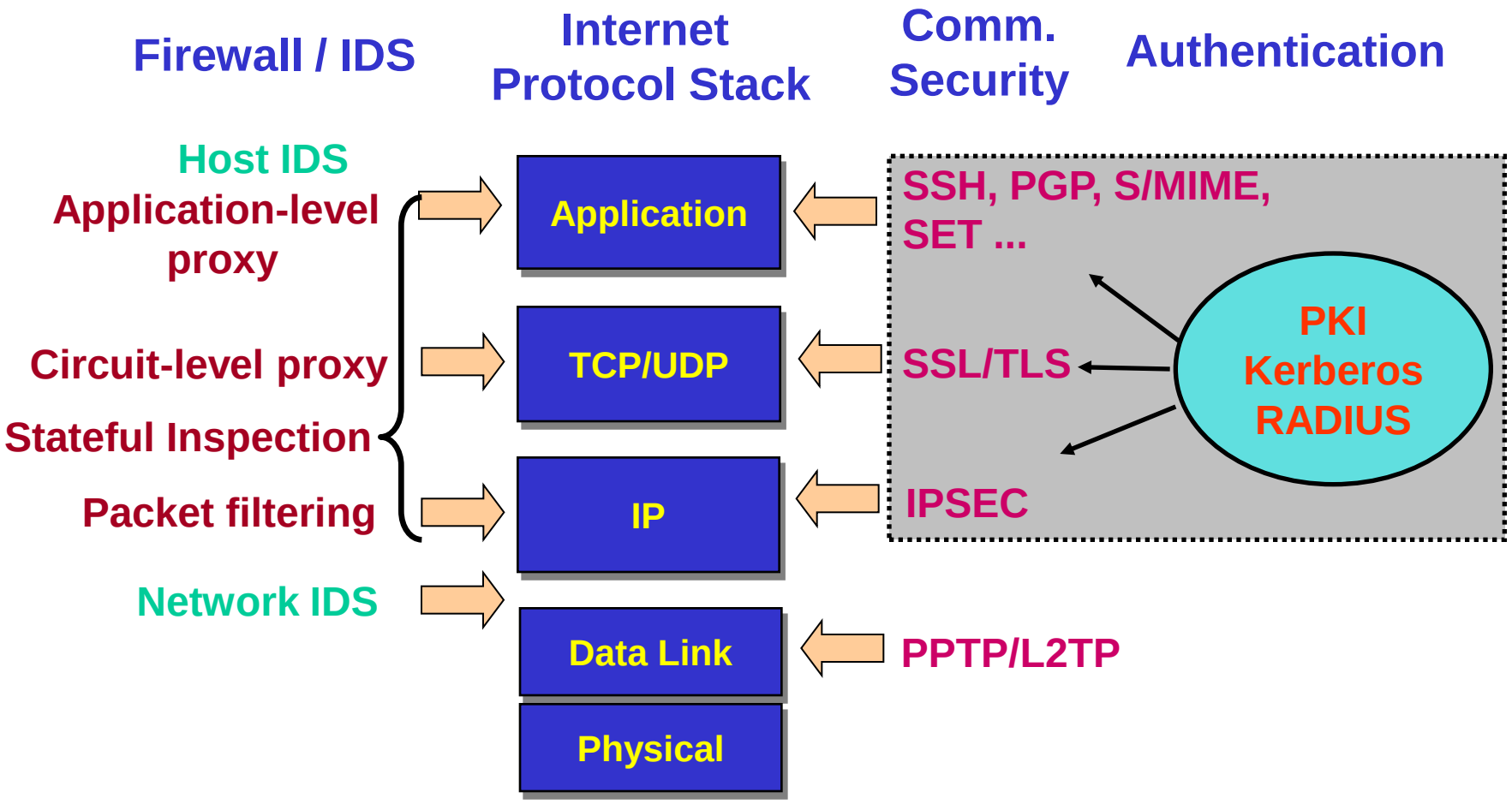
Lecture 2. Network Security
네트워크 보안

2008. 10. 17

Prof. Byoungcheon Lee
Joongbu University
sultan (at) joongbu . ac . kr

Major Internet Security Technologies



Contents

1. Security Attacks and Countermeasures
2. Firewall and IDS
3. Authentication and Certification
4. Securing Communications
5. Security Management

1. Security Attacks and Countermeasures

Security Vulnerabilities of TCP/IP

- TCP/IP was designed for connectivity, not considering security
- Host implementation vulnerabilities
  - Software “had/have/will have” bugs
  - Some elements in the specification were left to the implementers

Security Attacks - Passive

- **Passive attacks**
  - **Observing the information from the system**
  - Release of message contents
    - Sniffing, Wiretap
    - TEMPEST : detecting information from Transient Electromagnetic Pulse
  - Traffic analysis
- Against passive attacks
  - Difficult to **detect** (after they occurred), because they do not involve any change of the data.
  - Thus, they should be **prevented** rather than be **detected.**

Security Attacks - Active

- **Active attacks**
  - **Try to alter system resources or affect their operation**
  - **Creating illegitimate messages**
    - **Masquerade (who)**
    - **Replay (when)**
    - **Modification of messages (what)**
  - **Denying legitimate messages**
    - **Repudiation**
  - **Making system facilities unavailable**
- Against active attacks
  - Difficult to prevent, because of many new vulnerabilities.
  - So, the goal is to **detect** active attacks and to **recover** as soon as possible.

Various Security Attacks

- Virus : program fragment that, when executed, attached itself to other programs
- 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

Attacks on Different Layers

- IP Attacks
  - Packet sniffing, Address spoofing, IP fragmentation attack
- ICMP Attacks
  - No authentication in ICMP, ICMP redirect, Collect information
- Routing Attacks
  - Unauthenticated routing protocols control Internet reachability
- TCP Attacks
  - Session hijacking, Session poisoning
- Application Layer Attacks
  - Applications which DO NOT authenticate properly
  - Authentication information is transmitted in clear: FTP, Telnet, POP
  - DNS insecurity: DNS poisoning, DNS zone transfer

Denial of Service (DoS, 서비스거부공격)

- 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)

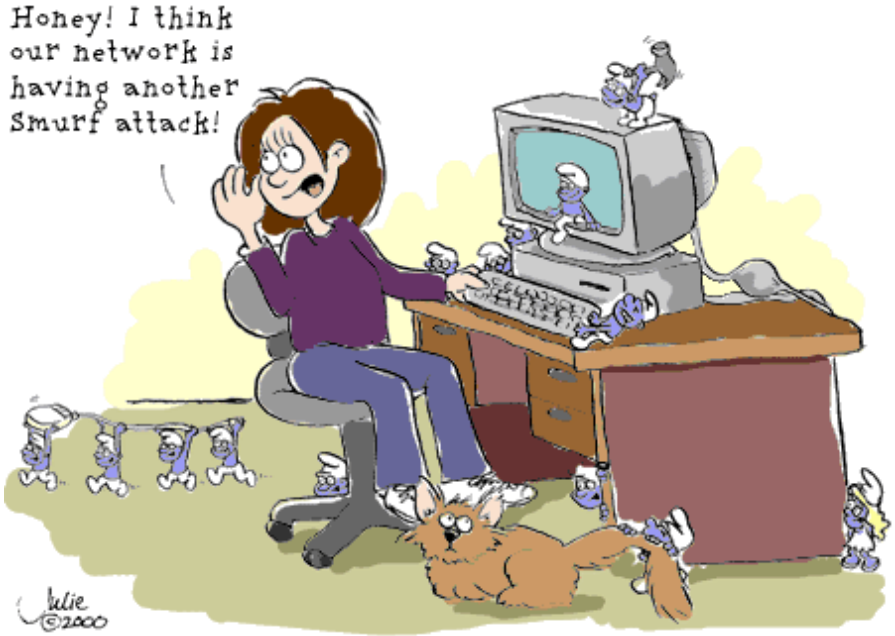
SYN Flooding Attack

- 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

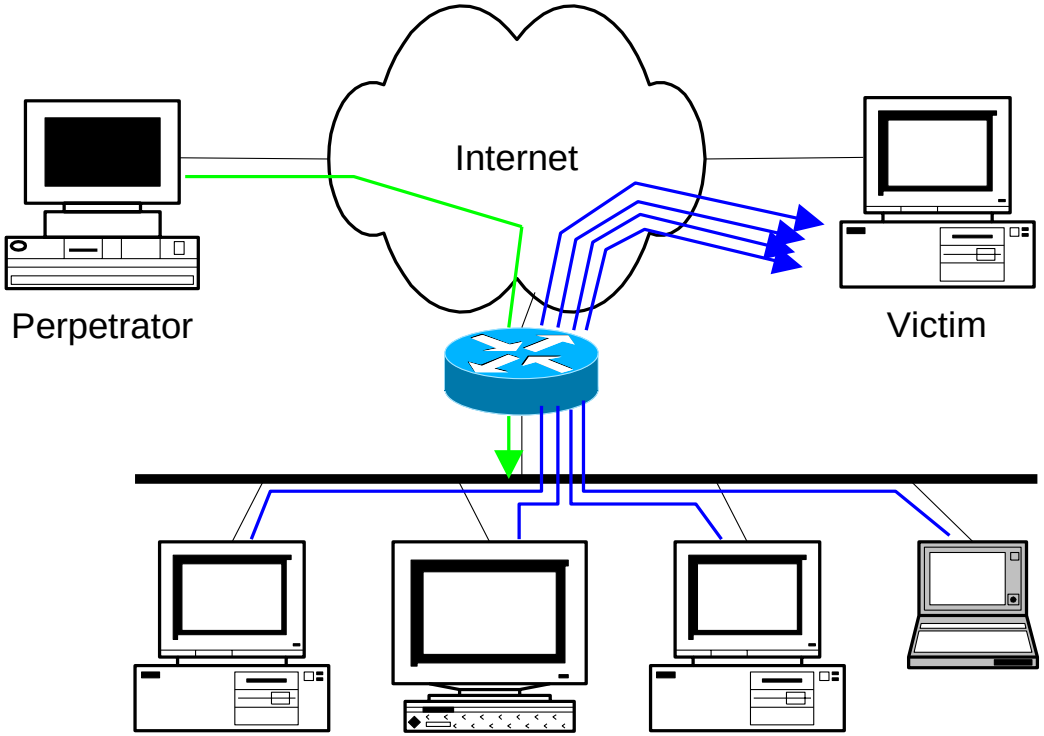
- SMURF
  - A way of generating a lot of computer network traffic to a victim site
  - Source IP address of a broadcast ping is forged, then large number of machines respond back to victim, overloading it



SMURF Attack

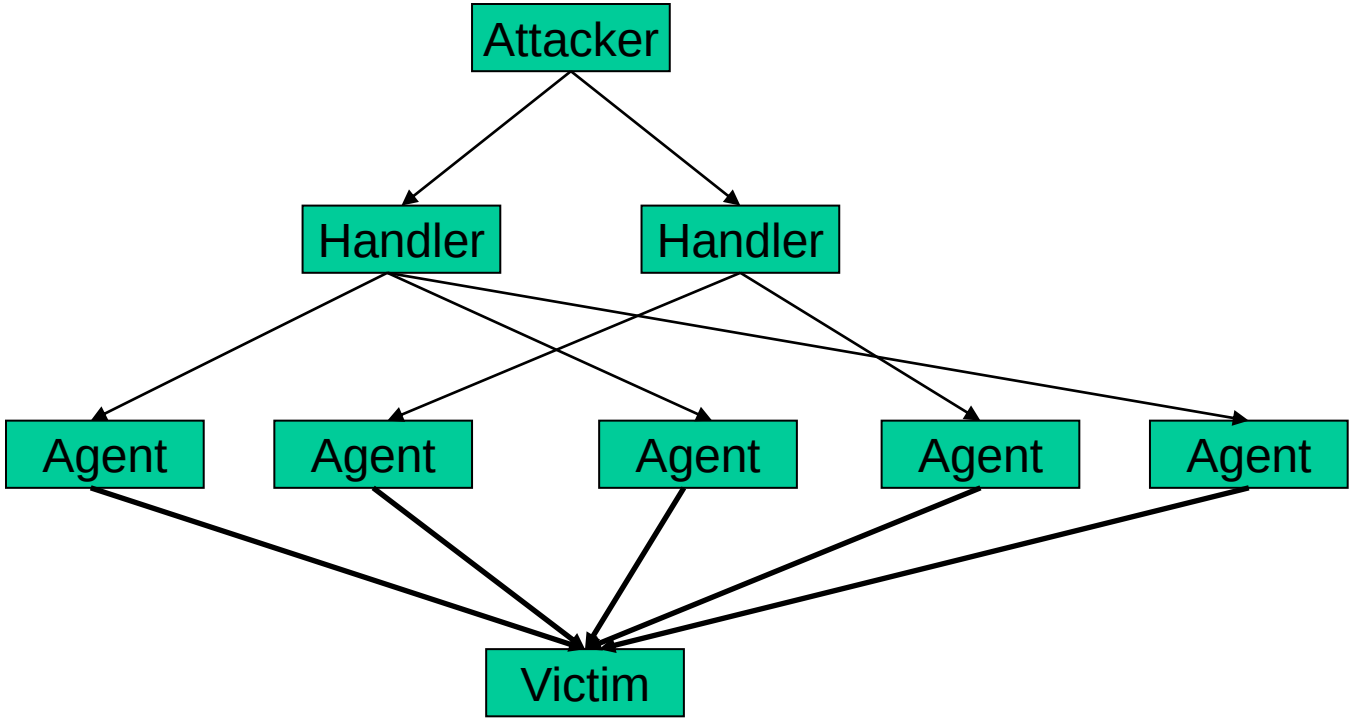
ICMP echo (spoofed source address of victim)
Sent to IP broadcast address

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

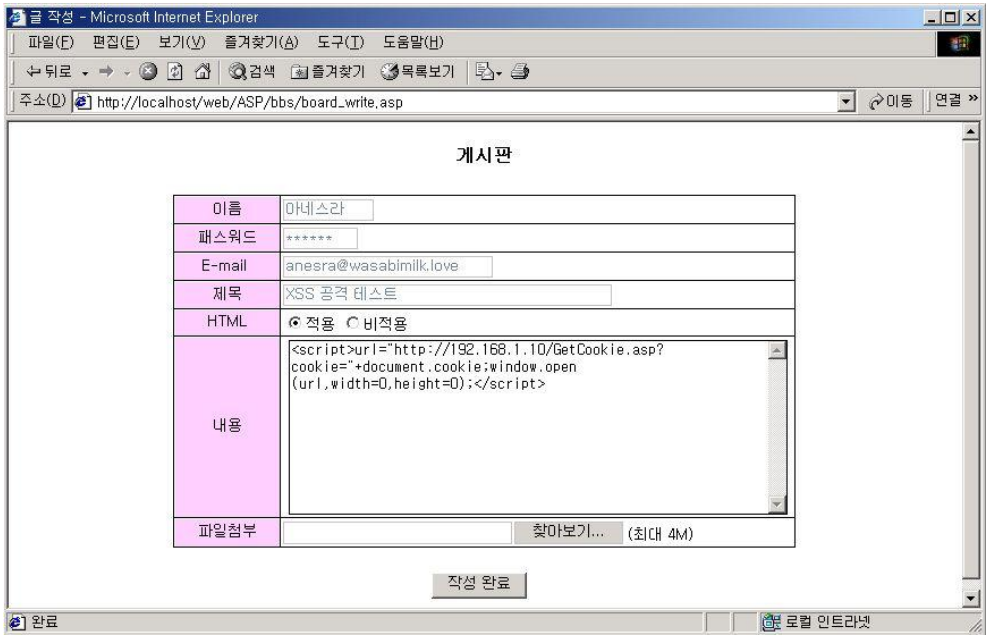


Web Services Threats

- 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
  - XSS (cross site scripting)
  - File upload
  - Directory traversal, Directory listing
  - Skipping authentication
  - SQL injection



Spyware and Adware

- Spyware
  - Any technology that aids in gathering information about a person or organization without their knowledge.
  - 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

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.

Links to http://82.90.165.65/citi

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

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

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 engineering
  - Education

2. Firewall and IDS

Firewall and IDS

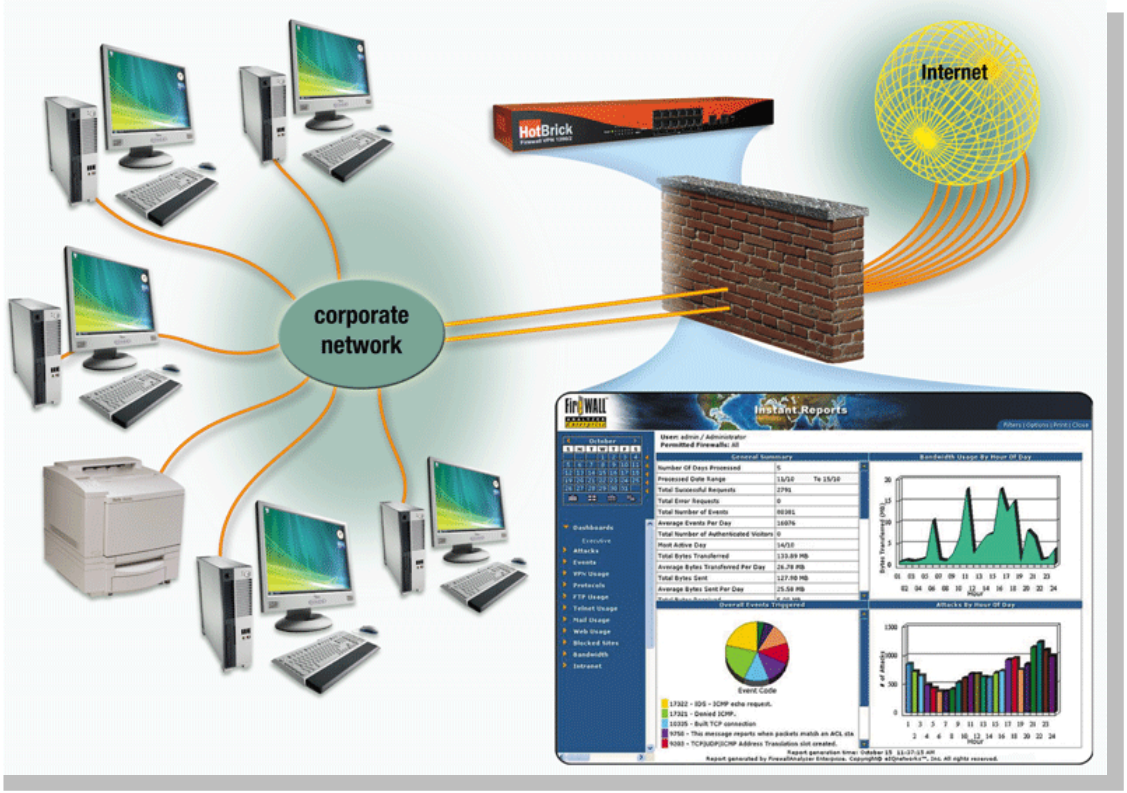
Firewall – Security Guard

IDS – Security monitor and alarm

Firewalls

- Basic problem
  - Many network applications and protocols have security problems that are fixed over time
  - Difficult for general users to keep up with changes and keep host secure
- Solution
  - Administrators limit access to end hosts by using a firewall
  - Firewall isolates organization's internal network from larger Internet, allowing some traffics specified in the policy, blocking others.
  - Firewall is kept up-to-date by administrators

Firewalls

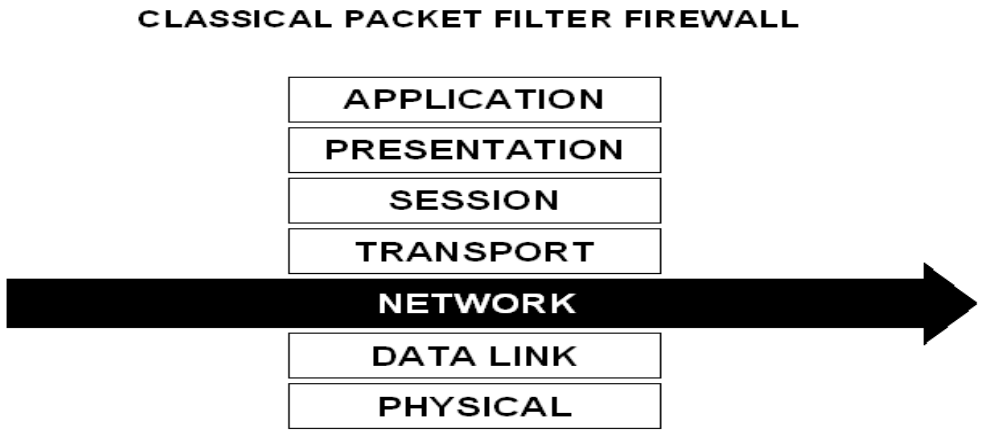


Two Types of Firewalls

- Packet Filter Firewall
- Application Proxy Firewall

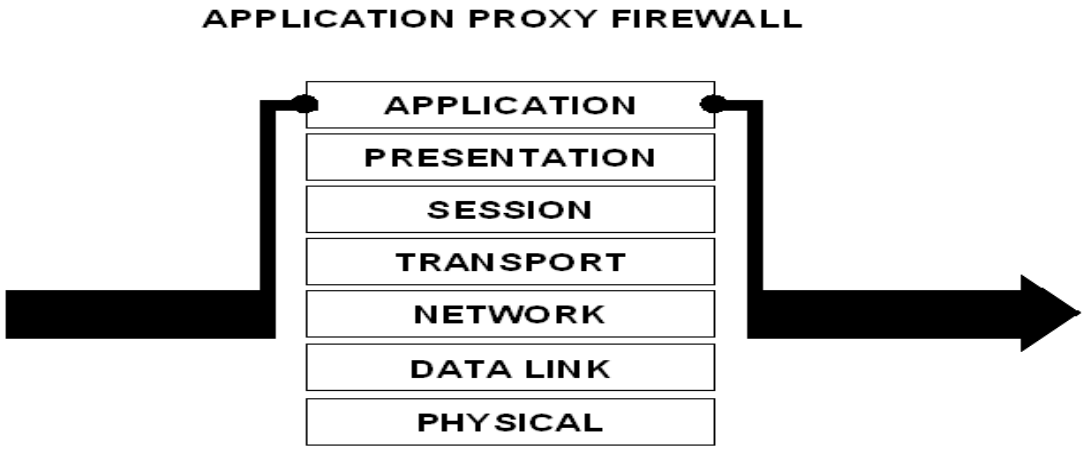
Packet Filter Firewalls

- 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

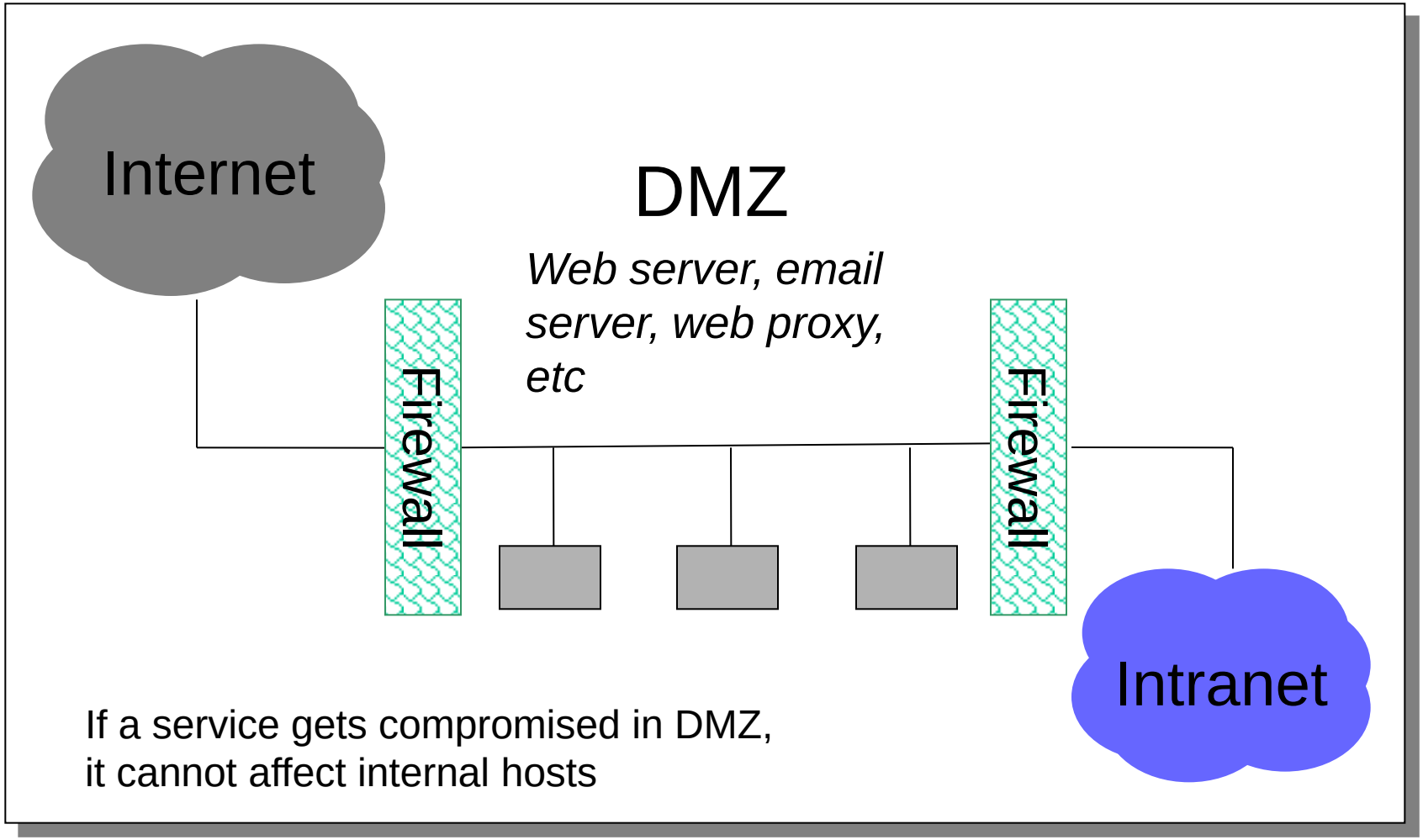
- Application Proxy Firewall
  - Full application-level awareness of attempted connections.



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

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)

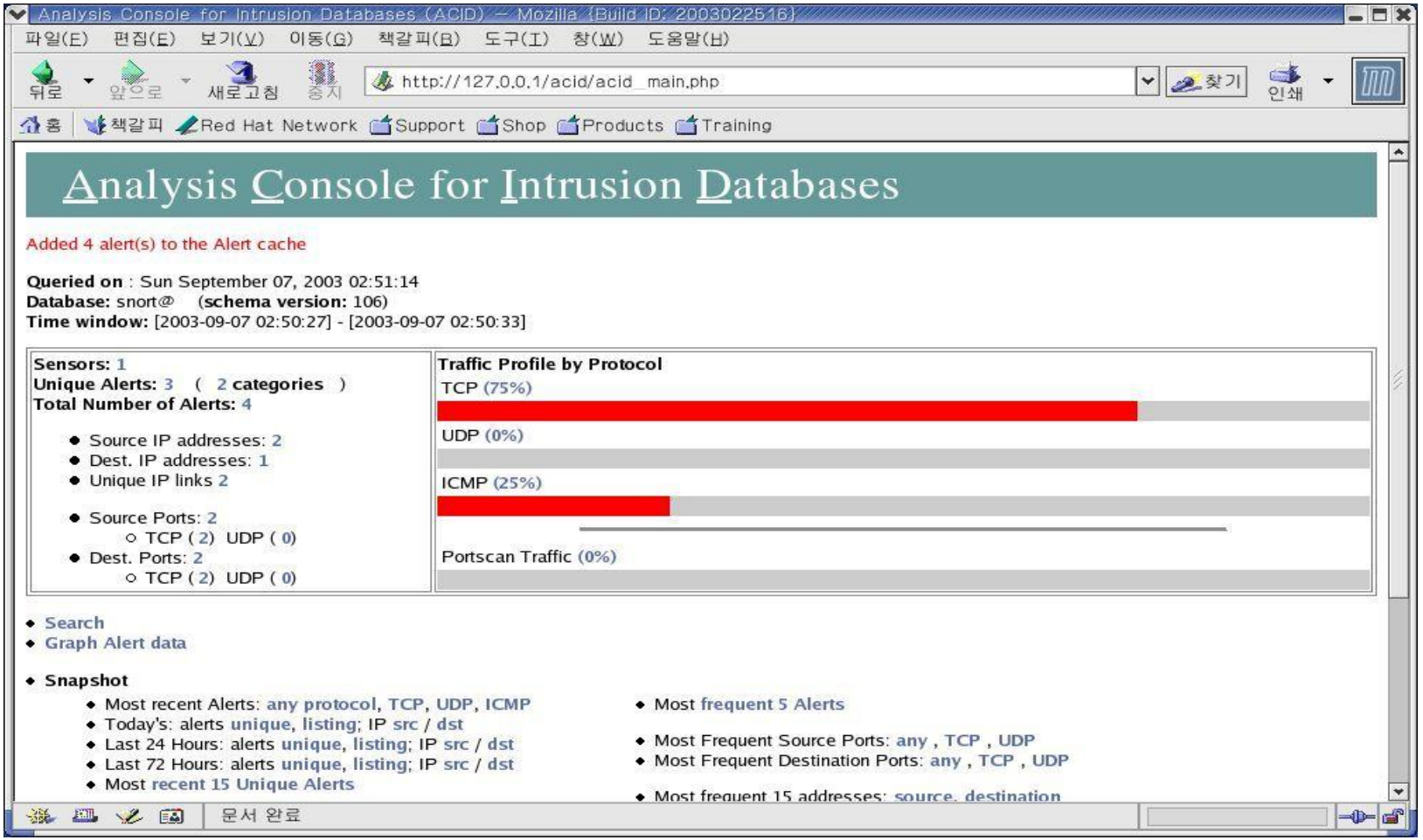
- Solution?
  - Intrusion Detection Systems
  - Monitor data and behavior
  - Report when identify attacks

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.

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)

3. Authentication and Certification

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

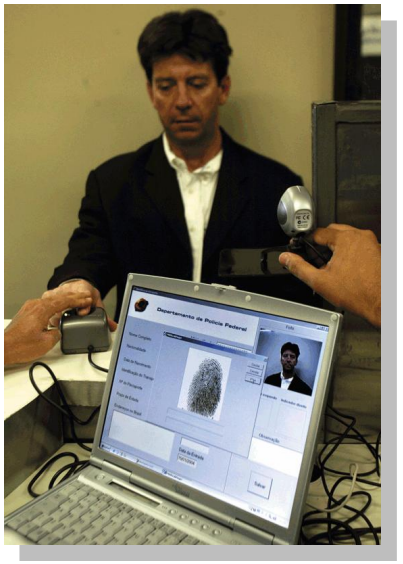
- Message Authentication
  - Show that a message was generated by an entity
  - Using digital signature or MAC

3 Approaches for Identification

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

RSA SecurID

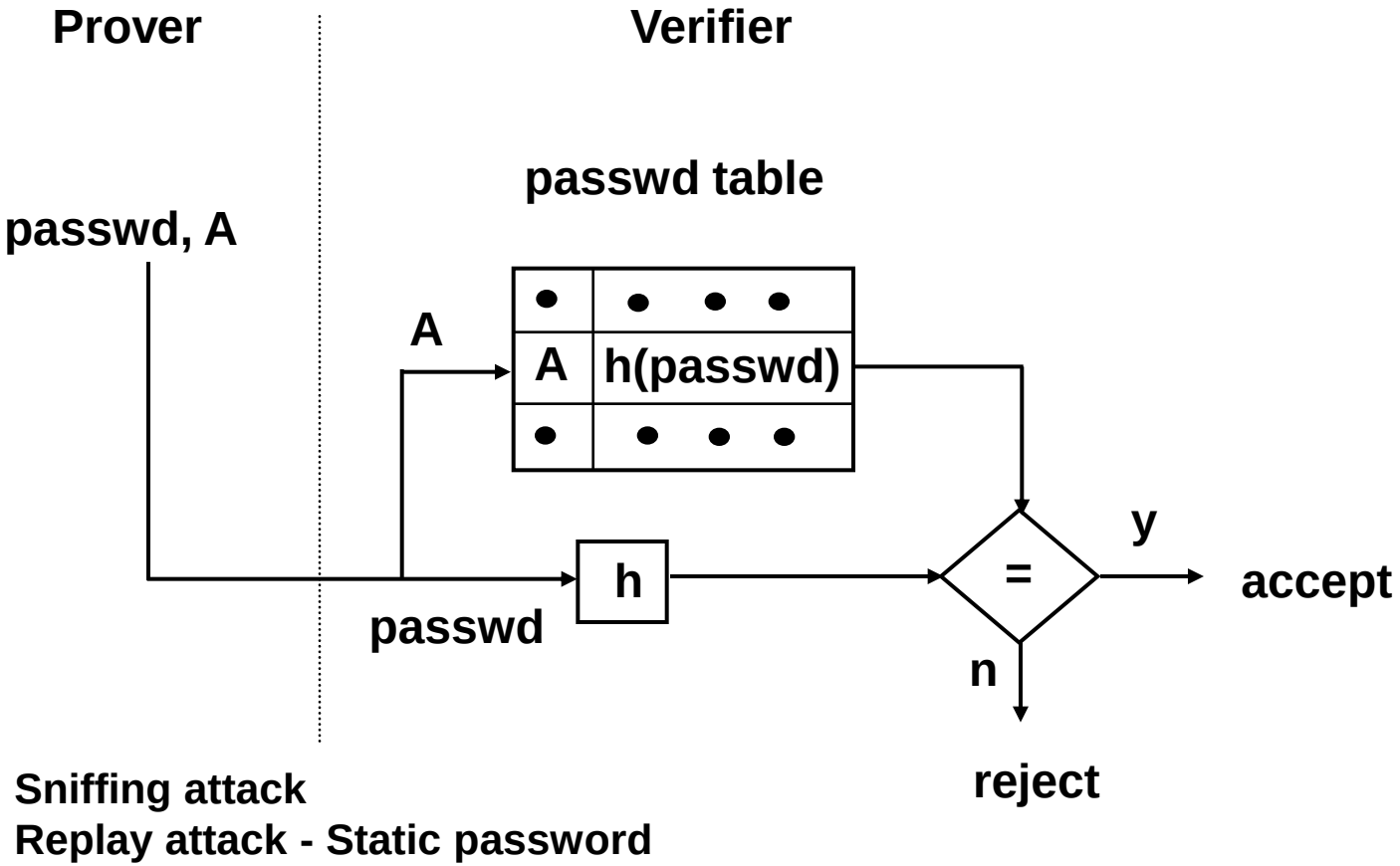
Two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator)



Identification Schemes

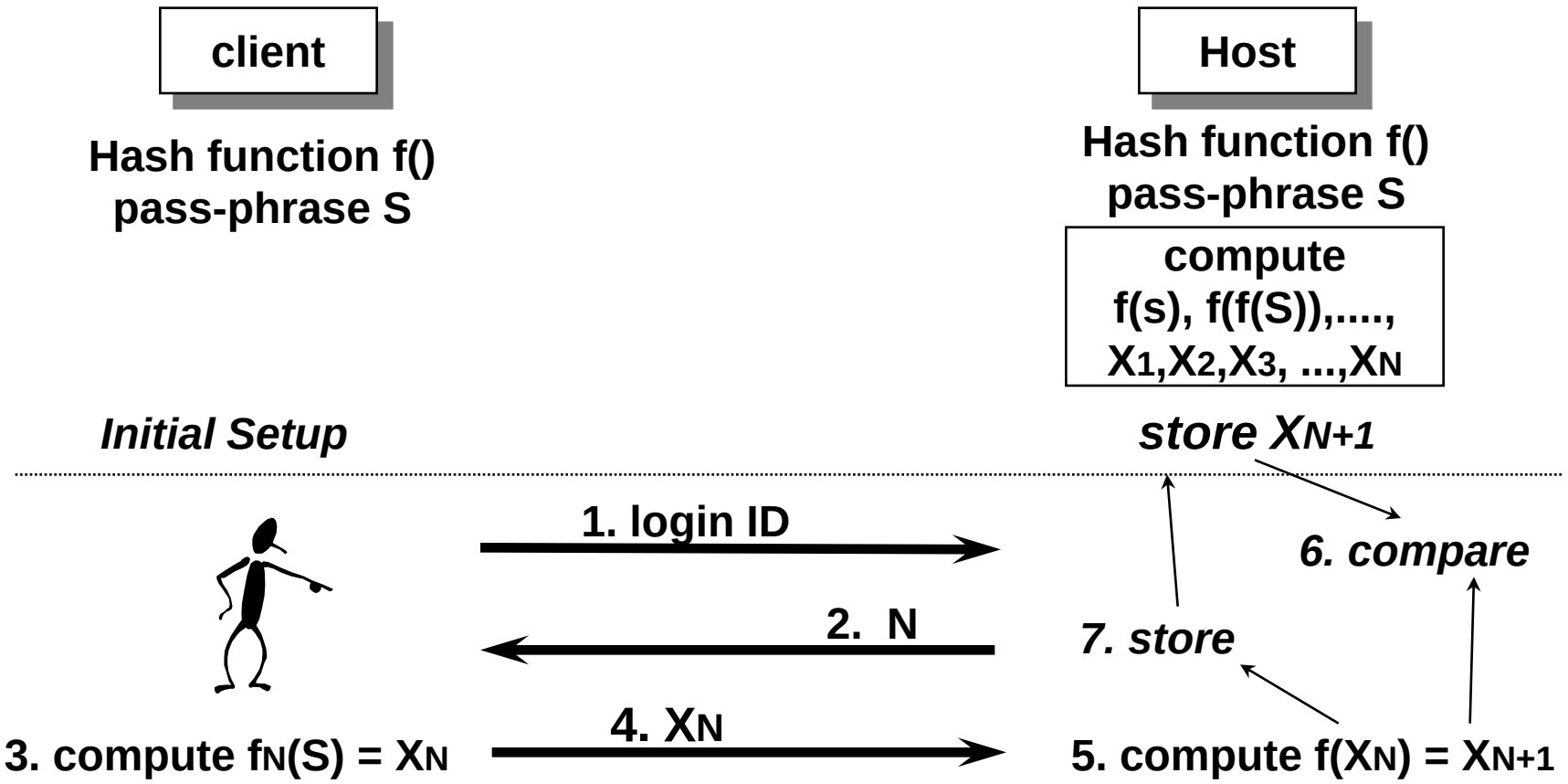
- Password-based scheme (weak authentication)
  - crypt *passwd* under UNIX
  - one-time password
- Challenge-Response scheme (strong authentication)
  - Symmetric cryptosystem
  - MAC (keyed-hash) function
  - Asymmetric cryptosystem
- Using Cryptographic Protocols
  - Fiat-Shamir identification protocol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

$u \in_R Z_q^*$

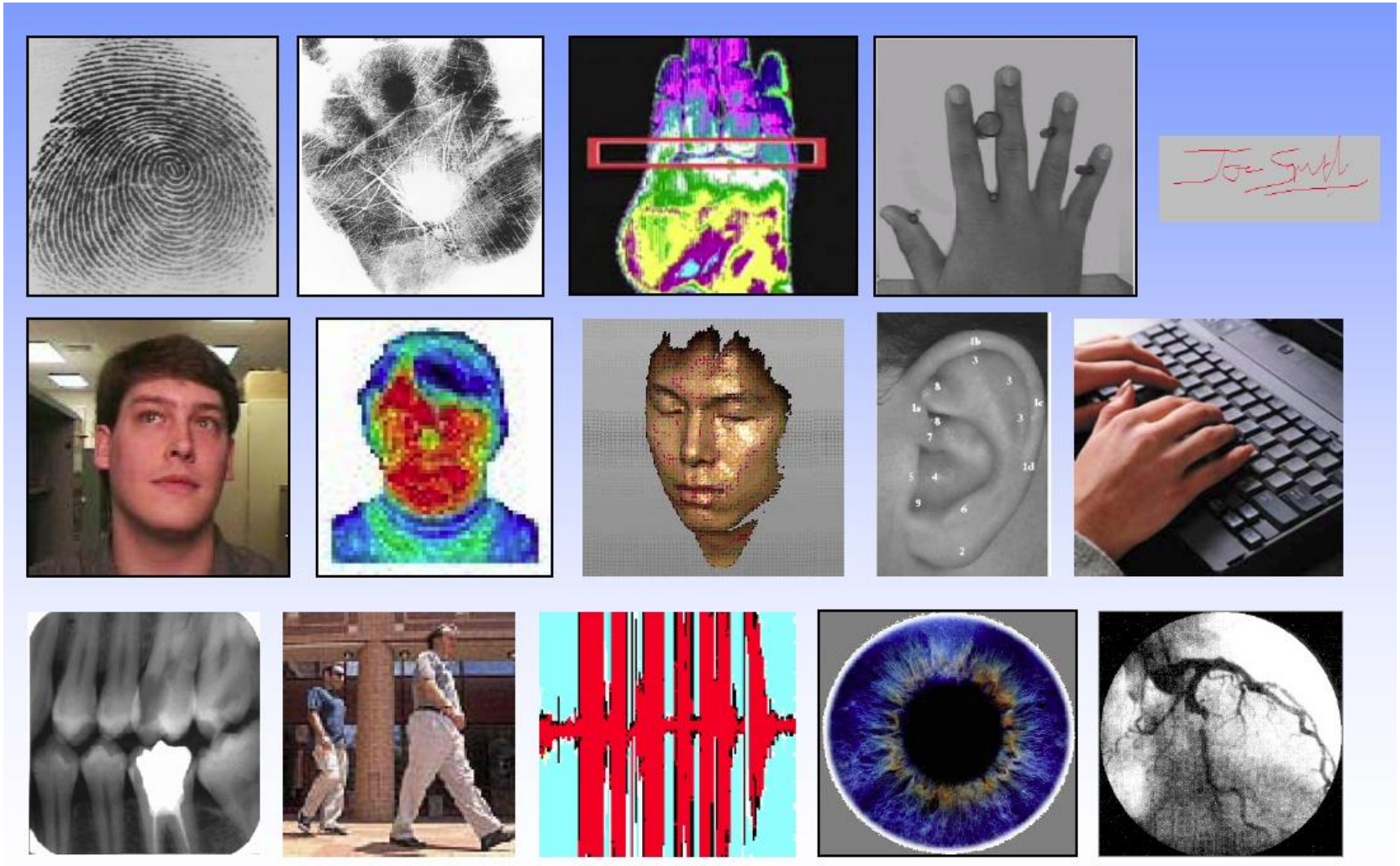
← u **Challenge**

$w = t - ux \bmod q$

w **Response** →

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

Identification using Biometric Trails



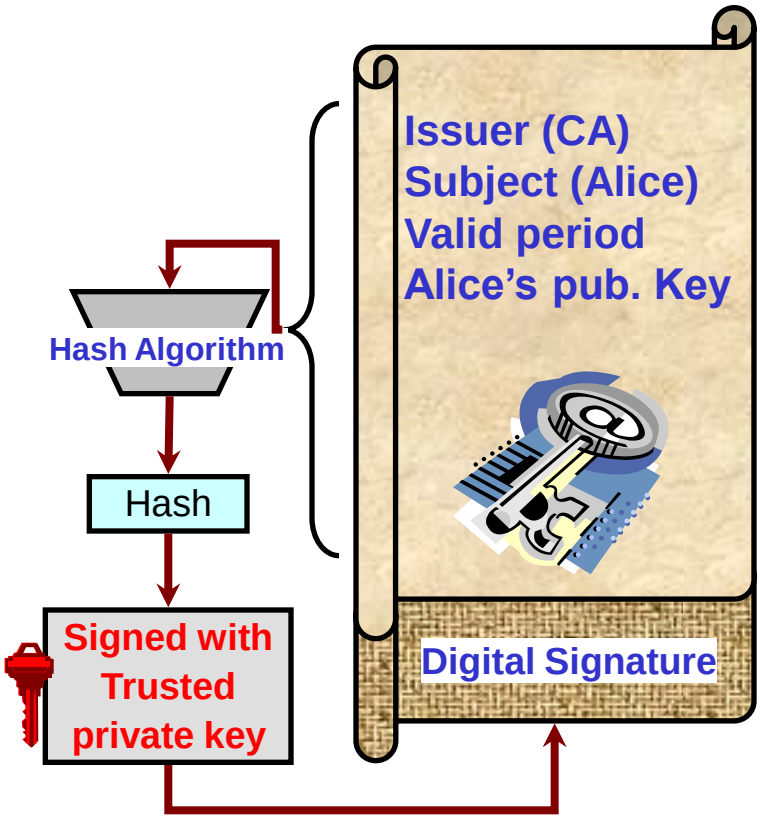
Certificate-based Authentication

❖ Digital Certificate

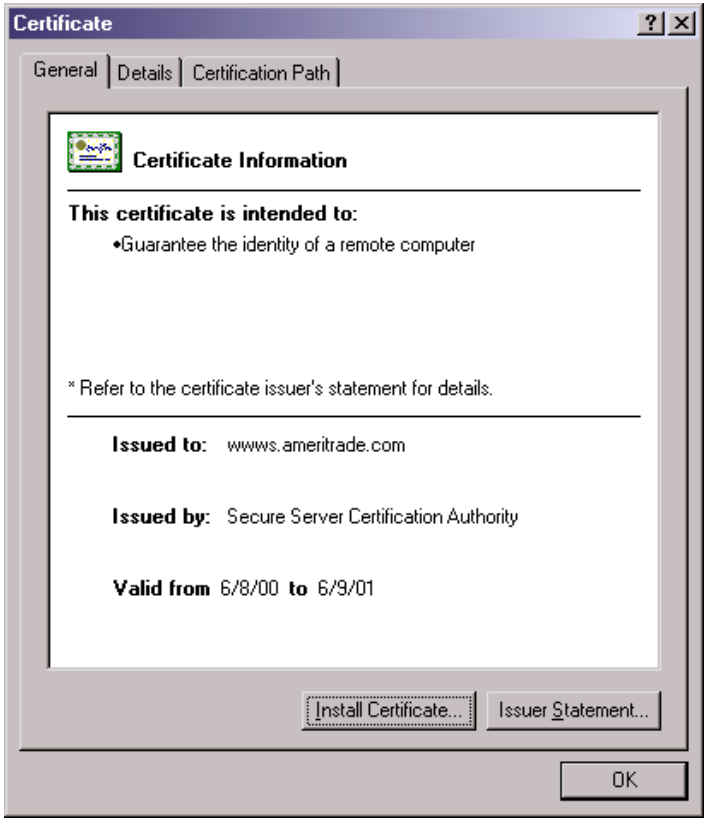
- ✓ A file containing Identification information (CA's name (Issuer), Alice's name (Subject), valid period, Alice's public key, etc) and digital signature signed by trusted third party (CA) to guarantee its authenticity & integrity

❖ 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

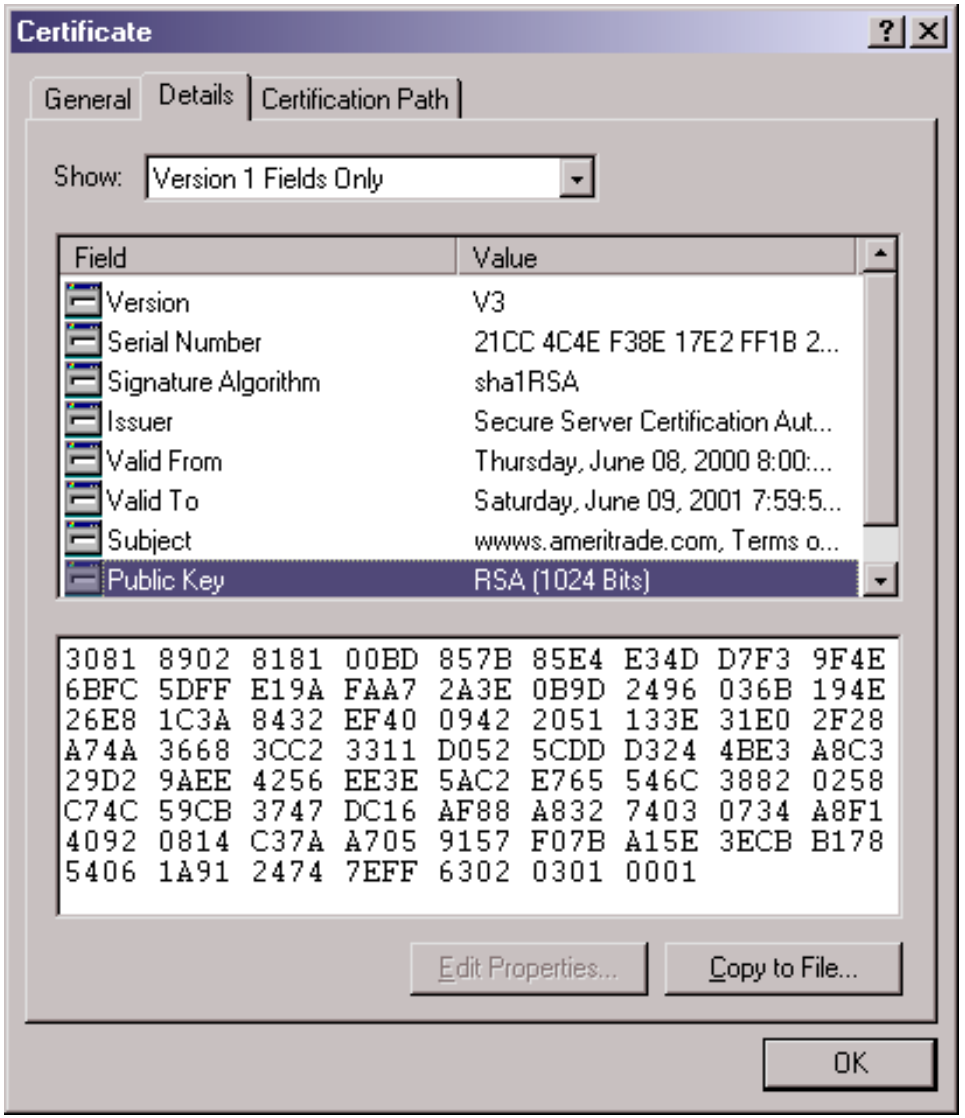


Certificate-based Authentication



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

Certificate



X.509 V3 Certificate Format

```
Certificate  ::=  SEQUENCE  {
     tbsCertificate                TBSCertificate,
     signatureAlgorithm            AlgorithmIdentifier,
     signatureValue                BIT STRING  }

   TBSCertificate  ::=  SEQUENCE  {
     version                       [0]  EXPLICIT Version DEFAULT v1,
     serialNumber                   CertificateSerialNumber,
     signature                     AlgorithmIdentifier,
     issuer                        Name,
     validity                      Validity,
     subject                       Name,
     subjectPublicKeyInfo          SubjectPublicKeyInfo,
     issuerUniqueID                [1]  IMPLICIT UniqueIdentifier OPTIONAL,
                                   -- If present, version shall be v2 or v3
     subjectUniqueID               [2]  IMPLICIT UniqueIdentifier OPTIONAL,
                                   -- If present, version shall be v2 or v3
     extensions                    [3]  EXPLICIT Extensions OPTIONAL
                                   -- If present, version shall be v3
     }
```

Sample Certificate

```
Certificate:
    Data:
        Version: v3 (0x2)
        Serial Number: 3 (0x3)
        Signature Algorithm: PKCS #1 MD5 With RSA Encryption
        Issuer: OU=Ace Certificate Authority, O=Ace Industry, C=US
        Validity:
            Not Before: Fri Oct 17 18:36:25 1997
            Not  After: Sun Oct 17 18:36:25 1999
        Subject: CN=Jane Doe, OU=Finance, O=Ace Industry, C=US
        Subject Public Key Info:
            Algorithm: PKCS #1 RSA Encryption
            Public Key:
                Modulus:
                    00:ca:fa:79:98:8f:19:f8:d7:de:e4:49:80:48:e6:2a:2a:86:
                    ed:27:40:4d:86:b3:05:c0:01:bb:50:15:c9:de:dc:85:19:22:
                    43:7d:45:6d:71:4e:17:3d:f0:36:4b:5b:7f:a8:51:a3:a1:00:
                    98:ce:7f:47:50:2c:93:36:7c:01:6e:cb:89:06:41:72:b5:e9:
                    73:49:38:76:ef:b6:8f:ac:49:bb:63:0f:9b:ff:16:2a:e3:0e:
                    9d:3b:af:ce:9a:3e:48:65:de:96:61:d5:0a:11:2a:a2:80:b0:
                    7d:d8:99:cb:0c:99:34:c9:ab:25:06:a8:31:ad:8c:4b:aa:54:
                    91:f4:15
                Public Exponent: 65537 (0x10001)
    Extensions:
        Identifier: Certificate Type
            Critical: no
            Certified Usage:
                SSL Client
        Identifier: Authority Key Identifier
            Critical: no
            Key Identifier:
                f2:f2:06:59:90:18:47:51:f5:89:33:5a:31:7a:e6:5c:fb:36:
                26:c9
```

```
Signature:
    Algorithm: PKCS #1 MD5 With RSA Encryption
    Signature:
        6d:23:af:f3:d3:b6:7a:df:90:df:cd:7e:18:6c:01:69:8e:54:65:fc:06:
        30:43:34:d1:63:1f:06:7d:c3:40:a8:2a:82:c1:a4:83:2a:fb:2e:8f:fb:
        f0:6d:ff:75:a3:78:f7:52:47:46:62:97:1d:d9:c6:11:0a:02:a2:e0:cc:
        2a:75:6c:8b:b6:9b:87:00:7d:7c:84:76:79:ba:f8:b4:d2:62:58:c3:c5:
        b6:c1:43:ac:63:44:42:fd:af:c8:0f:2f:38:85:6d:d6:59:e8:41:42:a5:
        4a:e5:26:38:ff:32:78:a1:38:f1:ed:dc:0d:31:d1:b0:6d:67:e9:46:a8:
        dd:c4
```

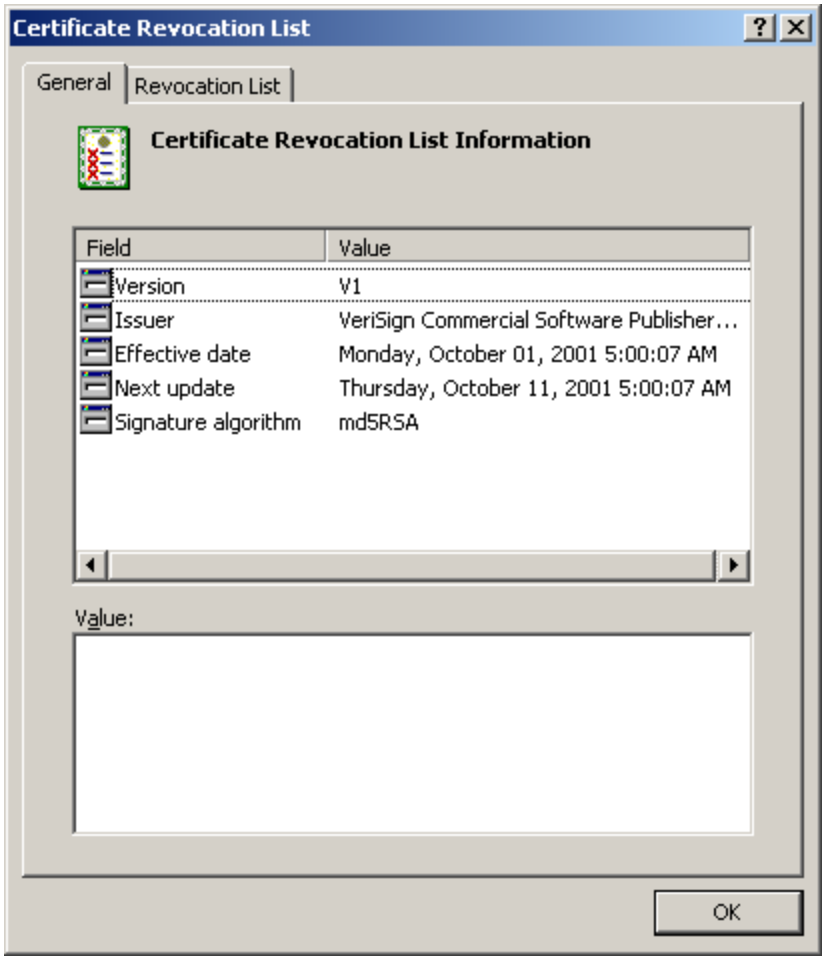
```
-----BEGIN CERTIFICATE-----
MIICKzCCAZSgAwIBAgIBAzANBgkqhkiG9w0BAQQFADA3MQswCQYD
VQQGEwJVUzERMA8GA1UEChMITmV0c2NhcGUxFTATBgNVBAsTDF
N1cHJpeWEncyBDQTAeFw05NzEwMTgwMTM2MjVaFw05OTEwMTgw
MTM2MjVaMEgxCzAJBgNVBAYTAlVTMREwDwYDVQQKEwhOZXRzY
2FwZTENMAsGA1UECxMEUHViczEXMBUGA1UEAxMOU3VwcmI5YSB
TaGV0dHkwgZ8wDQYJKoZIhvcNAQEFBQADgY0AMIGJAoGBAMr6eZiP
GfjX3uRJgEjmKiqG7SdATYazBcABu1AVyd7chRkiQ31FbXFOGD3wNktb
f6hRo6EAmM5/R1AskzZ8AW7LiQZBcrXpc0k4du+2Q6xJu2MPm/8WKuM
OnTuvzpo+SGXelmHVChEqooCwfdiZywyZNMmrJgaoMa2MS6pUkfQVAg
MBAAGjNjA0MBEGCWCGSAGG+EIBAQQEAwIAgDAfBgNVHSMEGDAW
gBTy8gZZkBhHUfWJM1oxeuZc+zYmyTANBgkqhkiG9w0BAQQFAAOBgQ
BtI6/z07Z635DfzX4XbAFpjlRl/AYwQzTSYx8GfcNAqCqCwaSDKvsuj/vwbf
91o3j3UkdGYpcd2cYRCgKi4MwqdWyLtpuHAH18hHZ5uvi00mJYw8W2w
UOsY0RC/a/IDy84hW3WWehBUqVK5SY4/zJ4oTjx7dwNMdGwbWfpRqjd
1A==
-----END CERTIFICATE-----
```

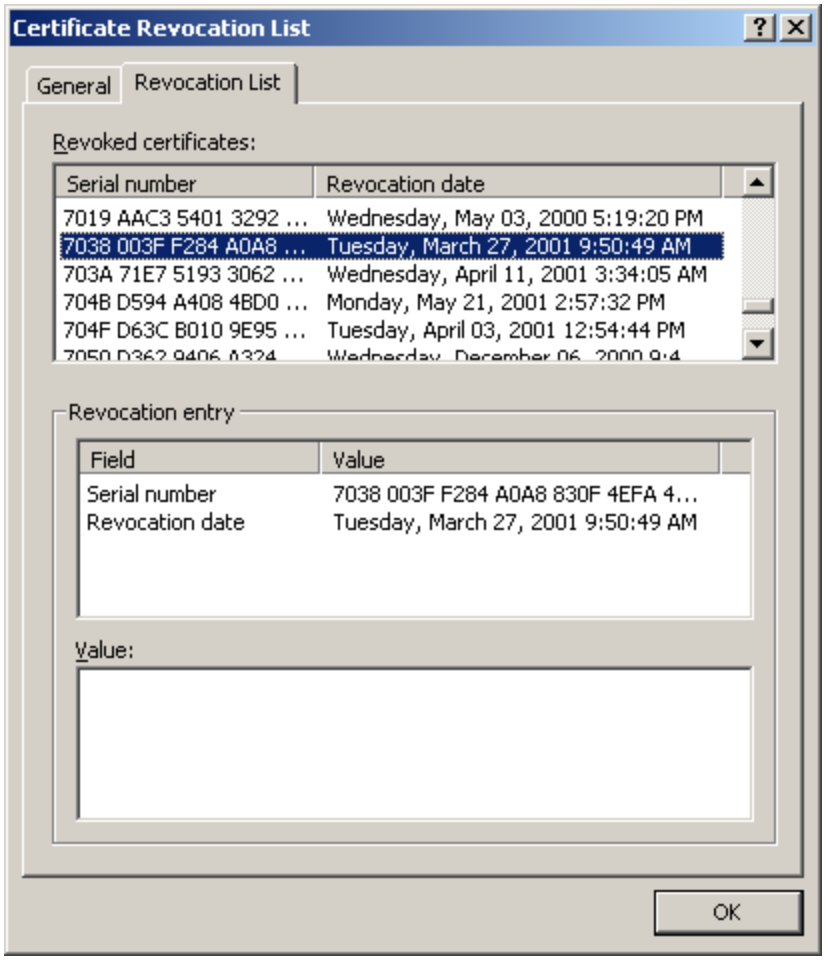
How to Revoke a Certificate?

- Certificate Revocation List (CRL)
  - A digital document which has a list of revoked certificates
  - Signed by CA
  - Defined in X.509 v2

- Why revoke a certificate?
  - When the user leave (retire from) the organization
  - Lost the private key, need to use a new key

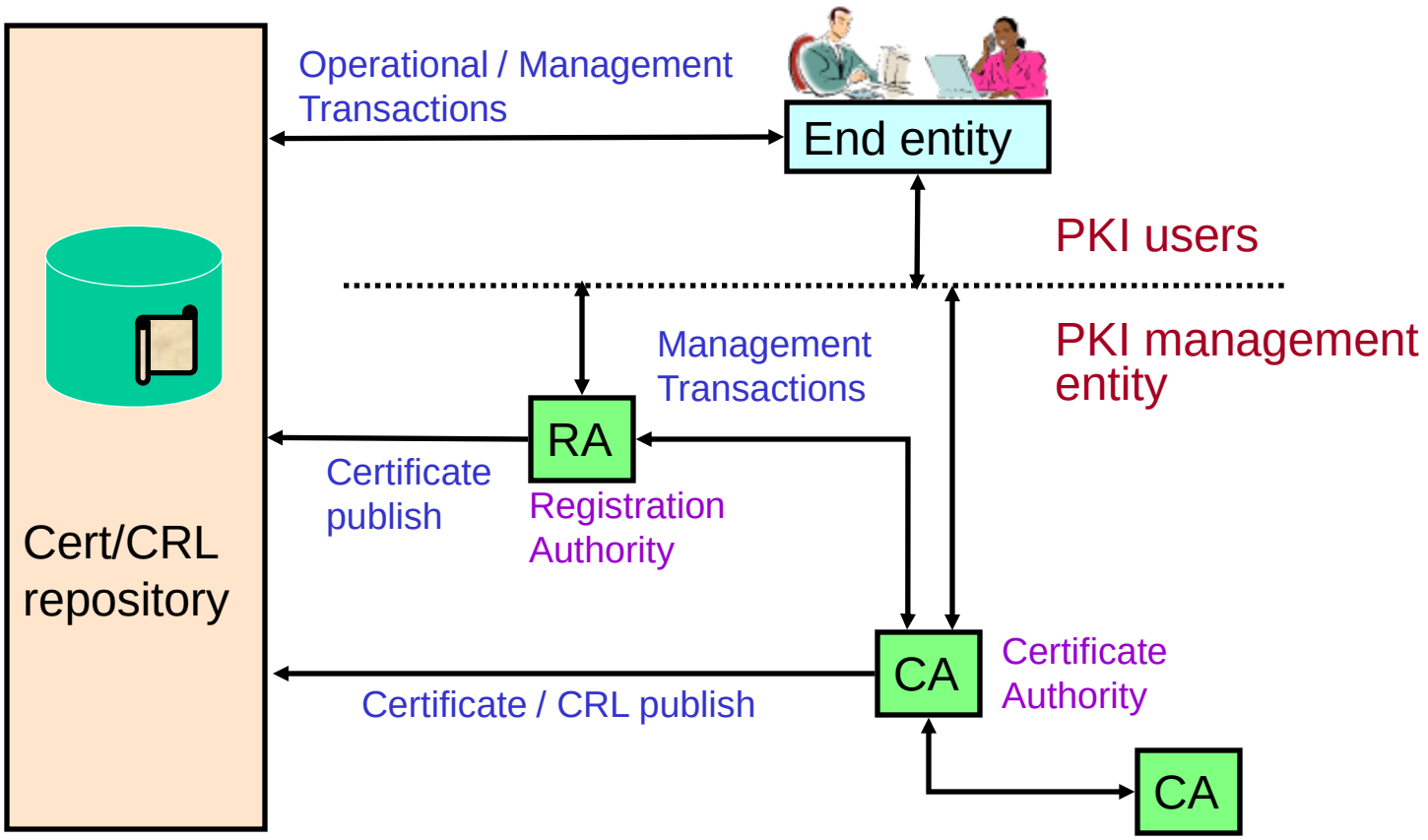
Certificate Revocation List



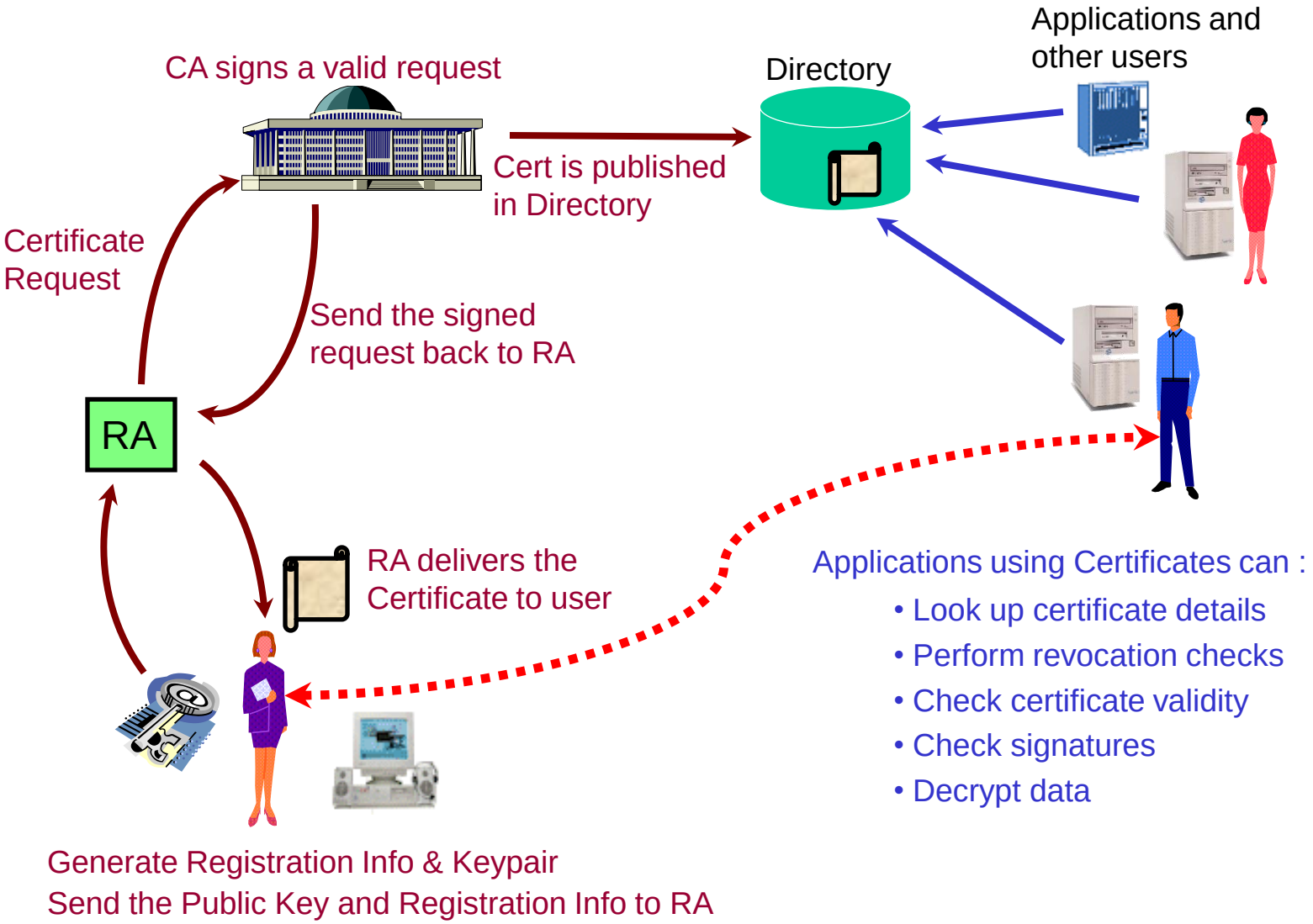


Public Key Infrastructure (PKI) Architecture

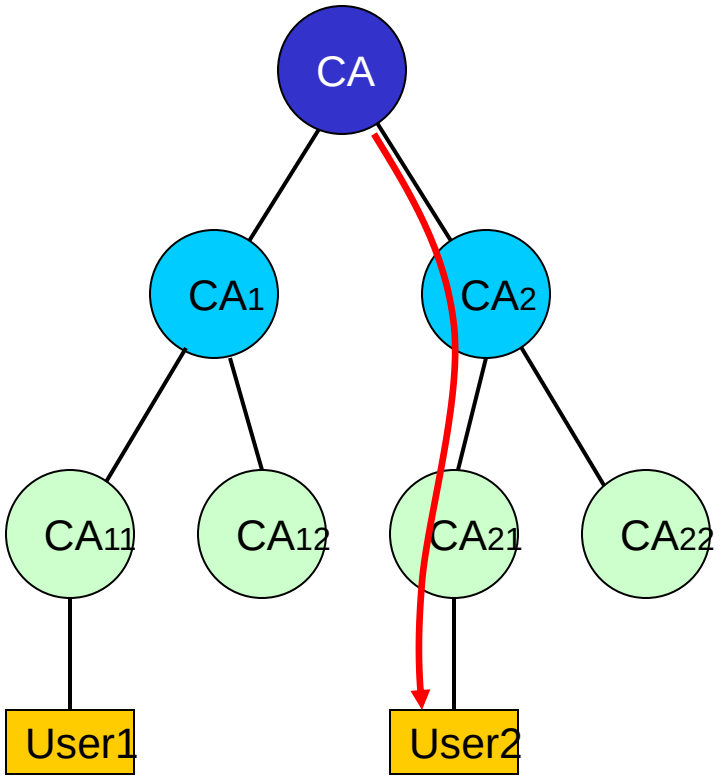
PKI is the hardware, software, people, policies, & procedures
needed to create, manage, store, distribute, & revoke certificates



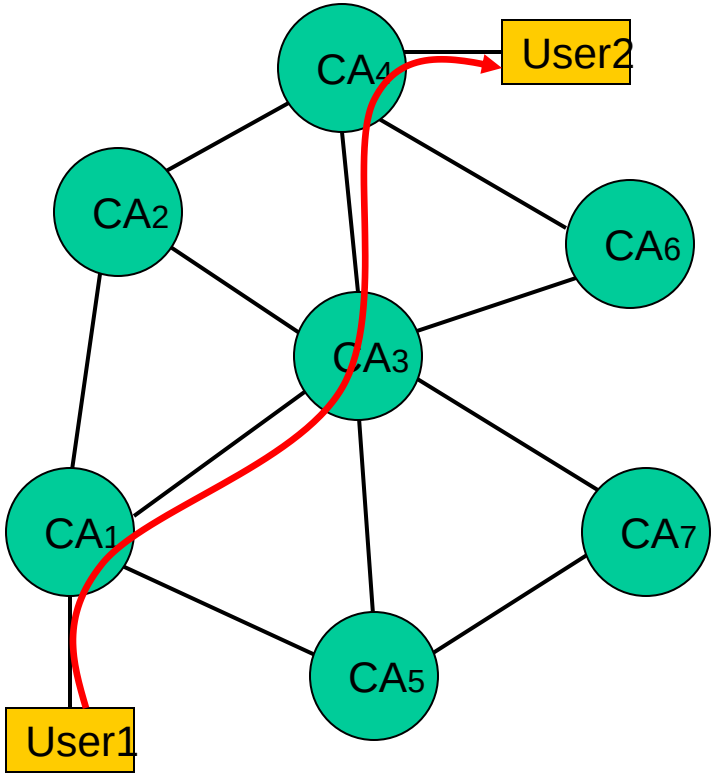
How a PKI works?



PKI Hierarchy - Trust Relationship

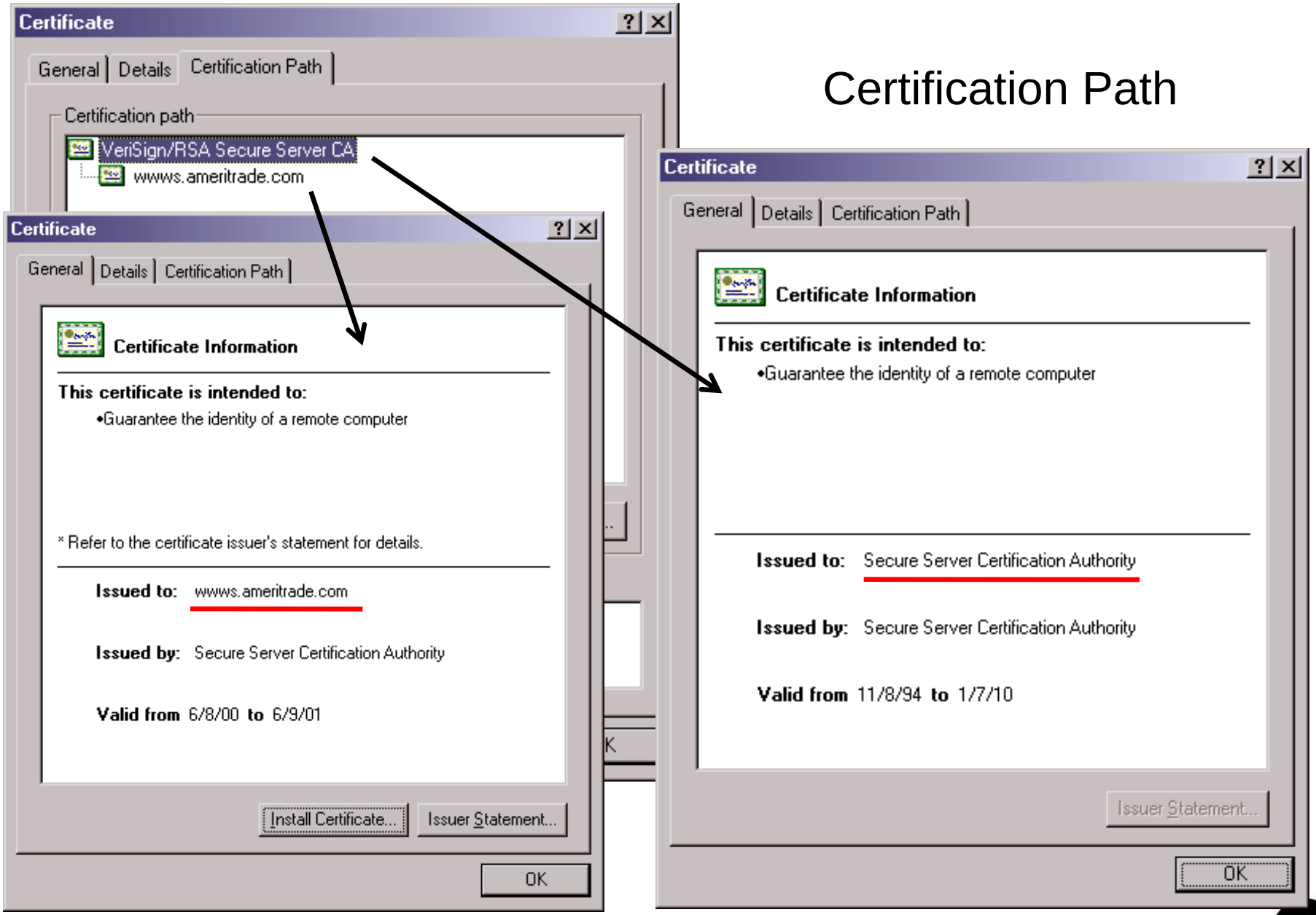


Hierarchical Structure



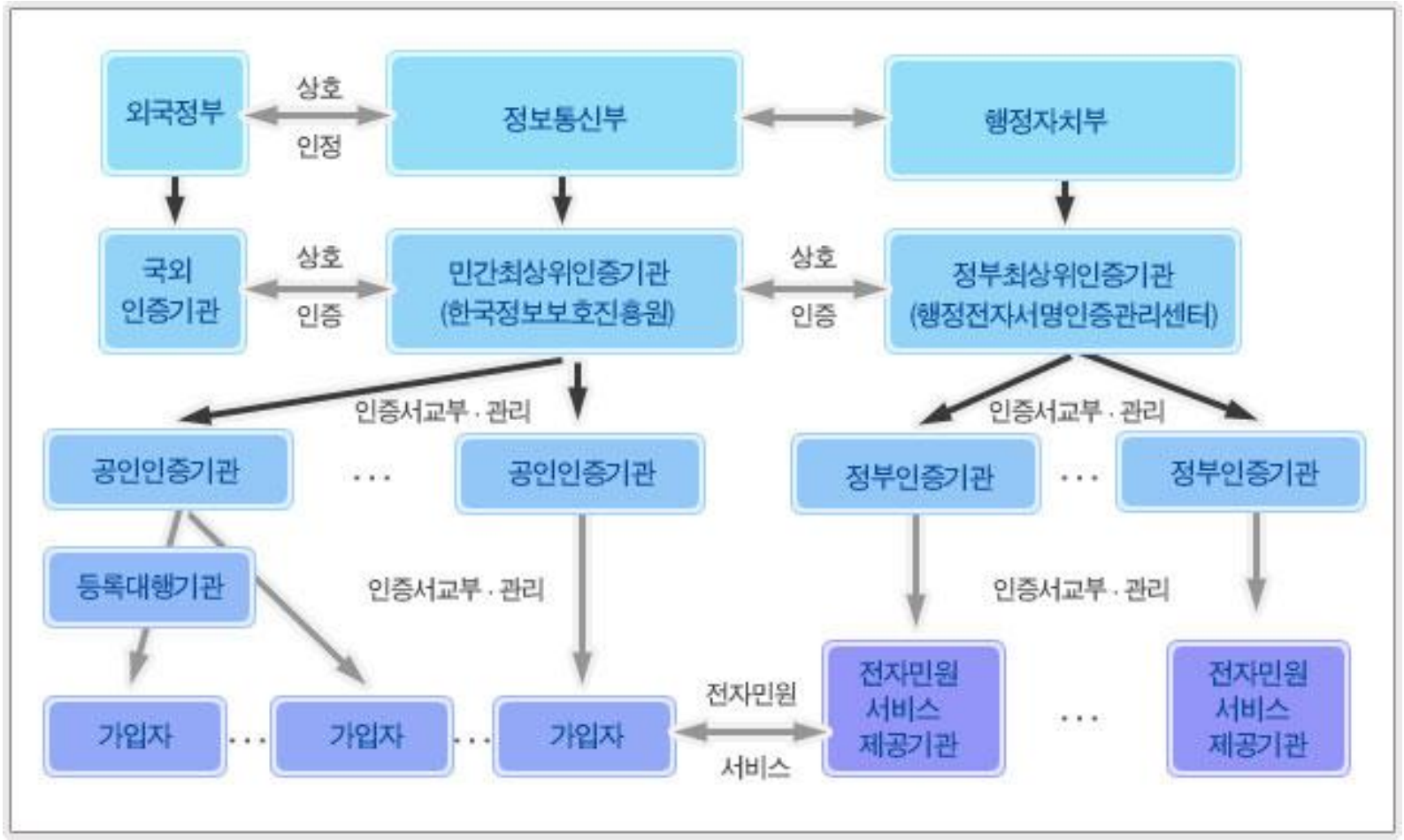
Network Structure

Certification Path



Korean PKI Structure

전자서명 인증관리센터
http://www.kisa.or.kr/kisa/kcac/jsp/kcac.jsp



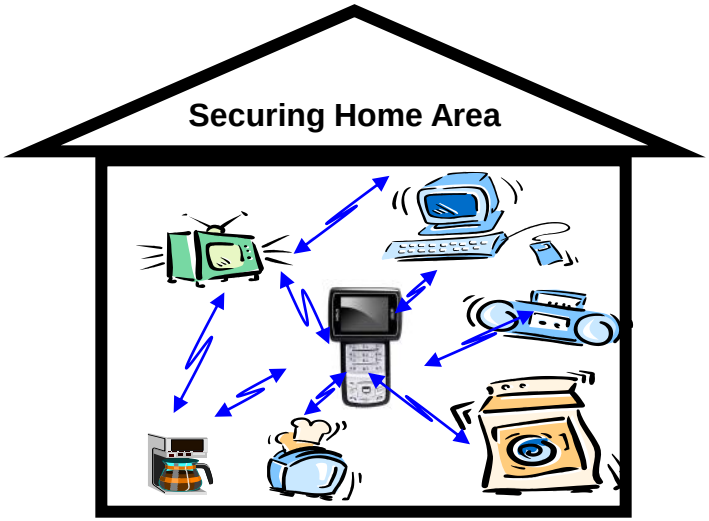
Korean PKI Structure

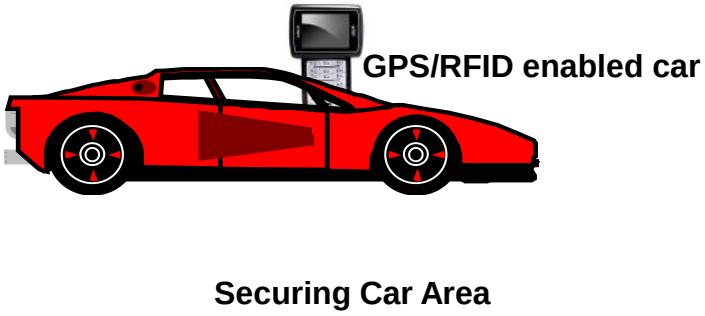
전자서명법 제4조의 규정에 의하여 지정된 공인인증기관

- 한국정보인증(주) http://www.signgate.com
- (주)코스콤 http://www.signkorea.com
- 금융결제원 http://www.yessign.or.kr
- 한국정보사회진흥원 http://sign.nca.or.kr
- 한국전자인증(주) http://gca.crosscert.com
- 한국무역정보통신 http://www.tradesign.net

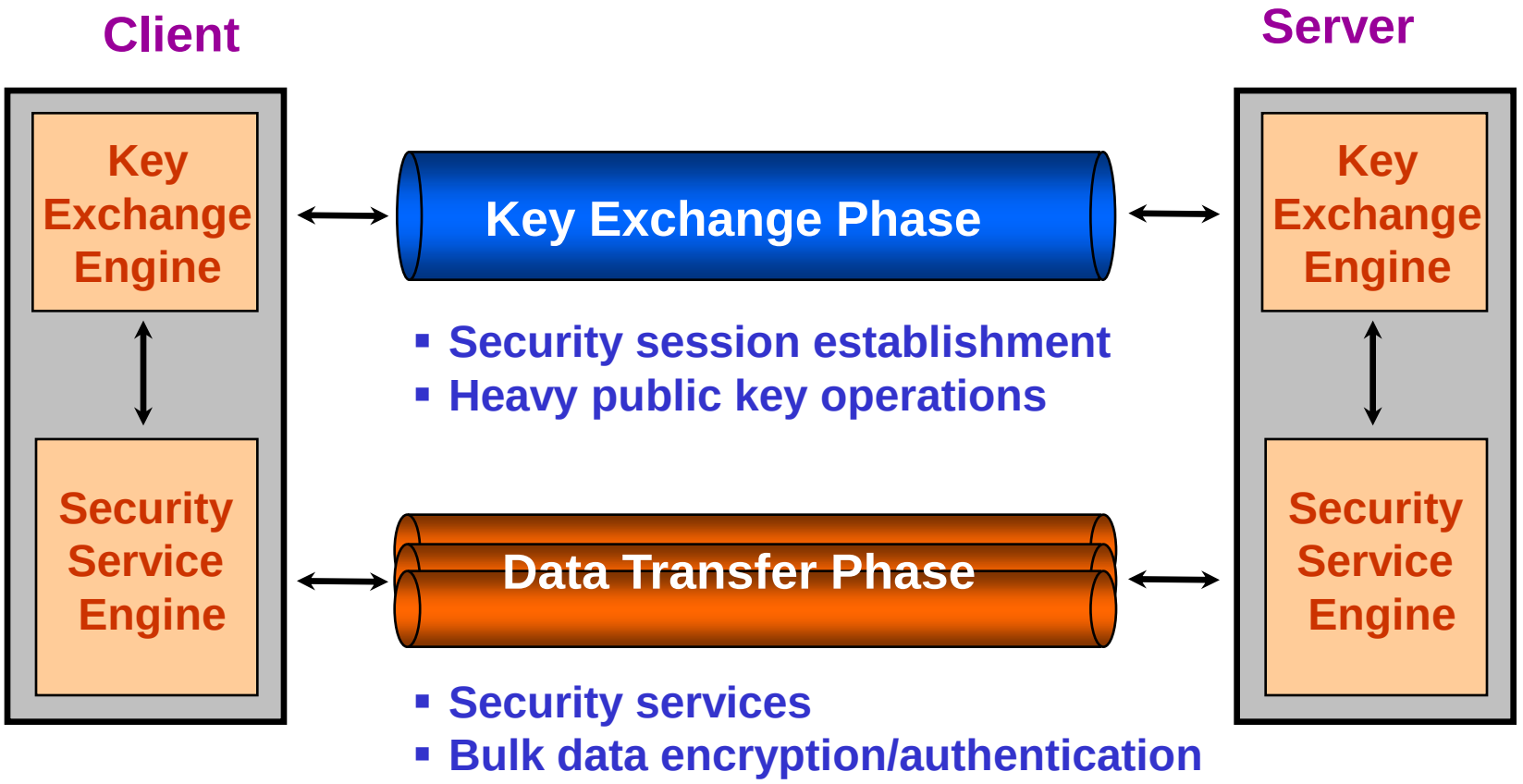
4. Communications Security

Lots of Communications





Communications Security Protocols



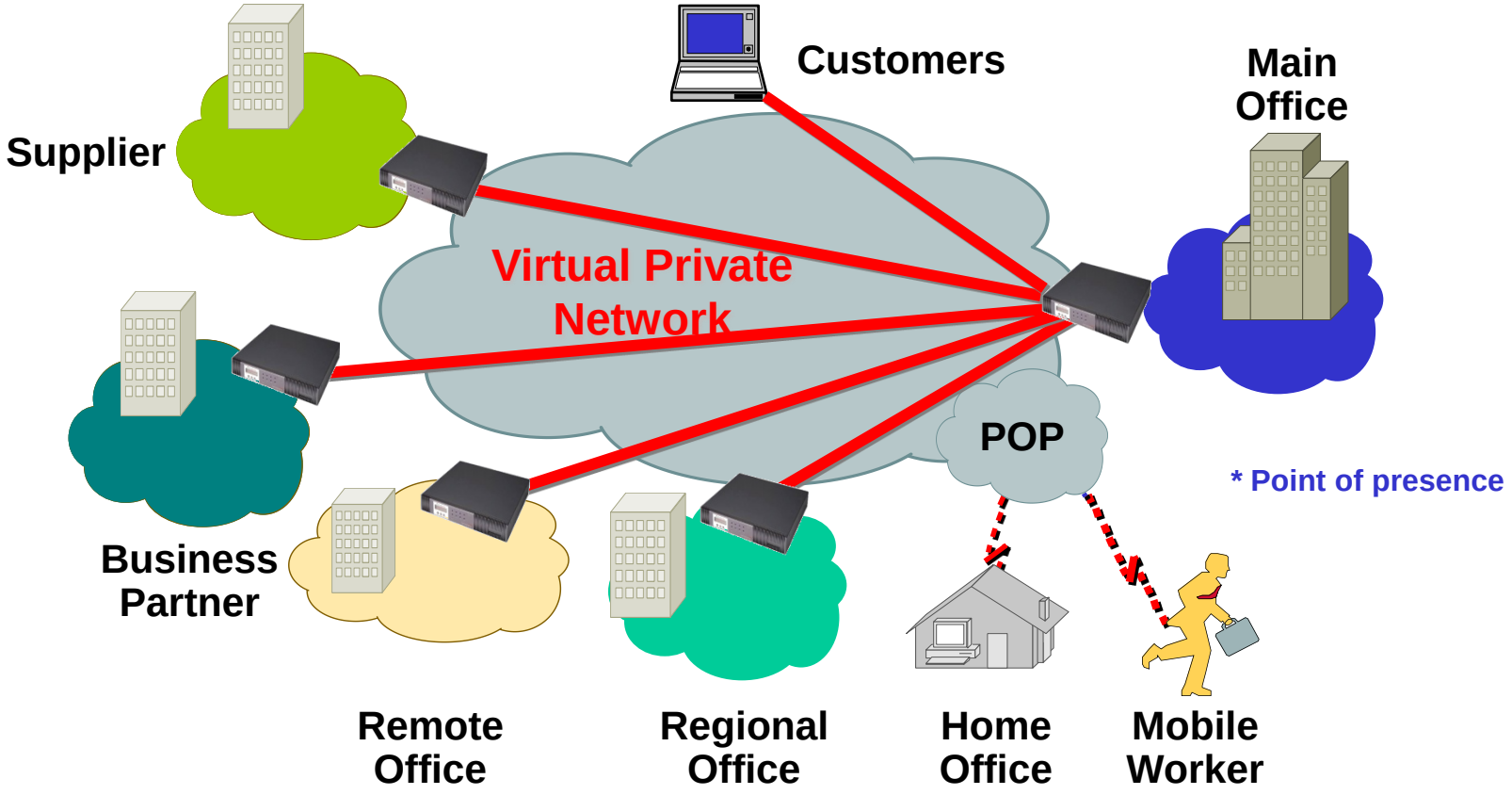
- Security session establishment
- Heavy public key operations

- Security services
- Bulk data encryption/authentication

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

Virtual Private Network (VPN)

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

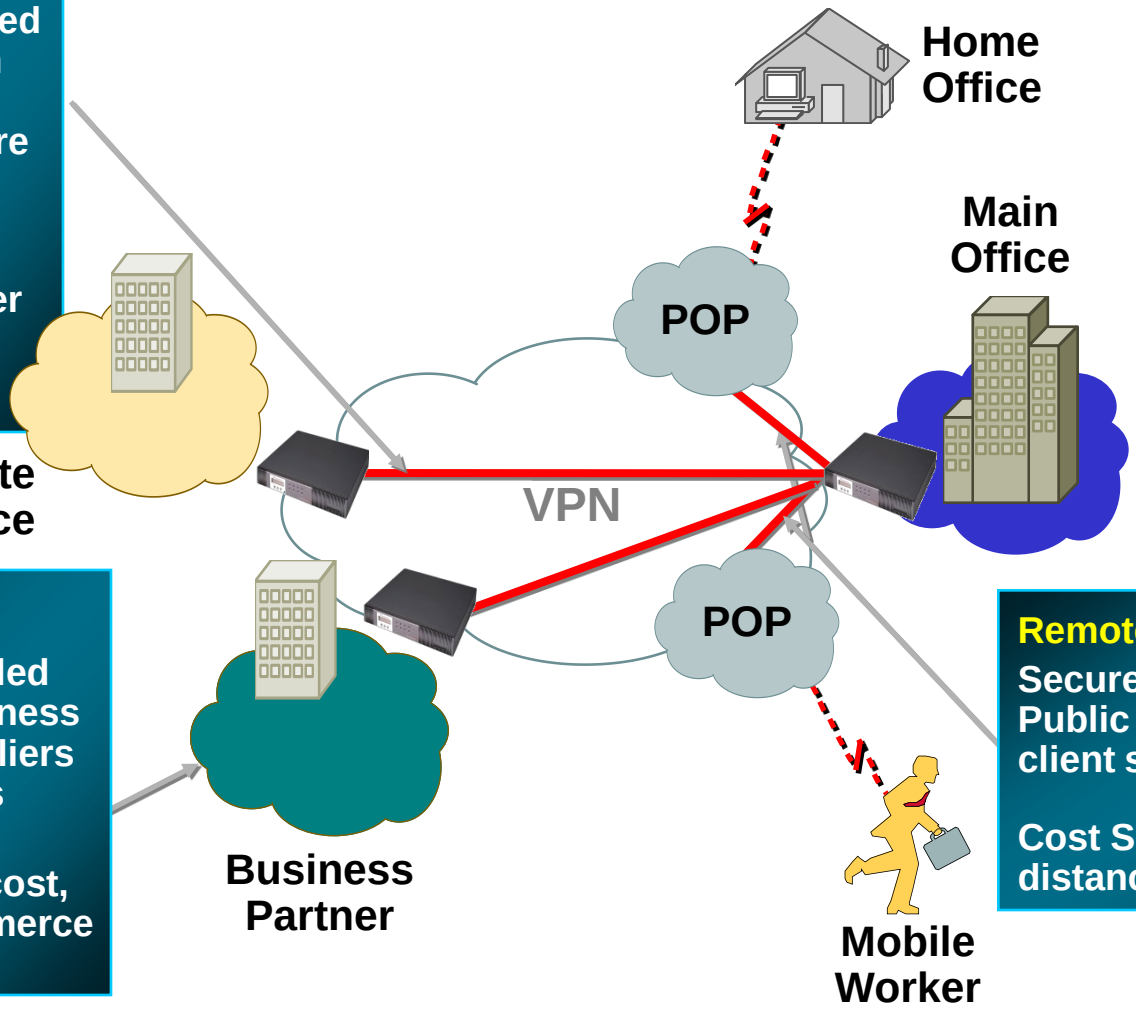


VPN Business Applications

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

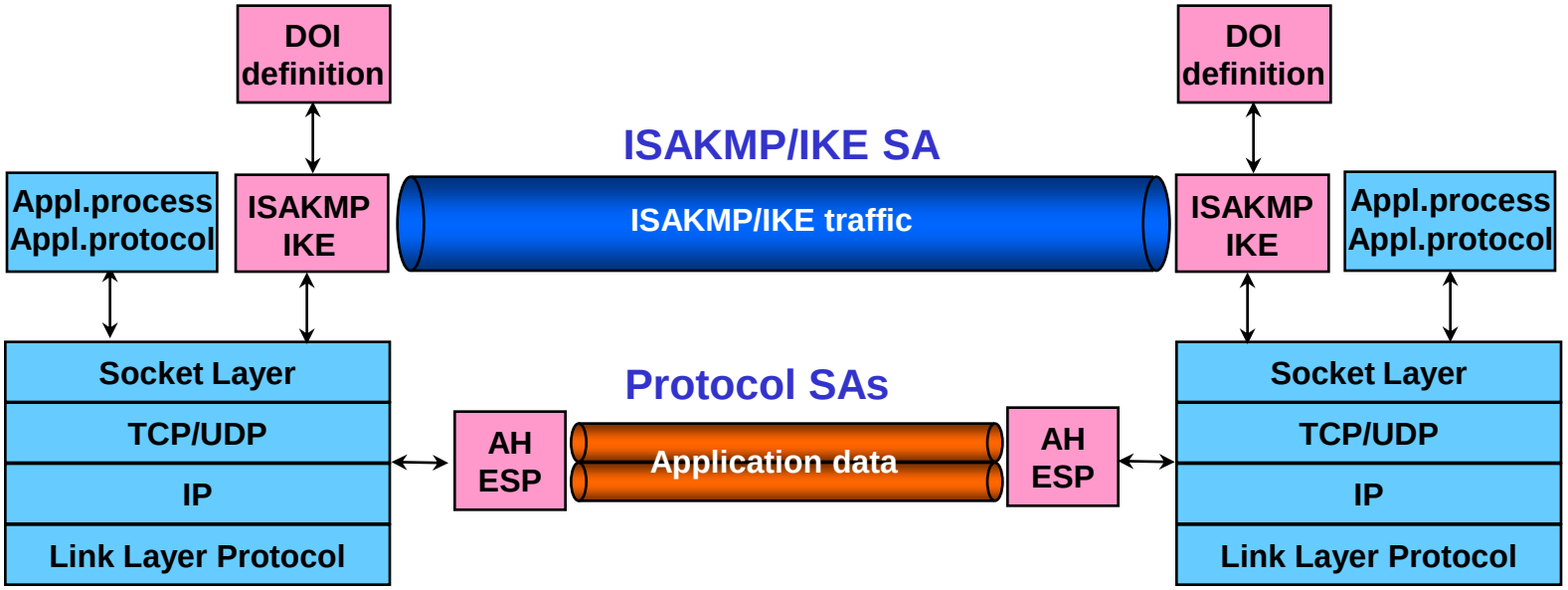
IPSec: IP-layer Security Protocol

- **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

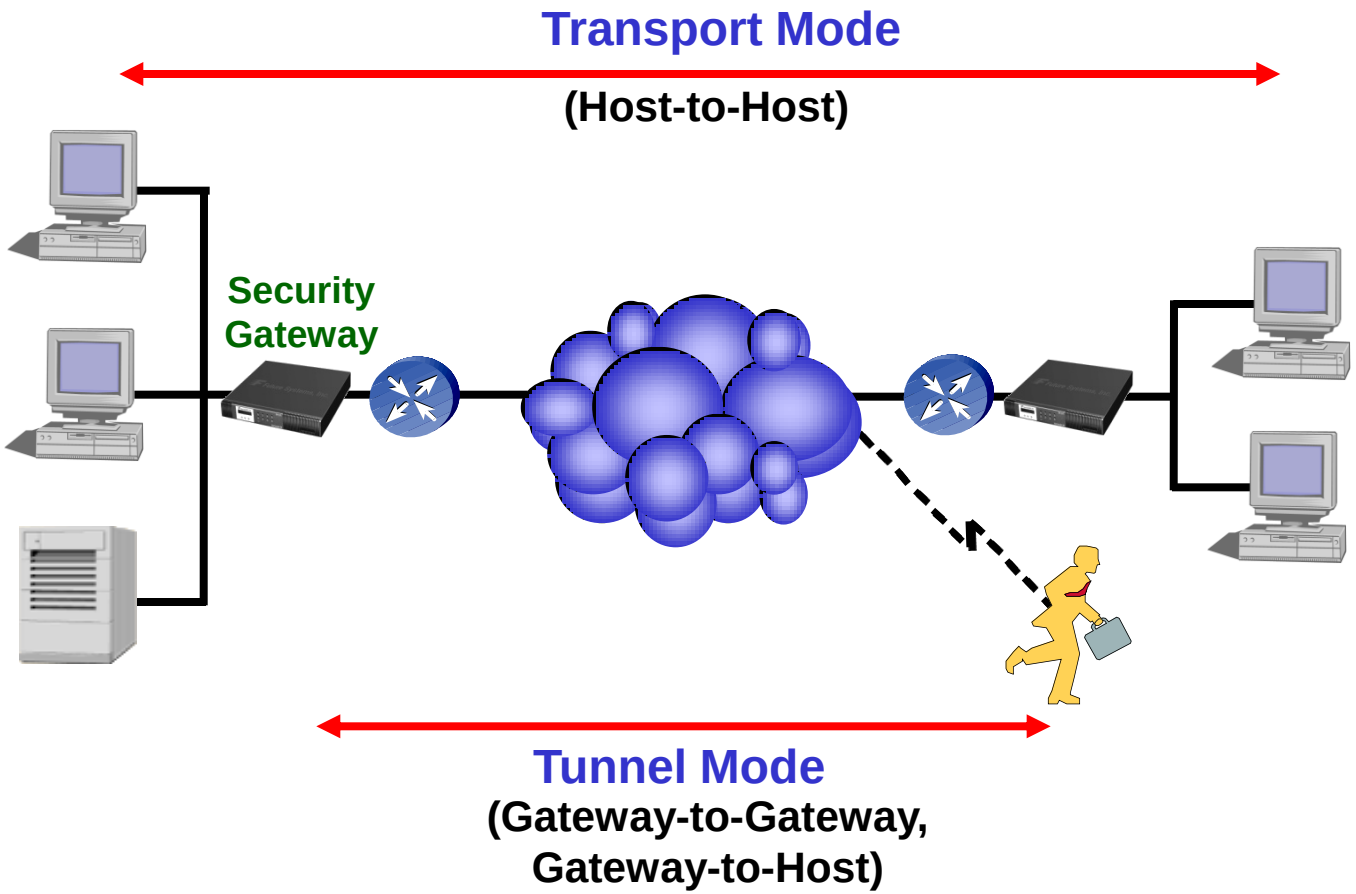


Phase I (ISAKMP SA) : SA negotiation between two ISAKMP servers

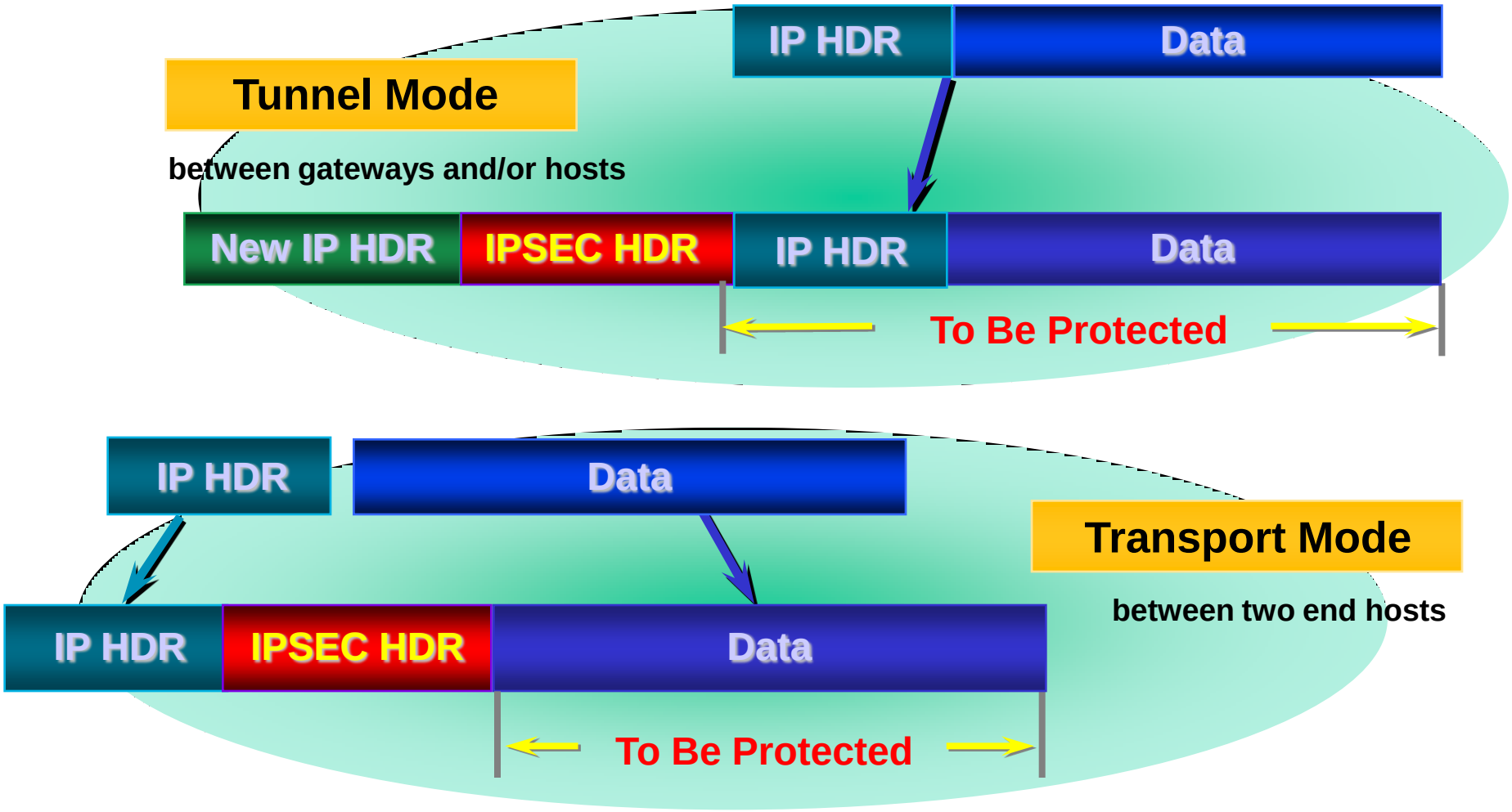
Phase II (Protocol SA) : SA negotiation for other security protocols (e.g., IPSEC AH) under the protection of ISAKMP SA

IPSec Mode of Operations

Transport Mode vs. Tunnel Mode



IPSec Mode of Operations

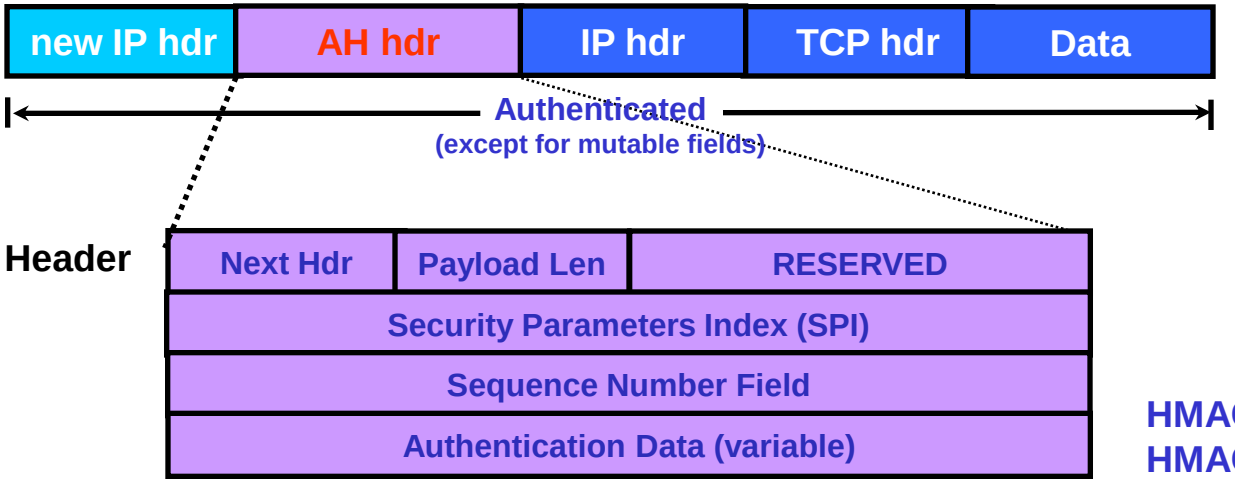


Authentication Header (AH)

Original IP Packet

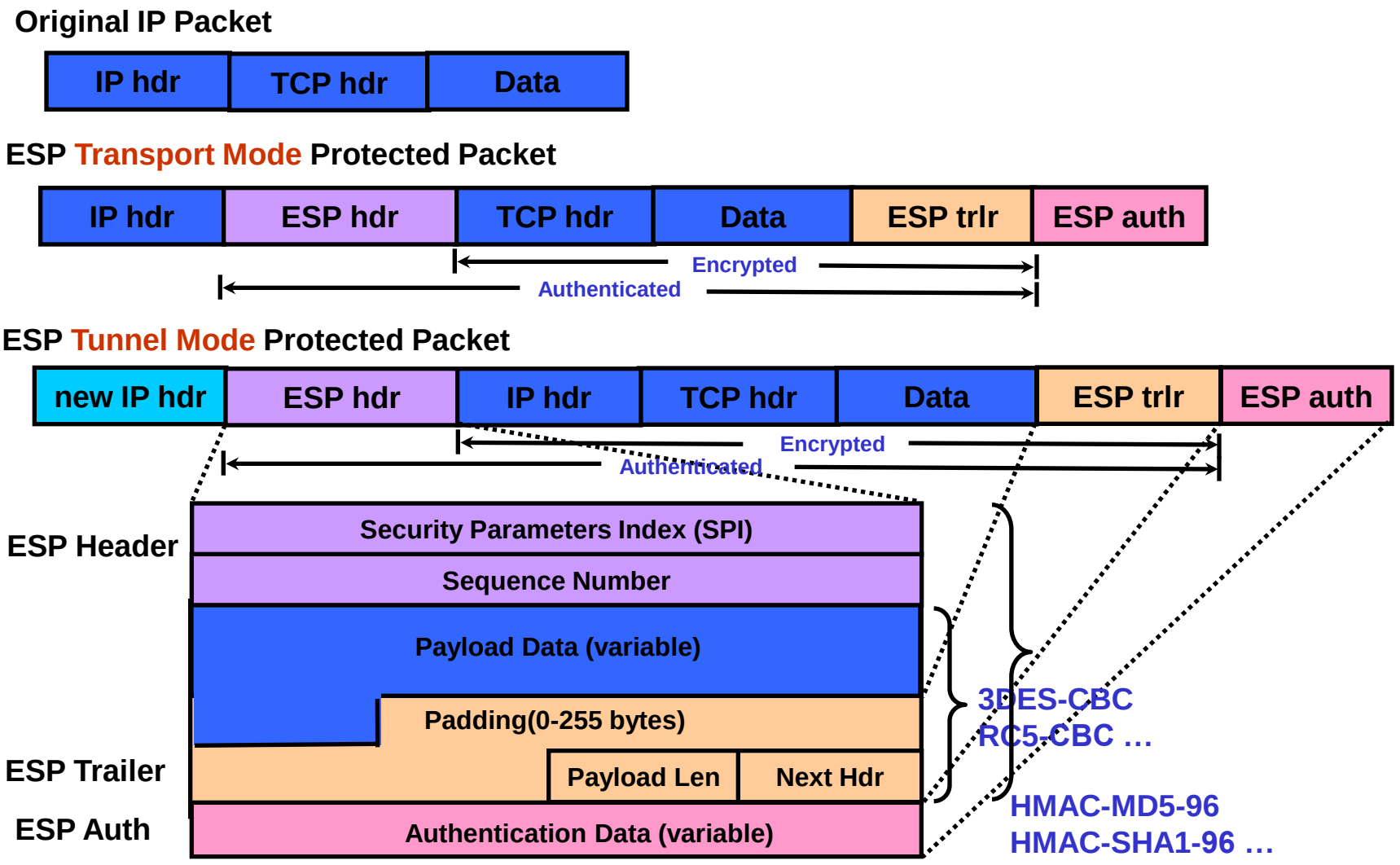
AH Transport Mode Protected Packet

AH Tunnel Mode Protected Packet

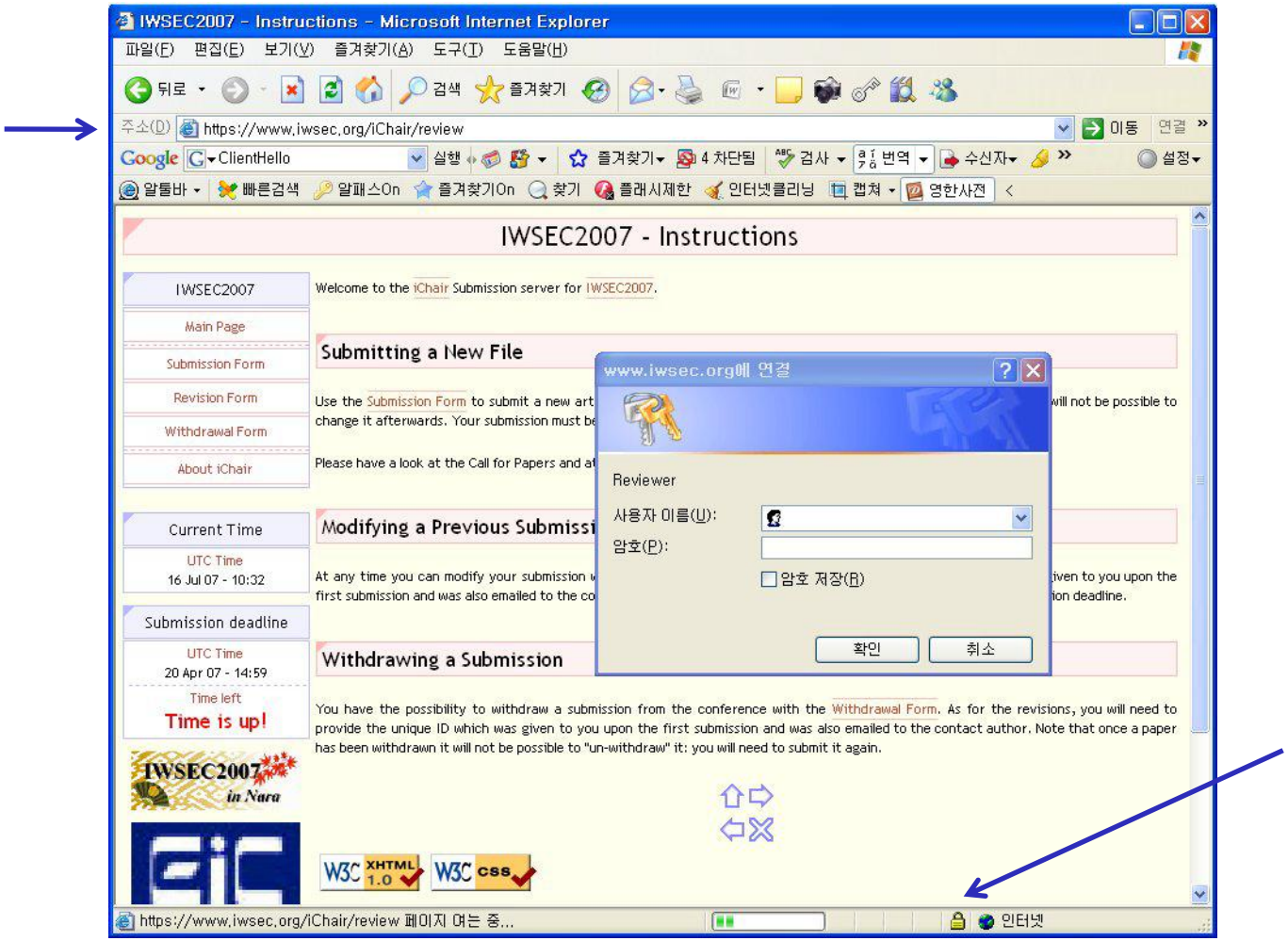


HMAC-MD5-96
HMAC-SHA1-96

Encapsulating Security Payload (ESP)



TLS: Transport Layer Security



Secure Sockets Layer (SSL)

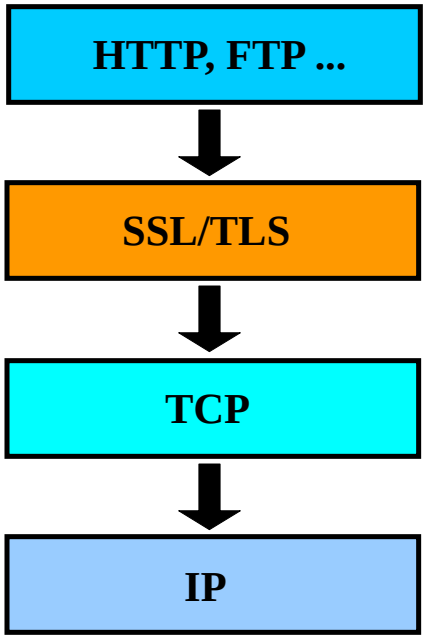
- Transport layer security to any TCP-based app. using SSL services.
  - used between Web browsers and Web servers for e-commerce (https).
- Security services:
  - server authentication
  - data encryption
  - client authentication (optional)

Transport Layer Security (TLS) Protocol

- **SSL/TLS**
  - Layered on top of reliable transport protocols, e.g., TCP
  - Application protocol independent
  - Record Protocol & Handshake Protocol

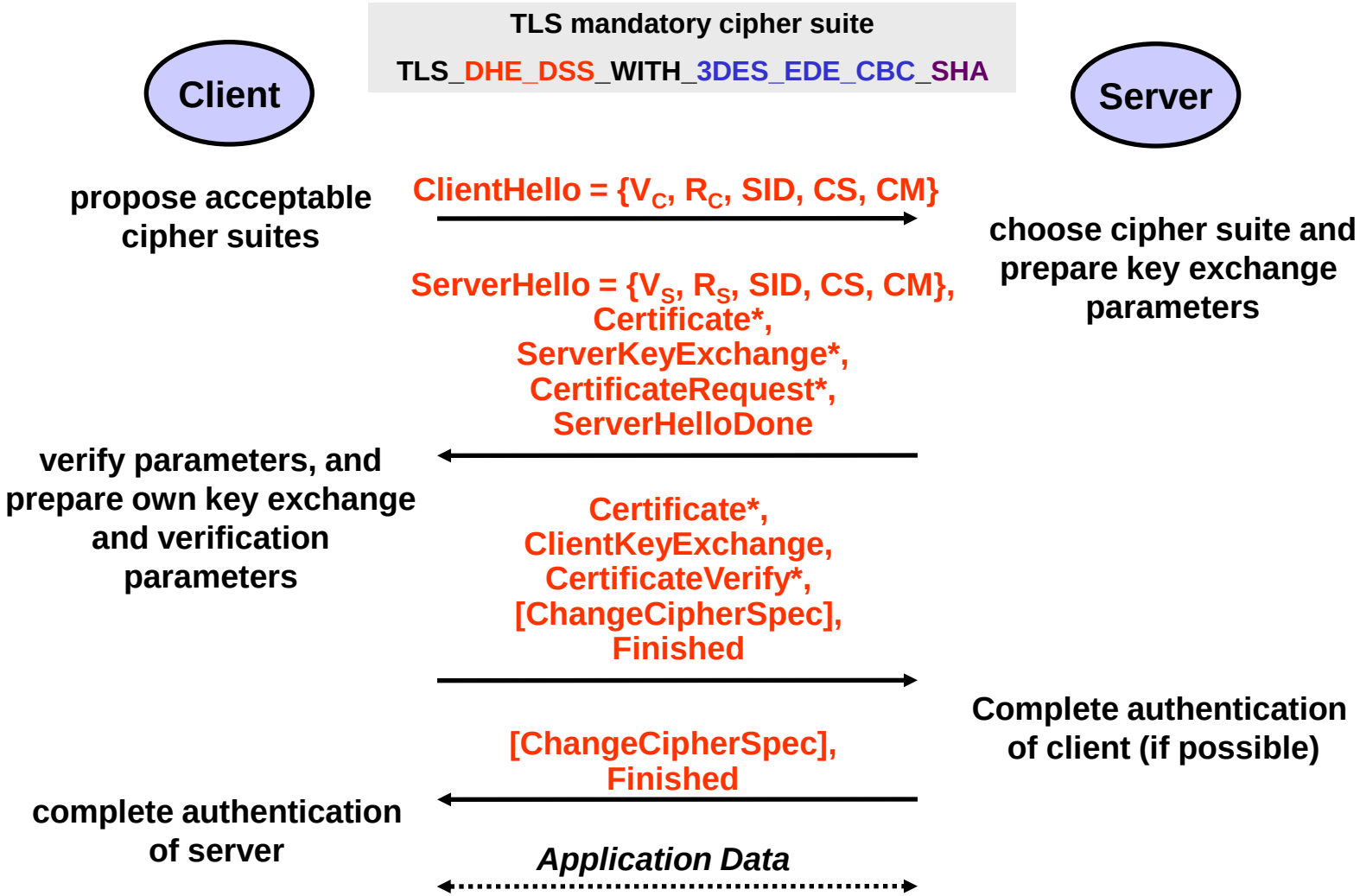
- **Record Protocol**
  - Encapsulation of higher level protocols
  - Data encryption using CBC block ciphers or stream ciphers
  - Data integrity using HMAC

- **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)

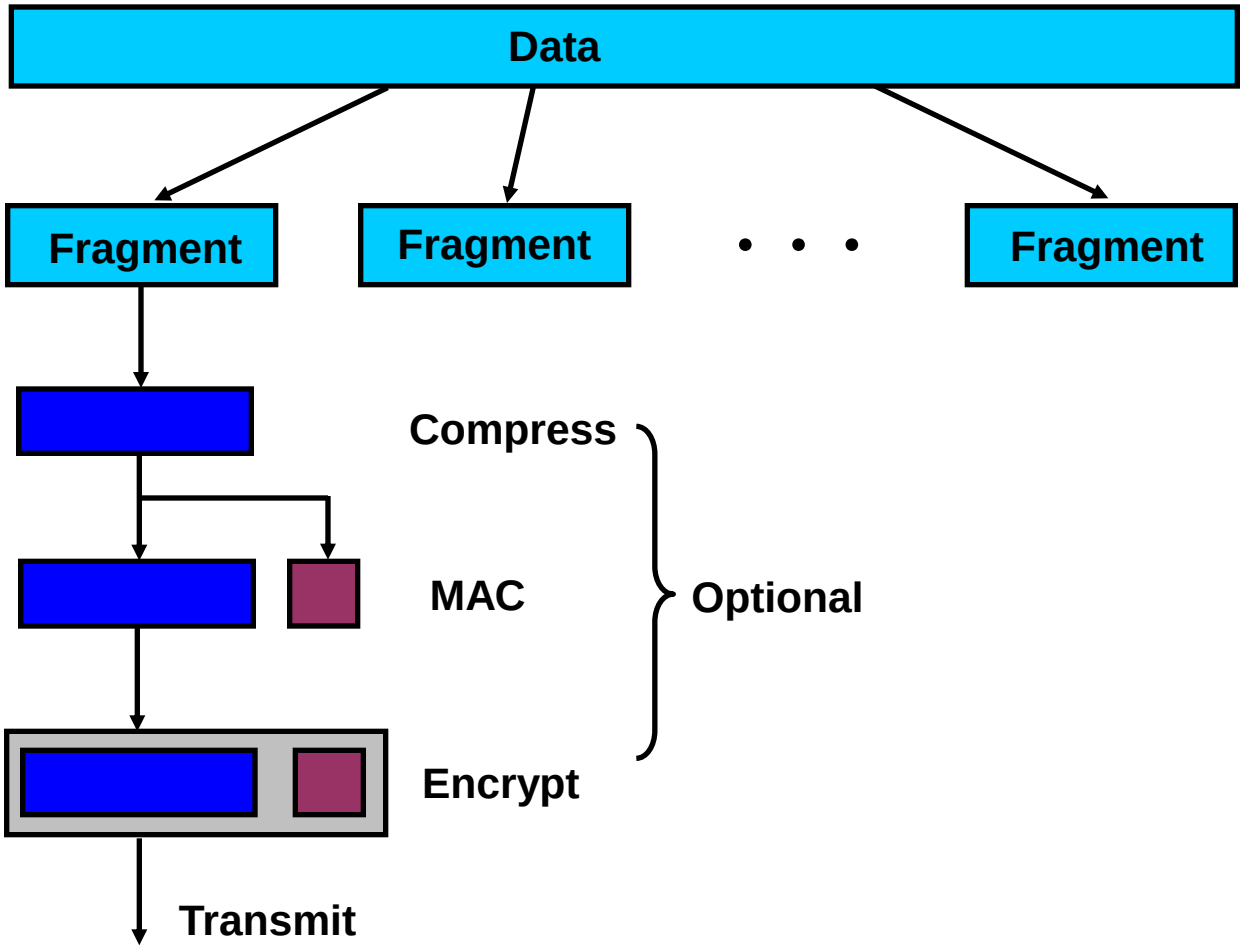


5 bytes

TLS Full Handshake



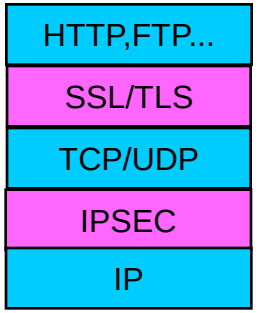
TLS Record Protocol



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)

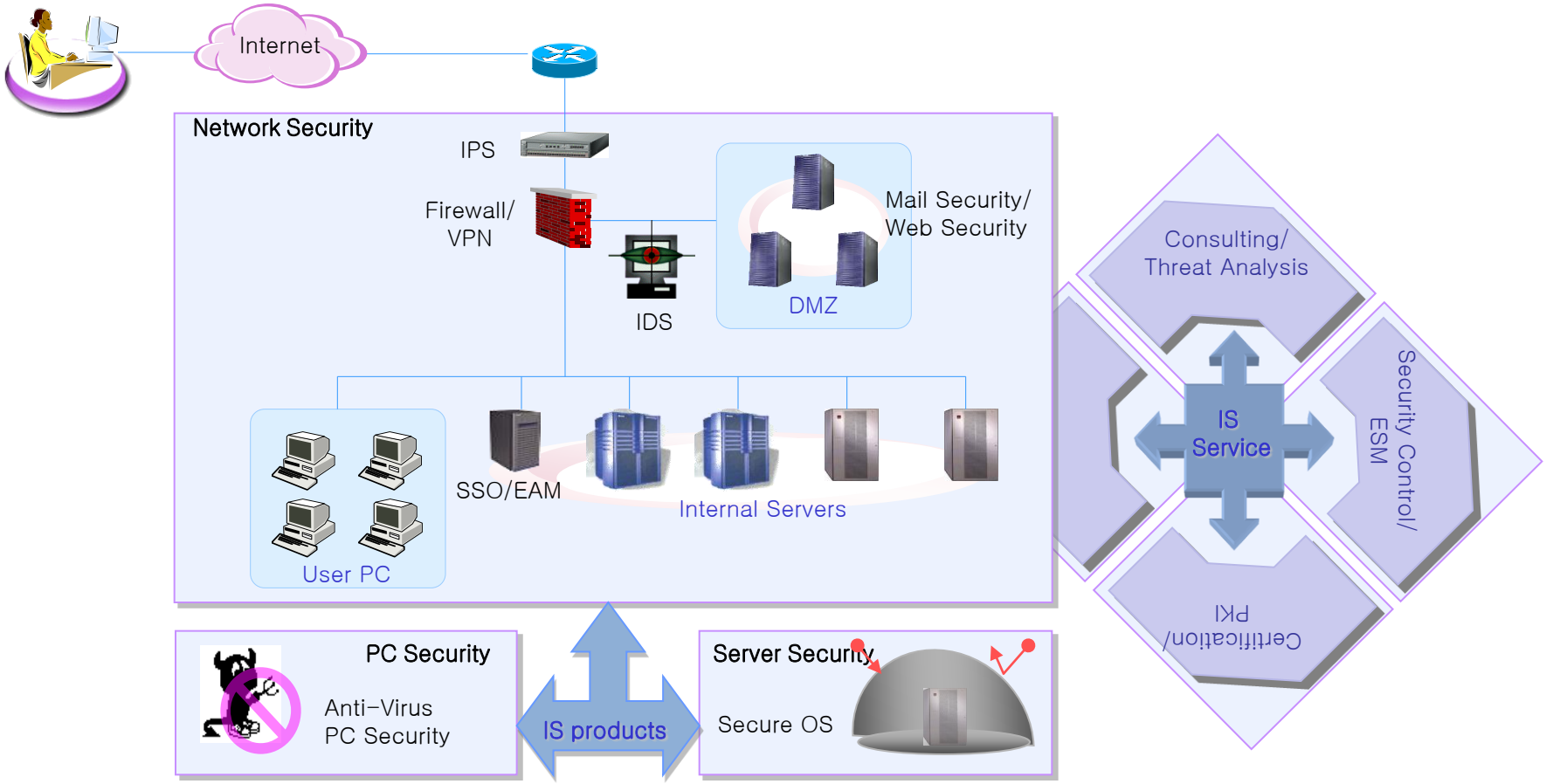


SSL/TLS

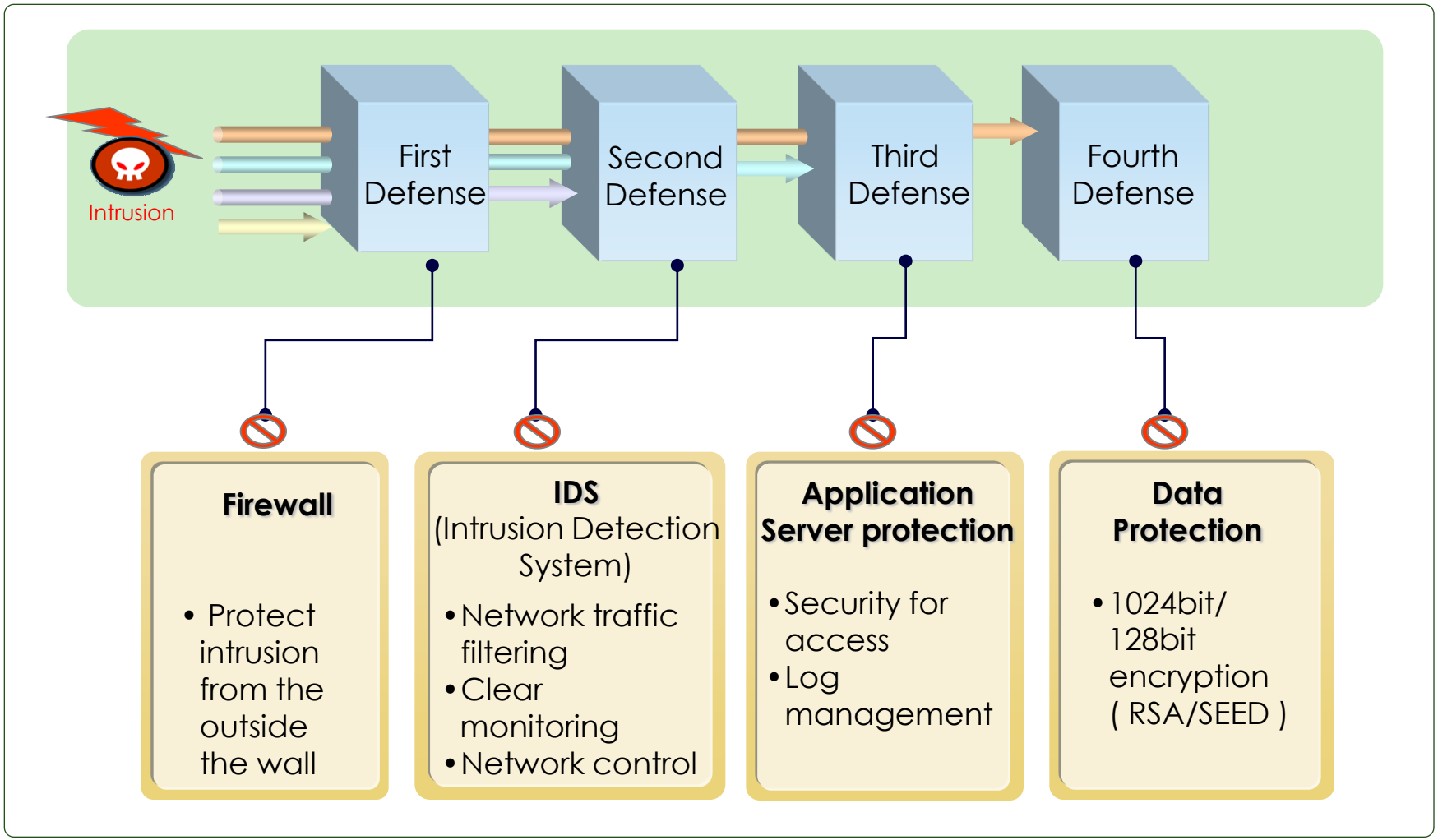
- Transport layer security protocol
- Confidentiality, Integrity, Authentication (usually client-to-server only)
- Works only with TCP (not UDP): HTTP, SMTP, POP3, NNTP, FTP, LDAP…
- Minimal changes to applications
- Client-Server model: Host-to-Server (secure Web transactions)
- Free : built in to nearly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

5. Security Management

Corporate Information Security



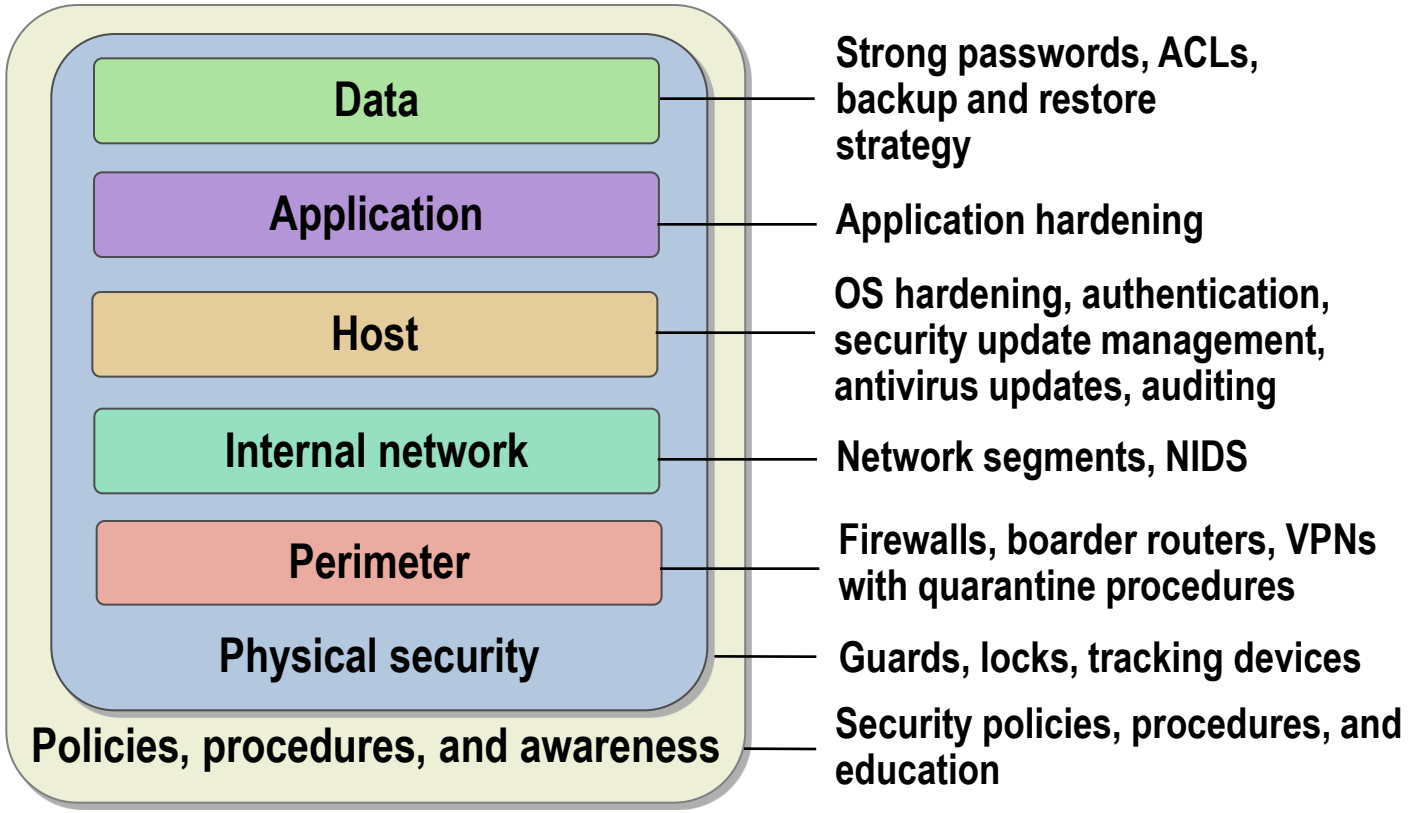
Simplified Security Diagram



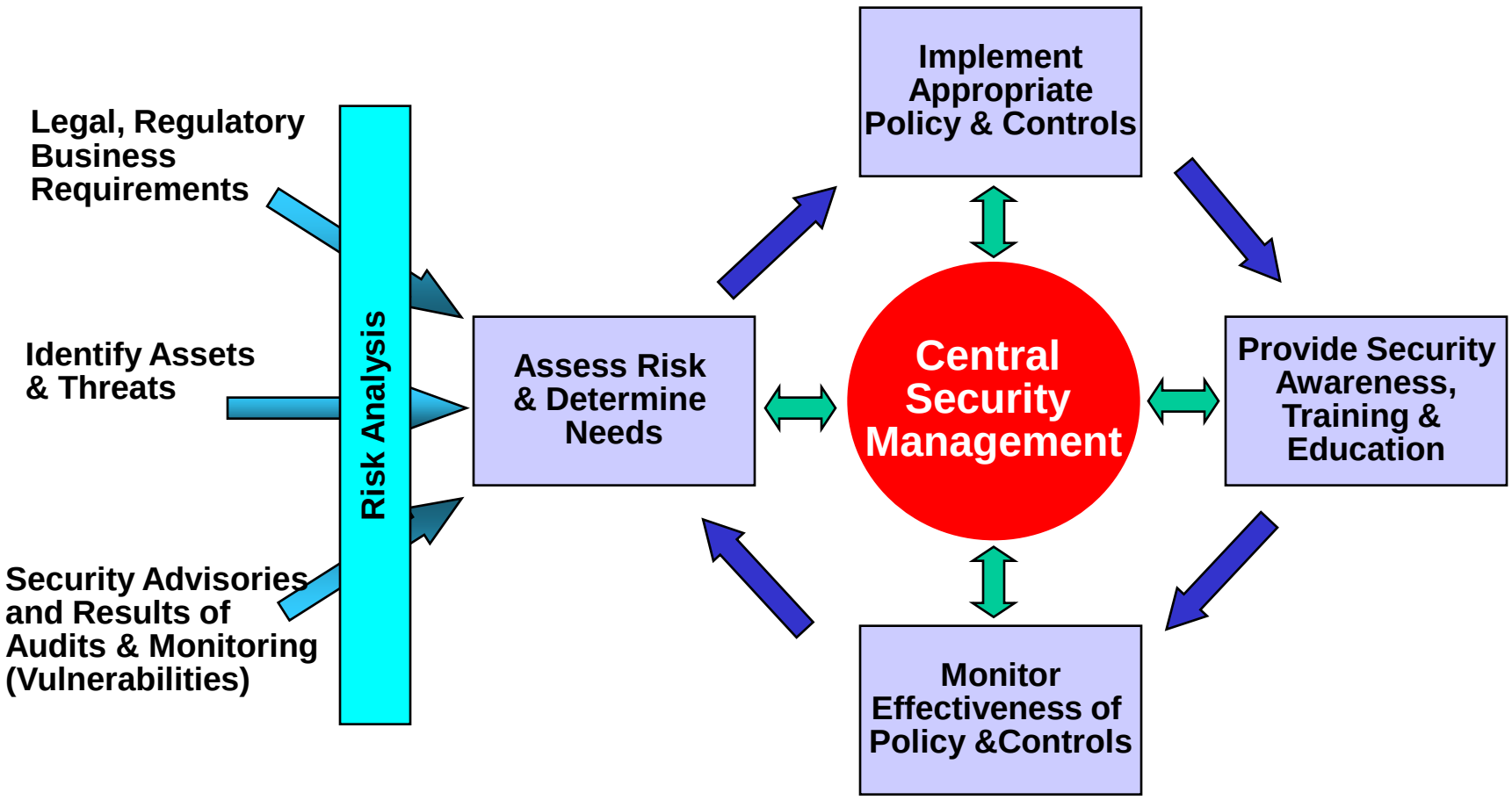
Understanding Defense-in-Depth

Using a layered approach:

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



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

Q & A

Thank you!