warnings
Found 98 security notes
192.84.149.15
192.135.13.30
192.84.134.50
192.84.134.83
192.135.13.14
192.84.134.247
192.84.156.197
192.84.134.146
192.135.13.1
192.135.13.3
192.135.13.7
192.84.134.55
192.84.134.115
192.135.36.143
192.84.134.75
192.84.149.100
192.84.156.250
192.135.36.139
192.84.134.145
192.84.134.124
echo (7/tcp)
discard (9/tcp)
daytime (13/tcp)
qotd (17/tcp)
chargen (19/tcp)
ftp (21/tcp)
smtp (25/tcp)
nameserver (42/tcp)
www (80/tcp)
Security note
Security warnings
Security holes
The webserver is likely vulnerable to a common IIS exploit from a hacker called 'Rain Forest Puppy'. This exploit enables an attacker to execute _ANY_ command on the server with Administrator Privileges. The exploit is made possible via a buffer overflow in /msadc/msadcs.dll
See BUGTRAQ ID 529 on www.securityfocus.com (http://www.securityfocus.com/bid/5
for more information.
Risk factor : High
CVE : CVE-1999-1011
Some of the following sample files are present :
/iissamples/issamples/fastq.idq
/iissamples/issamples/query.idq
Sort by port
Save as...
Save as NSR
Close

Security Guideline for General Users

- Use automatic OS patch
- Use Anti-virus, Anti-Spyware
- Use secure password, change password periodically
- Use passwords for booting, Windows login, shared folder, screen saver, etc
- Use authentic software, not illegal software
- Do not open uncertain emails, suspicious attachments
- Backup important data
- Switch-off computer when it is not used
- Utilize useful tools

Useful Tools

- Anti-Viruses
- PC firewalls
- Preventing access to harmful websites
- Spam mail protection
- Phishing filter
- Keyboard protection programs
- Process explorer
- Autoruns

7. Applications Security

- E-commerce in Korea

Brief overview of online statistics in Korea

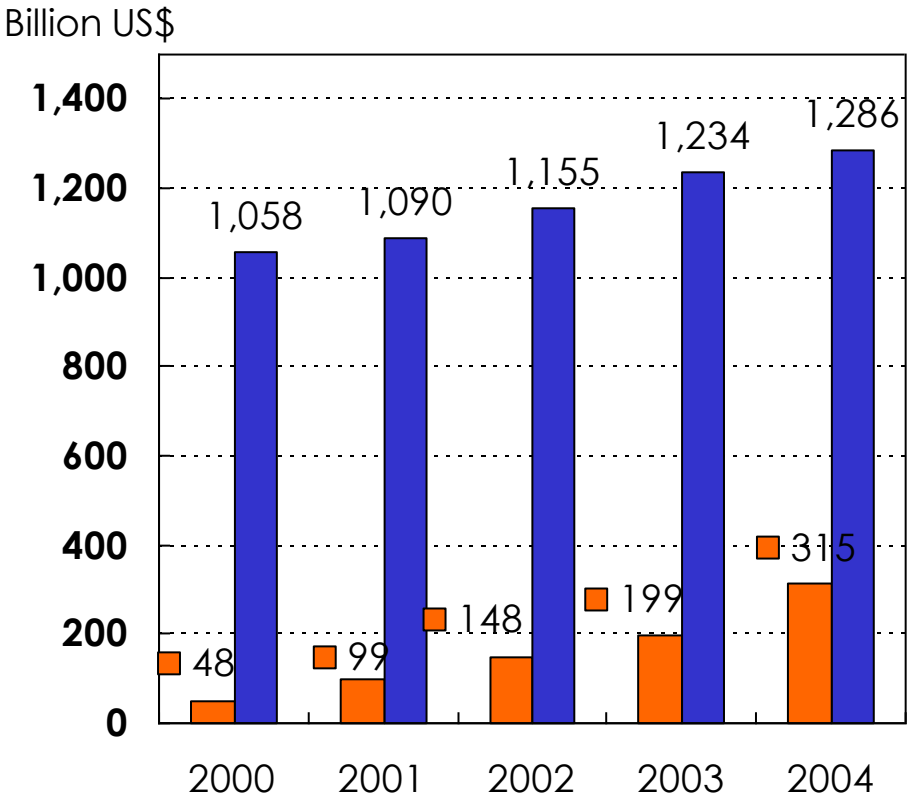
Total Population: 48 million
in 2005

Broadband User	90% of total households (12 million subscribers)
Mobile User	79% of total population (39 million users)
Licensed CA's Certificate	20% of total population (11 million certificates)

Online banking
25 million users

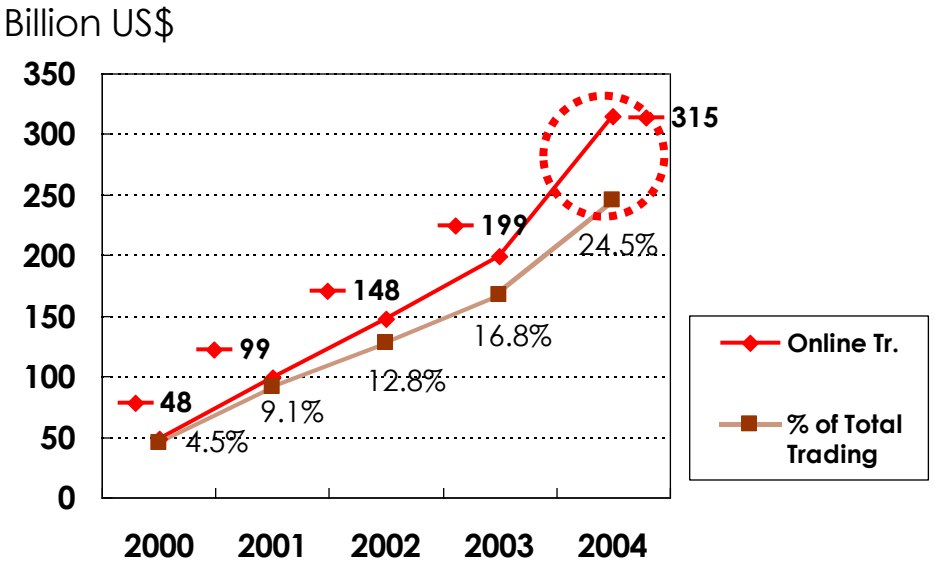
Online stock trading
70% of all transactions

e-Commerce Market Size in Korea



• Source: e-Commerce statistics
(2005 Korea National Statistical Office)

통계청이 3월 7일 발표한 전자상거래통계조사 결과에 따르면 2007년 우리나라 전자상거래 총규모는 516조 5,140억원으로 전년에 비해 24.9% 대폭 증가했다.



- Rapidly expanding area
- Reach to 24.5% of total trading volume in 2004

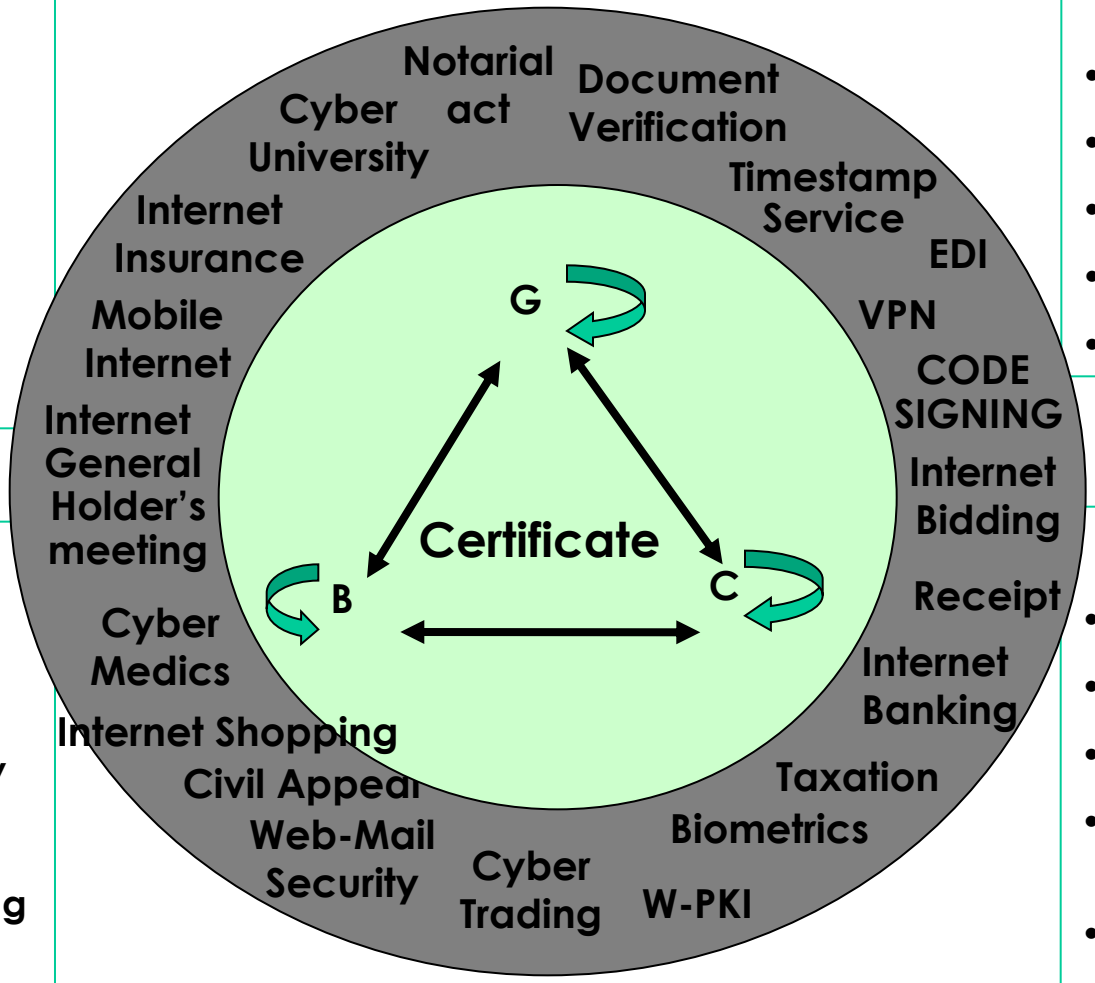
Business Cases

e-Biz

- Internet Shopping mall
- Ticket / Reservation
- On-Line Billing
- B2B Marketplace

Public

- Civil Appeal
- Digital Receipt
- Electronic supply
- Tax
- Electronic bidding
- Clearance



Finance

- Internet banking
- Cyber Trading
- Cyber insurance
- Elec. transfer
- Electronic currency

Others

- Medics
- Notarial act
- Cyber university
- General holder's meeting
- VPN
- Time Stamping

Some Examples

- Pay tax
  - http://www.giro.or.kr/
- e-Government
  - Certification document issuing
  - http://www.egov.go.kr/
- Online shopping and payment
  - Online bookstore http://www.yes24.com/
  - Credit card payment with certificate

Q & A

Thank you!