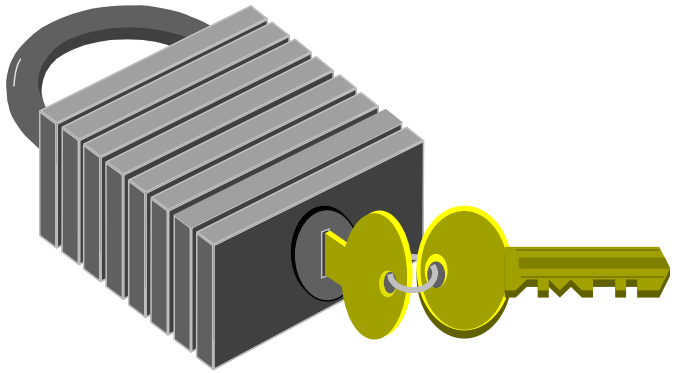
Internet Security



ECET 4840

Outline

- A Few Basic Concepts
  - Typical Client-Server Model
  - Reference Model
  - IPv4 Header Capture
  - IPv6 Architecture
  - TCP Header Capture
  - Demo (Services and Port)
  - Security Attacks & Services
  - Demo (Passive Attack)
  - Intruders and Embedded Programs
  - Demo (Antivirus)
- Cryptography and Authentication
  - Group Exercise (Crack the Code)
  - Public-Key Cryptography
  - Digital Signatures
  - Digital Certificates (CAs and the X.509 Standard)
  - Demo (Digital Certificate)
  - IPSec

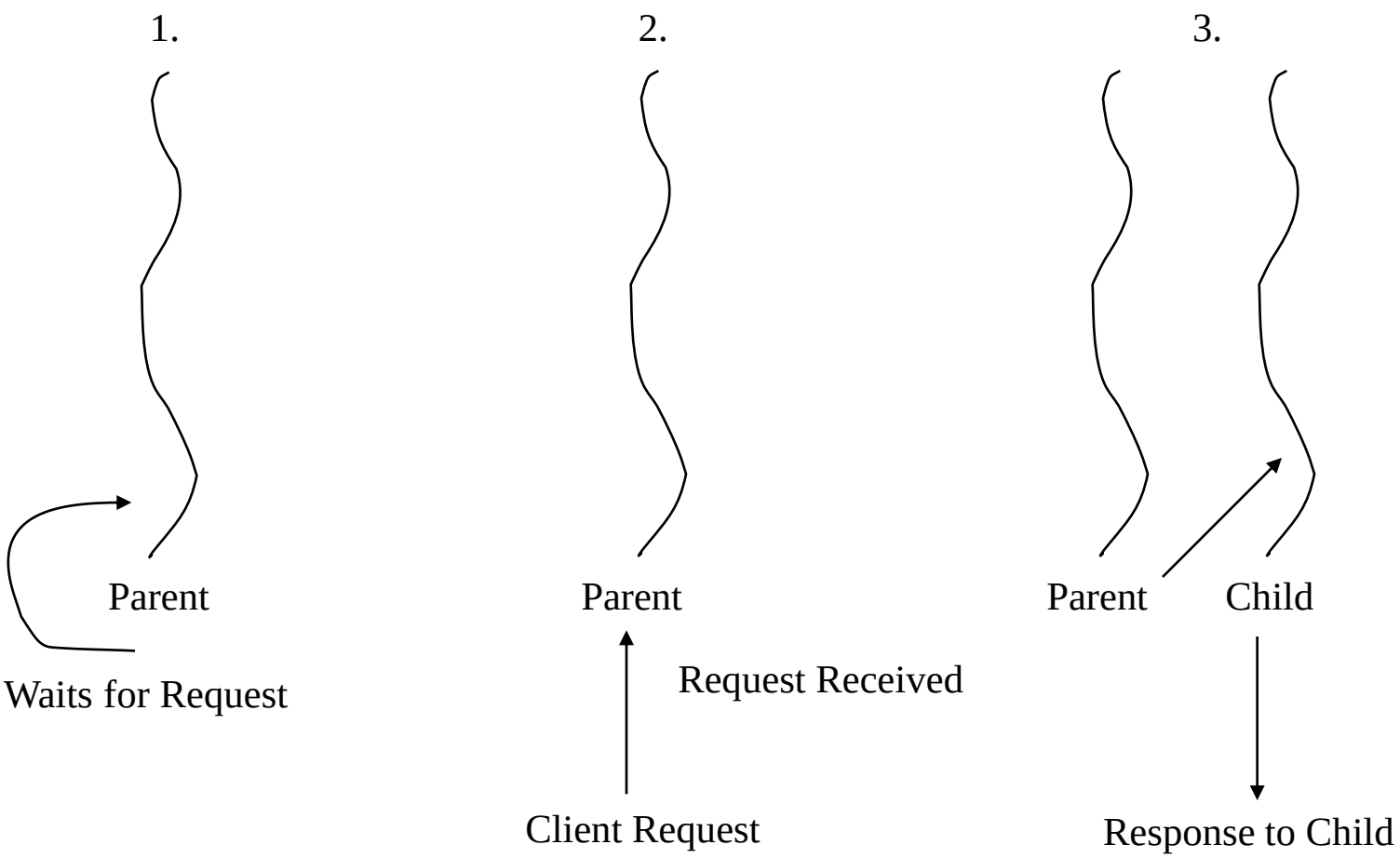
Internet Security

Outline

- Services Security
  - Login and FTP
  - Email Security
    - PGP (Pretty Good Privacy)
    - S/MIME (Secure Multipurpose Internet Mail Extension)
  - Web Security
    - Security Threats
    - SHTTP (Secure HTTP)
    - SSL (Secure Sockets Layer)
    - Java and ActiveX Issues
    - Demo (Java Applet)
    - Cookies
  - Firewalls
    - Packet Filtering
    - Application-level Gateway
    - Circuit-level Gateway
    - Bastion Servers
  - Addendum: Suggested Resources

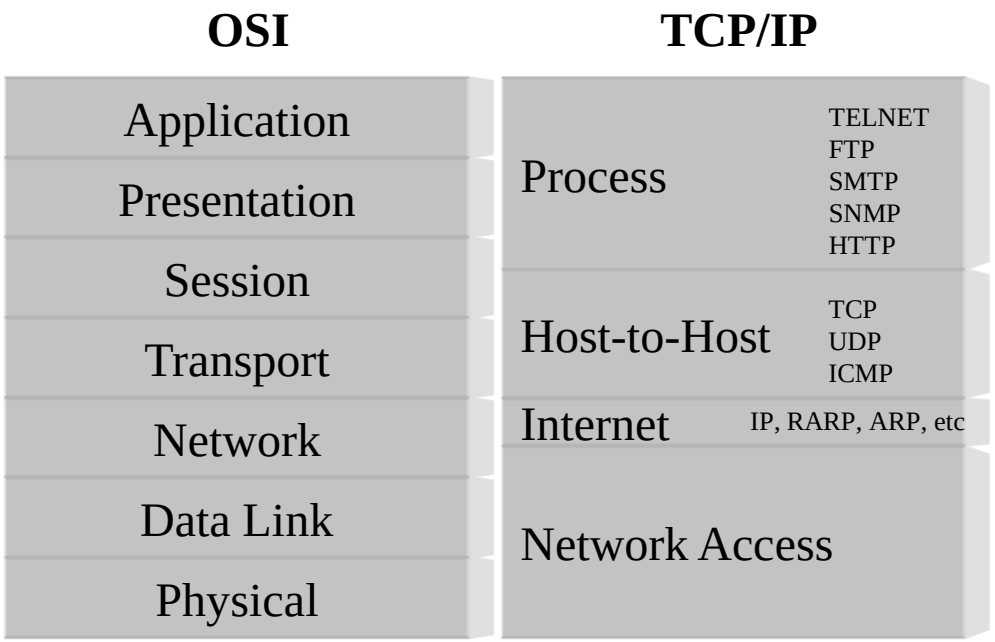
A Few Basic Concepts

Typical Client-Server Model



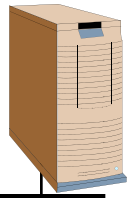
A Few Basic Concepts

Reference Models



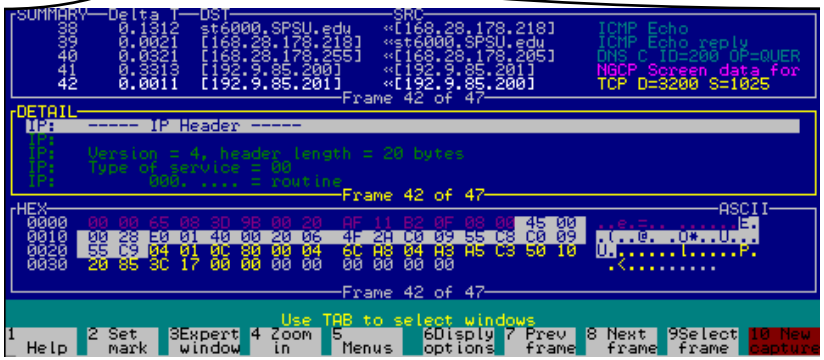
IPv4 Header Capture

Source = 192.9.85.200



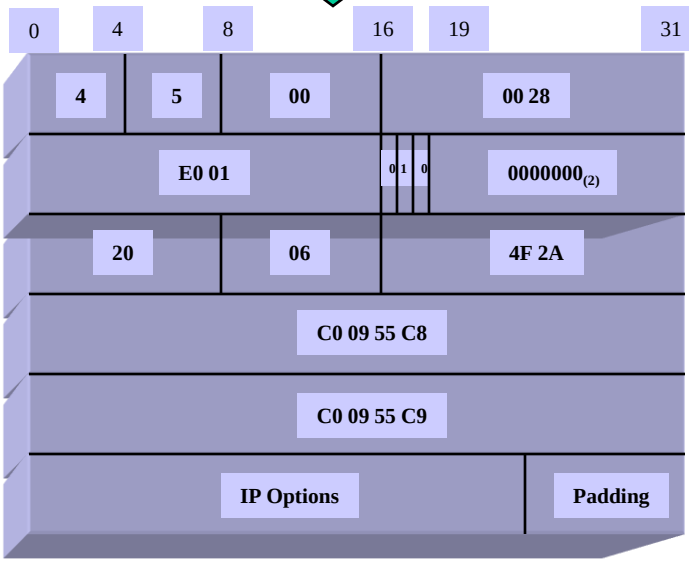
Destination = 192.9.85.201

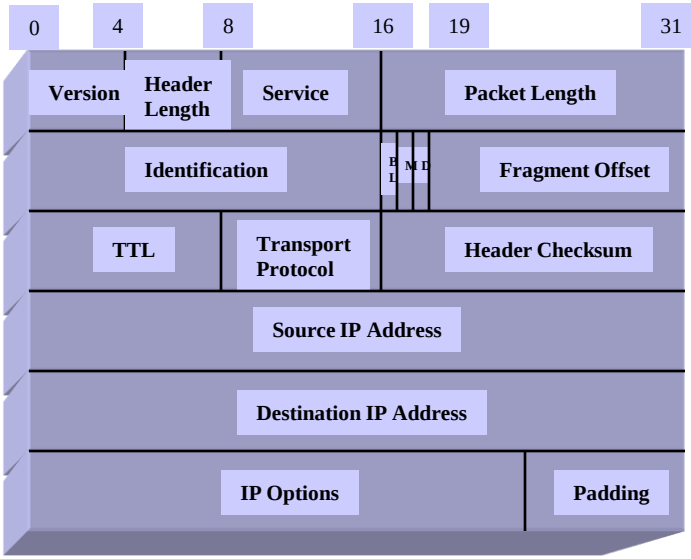
1



2

3

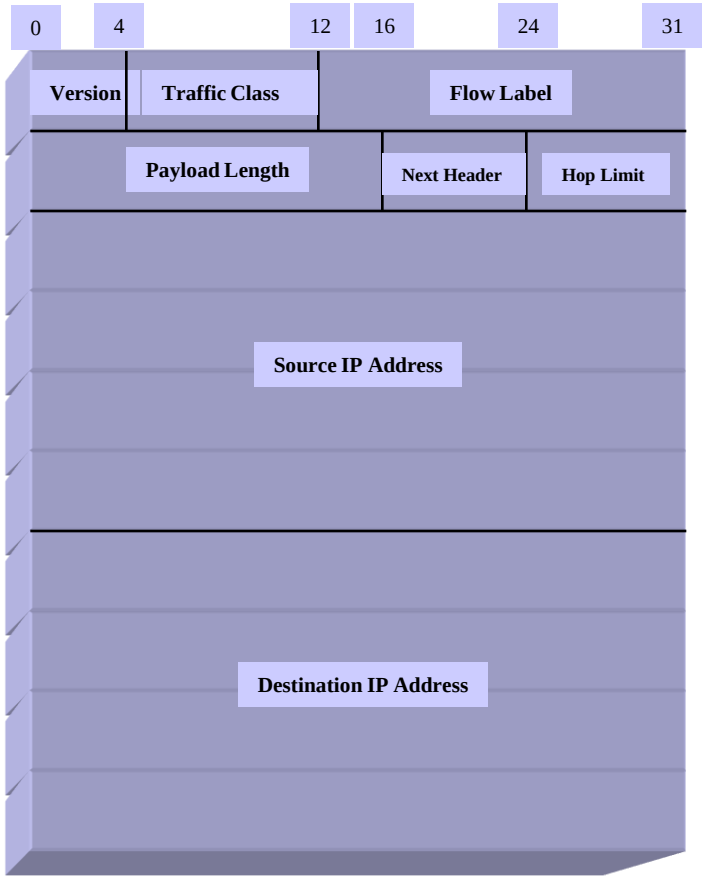




4

A Few Basic Concepts

IPv6 Architecture

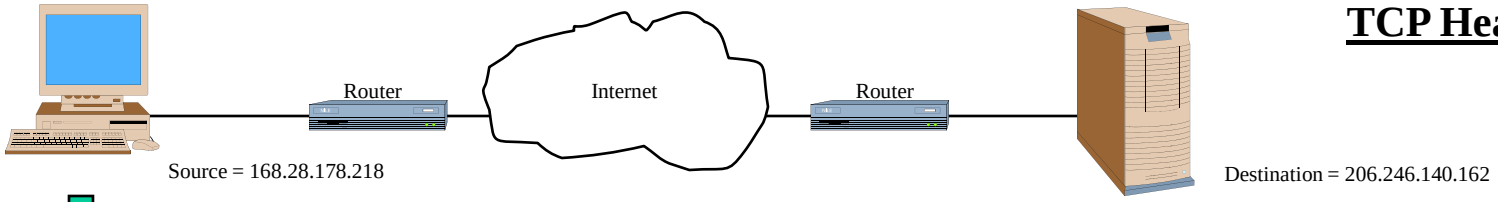


- Version: IP version 6
- Traffic Class: packet's class or priority
- Flow Label: special handling instructions
- Payload Length: packet - IPv6 header (bytes)
- Next Header: IPv6 extension or Layer 4
- Hop Limit: maximum hop count
- Source Address: sender's address (128 byte)
- Destination Address:recipient's address (128 bytes)
- Note - IPv6 can employ the following optional extension headers: Hop-by-Hop Header, Routing Header, Fragment Header, Authentication Header, Encapsulating Security Payload Header, and Destination Options Header.

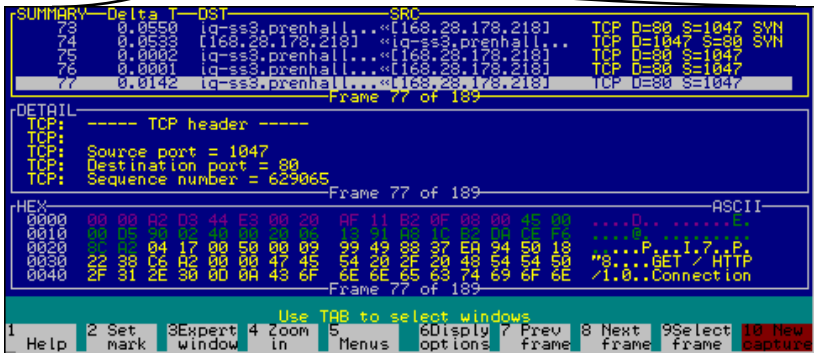
Southern Polytechnic State University (SPSU)Workstation

Prentice Hall Web Server

TCP Header Capture

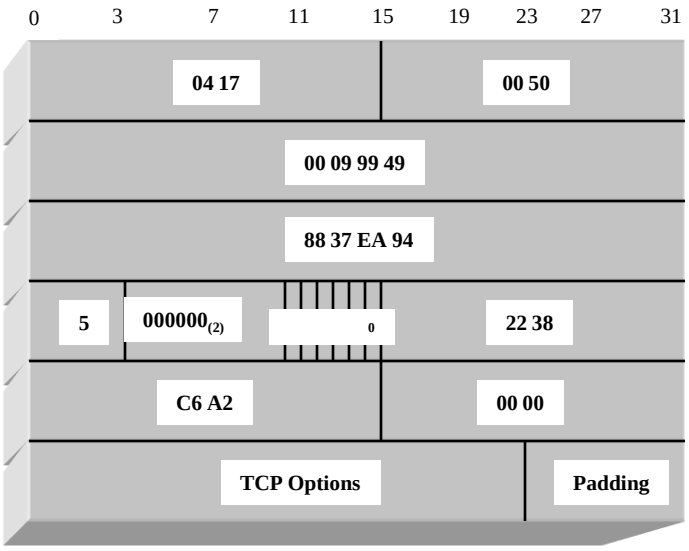


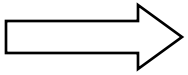
1

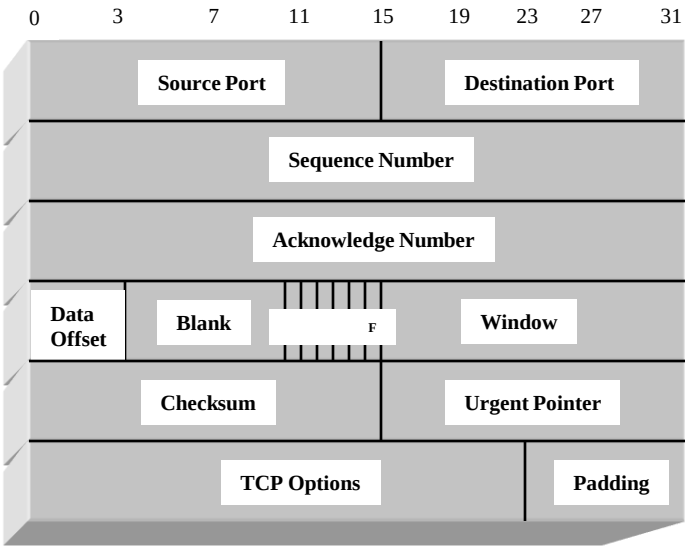


2

3







4

A Few Basic Concepts

Security Attacks

- Passive Attacks - intercept transmitted information
  - Message Content Interception
  - Traffic Analysis
- Active Attacks - modify data stream or create false data stream
  - Denial of Service (DoS) - disabling of services or network facilities in order to prevent normal operation
  - Replay - passive capture of a transmission in order to use it in an unauthorized manner
  - Message Modification - passive capture of a transmission(s) in order to modify its contents, sequence position, etc. so that it may be used in an unauthorized manner
  - Masquerade - pretending to be a different source either by using unauthorized network configuration information or captured transmissions.

A Few Basic Concepts

Security Services

- Access Control- the assignment of access rights to an individual or group account via means of authentication
- Service Availability - service access, reliability, and uptime
- Integrity - information is received in the identical form in which it was sent
- Confidentiality - protection of information while en route
- Authentication - verification that information (user and data) is from claimed source
- Nonrepudiation - the prevention of transmission denial from sender or receiver

A Few Basic Concepts

Intruders and Embedded Programs

- Intruders are generally referred to as hackers or crackers, whose network access intentions range from benign to malevolent. Access is usually gained by exploiting operating system or application weaknesses; this activity is known as hacking.
- To crack password files, crackers try: system default passwords, user information, short passwords (3 characters or less), online dictionaries, phone numbers, office numbers, license numbers, line taps, and Trojan horses
- Intrusion detection techniques include:
  - Statistical Anomaly
  - Rule-based Detection
- Audit records are required as input to all detection-based systems. Such records are usually maintained found in operating system or detection-specific log files. Auditing tool examples: Windows NT (C2CERT, Event Viewer, and Kane Security Analyst) and Unix (Tripwire, Tiger, Portmaster, Syslog, Forensics)
- Hacker tools bear names such as: SATAN, sscan, Mscan, stealth port scanner, Netcat, Nmap, L0pht Crack, L0pht AntiSniff, Ping O' Death, Sneakin, Loki, Scotty, Strobe, ISS, queso, curl, SSLeay/upget, Sam Spade, eEye IIS Hack, Reverse Telnet, Tone Loc, Qtip, Juggernaut, cgiscanner, Pandora, Chainsaw, Linsniff, DumpReg, DumpAcl, IP Network Browser, Back Orifice 2000 (BO2K).

A Few Basic Concepts

Intruders and Embedded Programs - continued

- TCP/IP and Unix-based utilities/applications that can be used by a hacker include: traceroute, ping, finger, WHOIS, nslookup, Telnet, FTP, SMTP, HTTP, r-based commands (e.g. rsh, rcp, rwho, rlogin), tftp, and more.

- Embedded Programs are categorized as either host dependent or host independent. Host dependent programs are parasitic in nature and must be appended to a previously healthy host file; they are activated only when the host program is running. Host independent programs are self-contained; they are usually activated at a prescheduled time or concurrently with a specific event (e.g. the day after the author's last paycheck). They also self-replicate.
  - Host dependent:
    - Trap door
    - Trojan Horse
    - Logic bombs

A Few Basic Concepts

Intruders and Embedded Programs - continued

- Viruses: a self-replicating segment of malicious code that attaches itself to an otherwise trusted program (e.g. the Melissa virus that affects Microsoft Outlook Express).
  - All viruses go through four phases: dormant, propagation, triggering, and execution.
  - Types of Viruses: stealth, polymorphic, boot sector, memory-resident, macro, and parasitic.
  - Antiviruses require periodic updates of their virus database (signatures and removal or quarantine procedures). Examples include: Norton Antivirus, MacAfee, and Fprot.
  - IBM's Digital Immune System

– Host independent:
  - Viruses
  - Worms
  - Bacteria

Cryptography and Authentication

Public-Key Cryptography

- First introduced in 1976 in a paper entitled “New Directions in Cryptography” by Whitfield Diffie and Martin Hellman
- Conventional, or symmetric, cryptosystems use a single key to encrypt and decrypt messages, whereas public-key, or asymmetric, cryptosystems use two complementary keys (public and private) to encrypt and decrypt messages.
  - Conventional Algorithms:

Algorithm	Key Size (bits)	Application
DES (Data Encryption Standard)	56	SET, Kerberos
Triple DES	112 or 168	PGP, S/MIME
AES (Advanced Encryption Standard)	128, 192, 0r 256	SET, Kerberos
IDEA (International Data Encrpyt)	128	PGP
Blowfish	upto 448	
RC5	upto 2048	
CAST-128 (Carlisle Adams & Stafford Tavares)	40 to 128	PGP
CAST-256 (Carlisle Adams & Stafford Tavares)	256	PGP
SkipJack	80	Clipper Chip

  - Public-Key Algorithms:

Algorithm	Key Size (bits)	Application
RSA (Ron Rivest, Adi Shamir, and Len Adleman)	upto 2048	key ex., A/E
Diffie-Hellman	upto 2048	key ex., A/E
DSS (Digital Signature Standard)	upto 2048	signature gen.
Elliptical Curve	upto 2048	

Cryptography and Authentication

Public-Key Cryptography - continued

- RSA Algorithm: an encryption scheme based upon the use of a block cipher technique.
  - Developed in 1977 by Ron Rivest, Adi Shamir, and Len Adleman at MIT
  - One of the most popular encryption algorithms
  - algorithm:
    - plaintext is encrypted in blocks using a binary value < n.
    - blocksize <= $\log_2(n)$
    - output block is referred to as cyphertext
    - Usage: Let M = message and C = block cyphertext
      - $C = M^e \bmod(n)$
      - $M = C^d \bmod(n) = (M^e)^d \bmod(n) = M^{ed} \bmod(n)$, n is common to both parties
    - Mathematical Process:
      - choose 2 prime numbers, p and q, such that n = pq
      - calculate T(n) = (p-1)*(q-1)
      - select e, with gcd(T(n), e)=1; 1 < e < T(n)
      - calculate d, $d = e^{-1} \bmod T(n)$
      - (e-1)T(n) + 1 = de
      - generate public key = {e,n}
      - generate private key = {d,n}

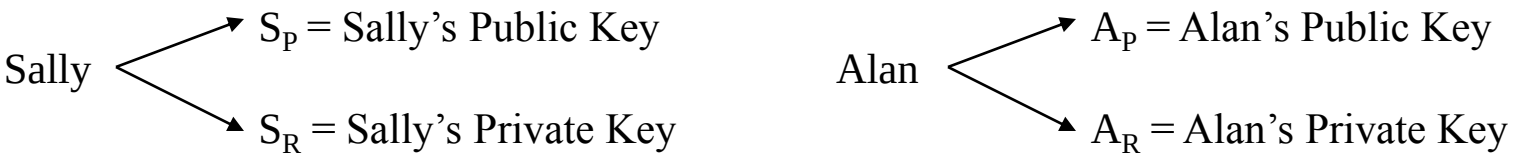
Public-Key Cryptography - continued

- Example:
  - choose p = 7, q = 17
  - n = pq = 119
  - T(n) = 6 x 16 = 96
  - gcd(T(n), e) = 1, e = 5
  - calculate $d = e^{-1} \text{mod} T(n)$, de = 4T(n) + 1 = 385, d = 77
  - plaintext encryption: let M = 19, $19^5 \text{mod}(119) = 20807.55462$, R = .55462 X 119 = 66
  - cyphertext decryption: $66^{77} \text{mod}(119)$, R = 19

Cryptography and Authentication

Public-Key Cryptography - continued

Public Key Encryption (inefficient), M = message



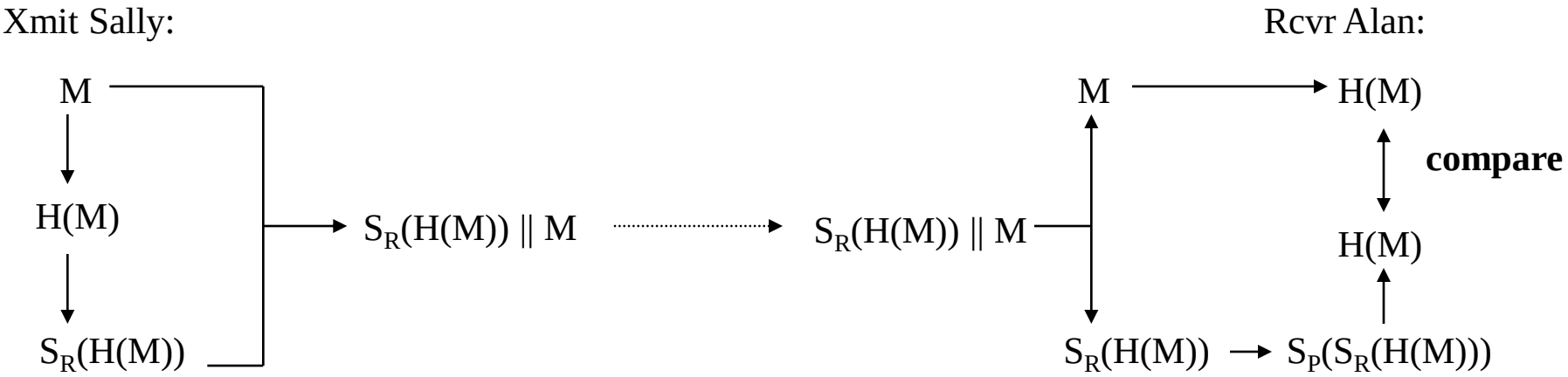
	Xmit Sally:		Rcvr Alan:		
Encryption:	$A_P(M)$	⟶	$A_R(A_P(M))$		
Authentication:	$A_P(S_R(M))$	⟶	$A_R(A_P(S_R(M)))$	⟶	$S_P(S_R(M))$

Cryptography and Authentication

Digital Signatures

- Digital signature: an encrypted digest of the message to be sent.
- Digests are sometimes referred to as a "fingerprint."
- Hash functions bears names such as SHA-1 (Secure Hash Algorithm), MD5 (Message Digest), and RIPEMD-160 (European RACE Integrity Primitives Evaluation).
- Digital signatures are concatenated to an encrypted message prior to transmission. They serve as a means of authentication upon reception.

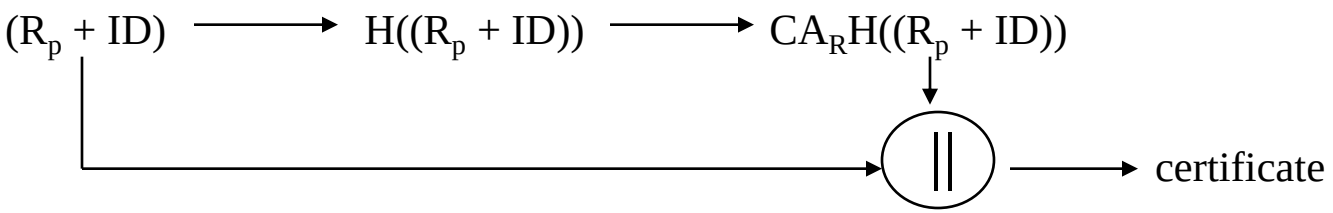
Unencrypted message with digital signature, M = message



Digital Certificates (CAs and the X.509 Standard)

- Public-Key encryption is vulnerable to the Middleman Attack in which a third person, the middleman, electronically impersonates the intended recipient of an encrypted message.
- Digital certificates remove the threat of the Middleman Attack.
- A digital certificate is comprised of the legitimate recipient's public key and user ID, which is digitally signed by a trusted third party, referred to as a certificate authority (CA).
- CAs might be governmental agencies, financial institutions, or other "trusted" sources.
- Upon taking ownership, the would-be recipient can freely publish the new certificate, which also contains their public key.
- Prior to the transmission of an encrypted message, the sender can verify the authenticity of the recipient's public key by decryption of the published certificate using the CAs public key.

Creation of a digital certificate, R = recipient, CA = certificate authority



Cryptography and Authentication

Digital Certificates (CAs and the X.509 Standard) - continued

- The X.509 standard is the authentication services portion of the more general ITU-T (International Telecommunications Union) X.500 standard, which defines an advanced set of distributed directory services.
- In essence, the X.509 standard defines three public-key certificate formats, a hierarchical trust system for CAs, and a means by which certificates may be revoked.
- X.509 certificates are used with many different encryption/authentication technologies including: S/MIME, SET (Secure Electronic Transactions ~ ecommerce), IPSec, and SSL/TLS.

Cryptography and Authentication

IPSec (IP Security)

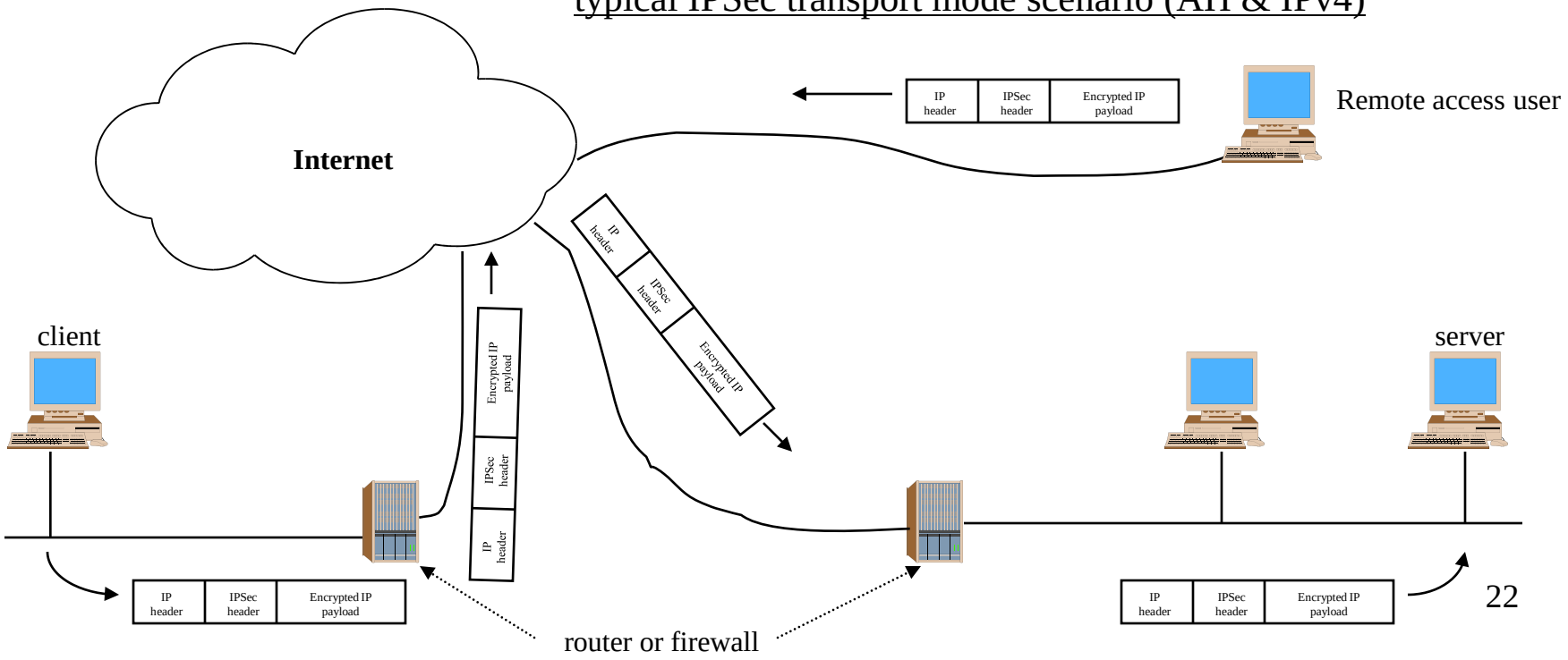
- By implementing security within the IP protocol, all information coming or going to a sight via TCP/IP can be secured, not just applications developed using security technologies.
- IPSec-based products have provisions to secure data traffic by using encryption and/or authentication headers within an IPv4 or IPv6.
- Common uses of IPSec are: the creation of VPNs (Virtual Private Networks), secure remote access, and enhanced security for ecommerce.
- IPSec is comprised of two distinct subprotocols: AH (Authentication Header) and ESP (Encapsulating Security Payload); AH employs only authentication, whereas, ESP employs authentication and encryption.
- IPSec employs a Security Policy Database (SPD) to determine which IP packets will receive IPSec services. Traffic receiving services is directed to the appropriate security association (SA) for processing.

Cryptography and Authentication

IPSec (IP Security) - continued

- AH and ESP support two modes of operation: transport and tunnel.

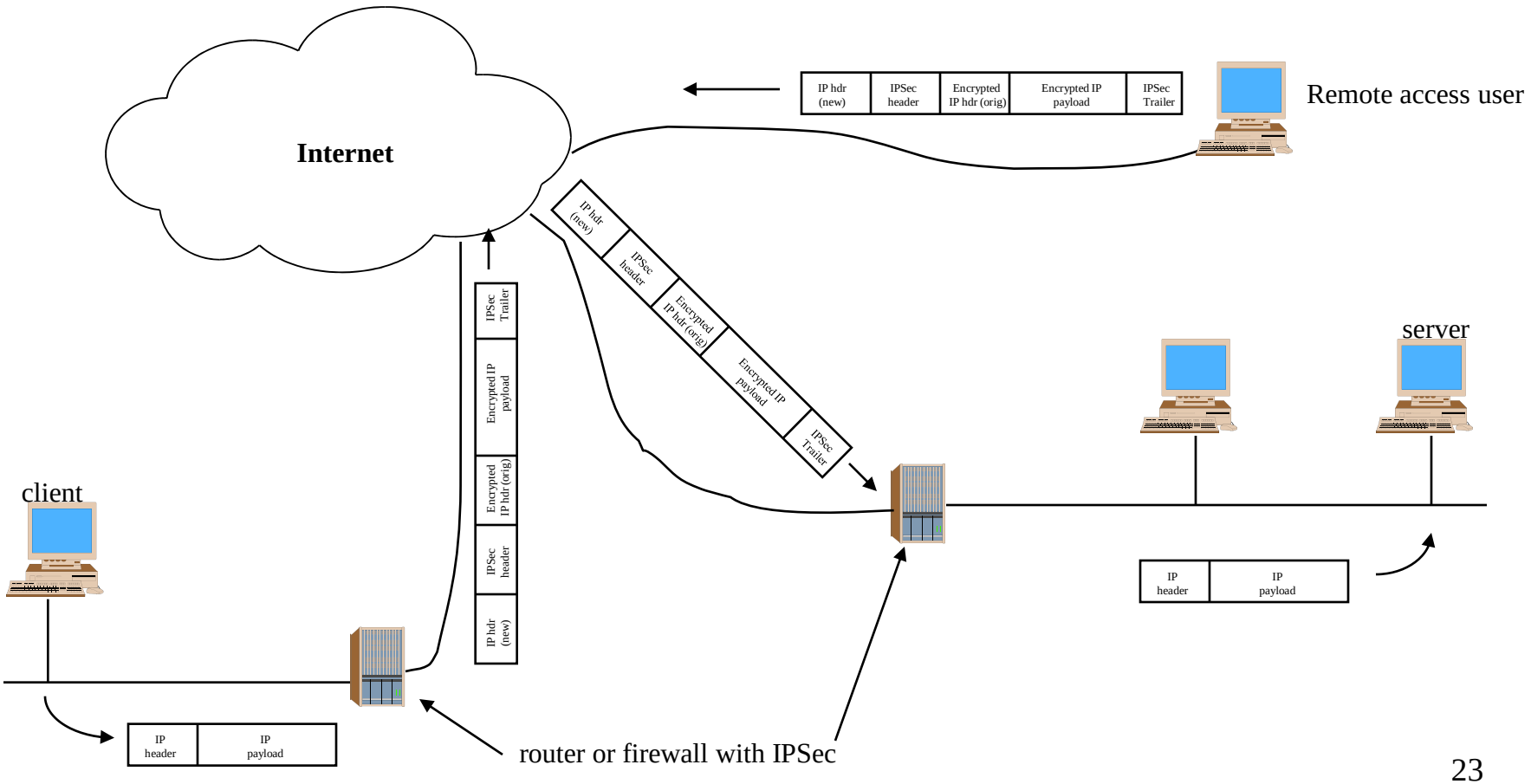
typical IPSec transport mode scenario (AH & IPv4)



Cryptography and Authentication

IPSec (IP Security) - continued

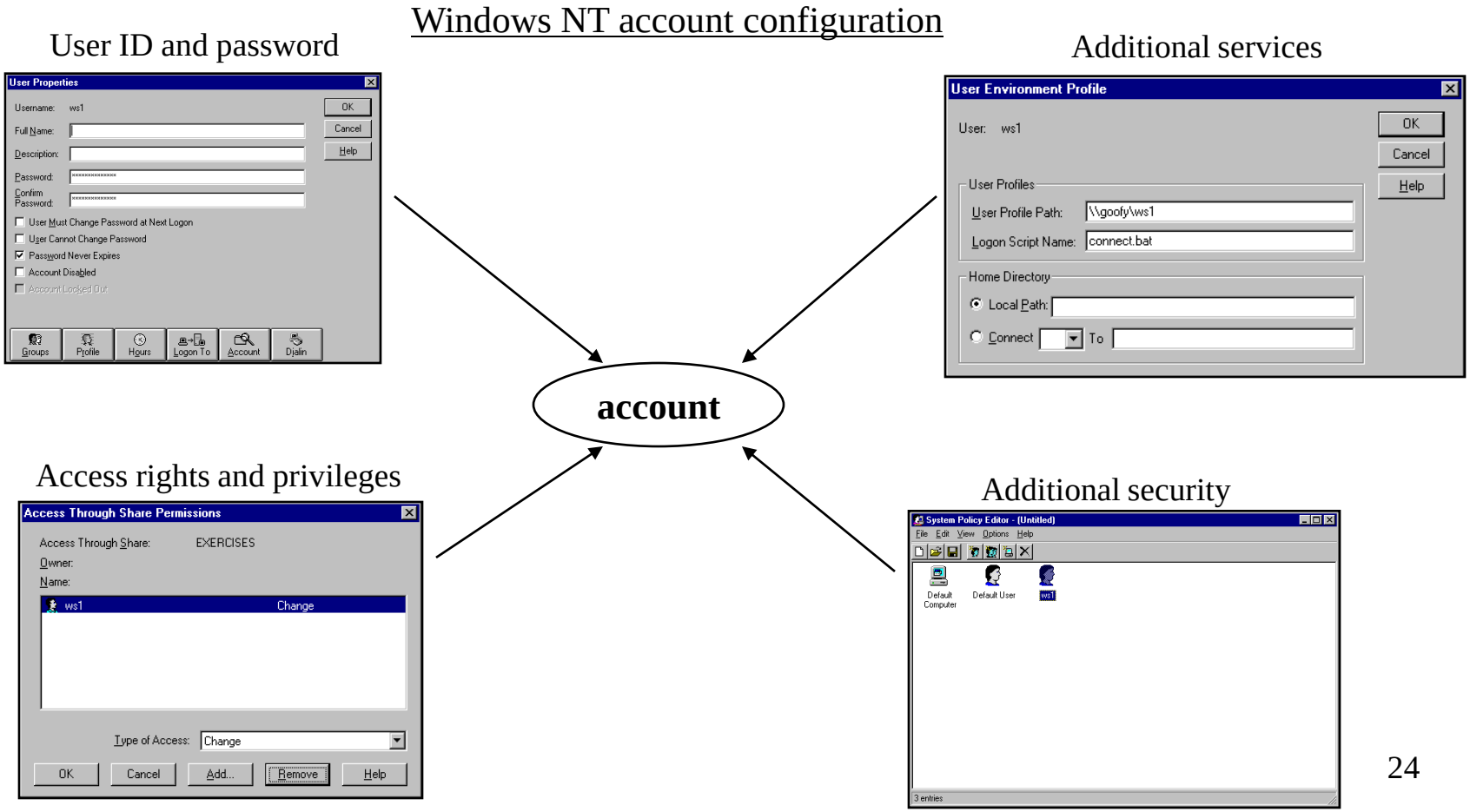
typical IPSec tunnel mode scenario (ESP & IPv4)



Security Services

Login and FTP

- The login process is comprised of several key subprocesses including: user ID and password (typically used for authentication), access rights and privileges, additional services received, and additional security applied. Similar processes are found in most operating systems, such as Windows NT and Unix.



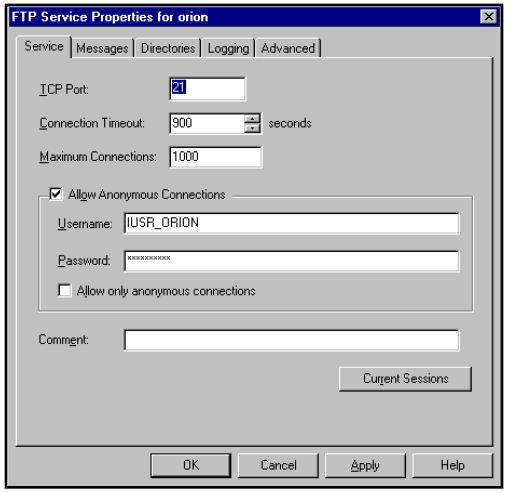
Security Services

Login and FTP - continued

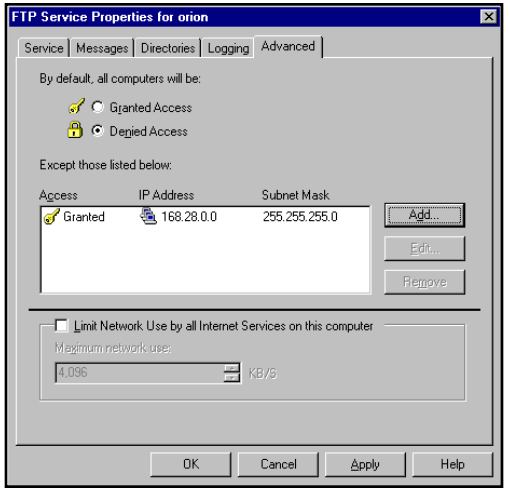
- Security can be applied to FTP in several ways including : packet filtering via its connection and data ports (I.e. using a firewall), account restriction, IP address restriction, log files, etc. Similar mechanisms are found in server-based operating systems, such as Windows NT and Unix.
- A common practice is to allow the general public access to certain secure areas using the account “anonymous.” As with any valid account, this account is vulnerable to hacker attacks. It can be disabled, thus requiring the would-be user to have an individual login account on that server.

Windows NT IIS FTP configuration

Anonymous login restriction



access restriction via address



Security Services

Email Security

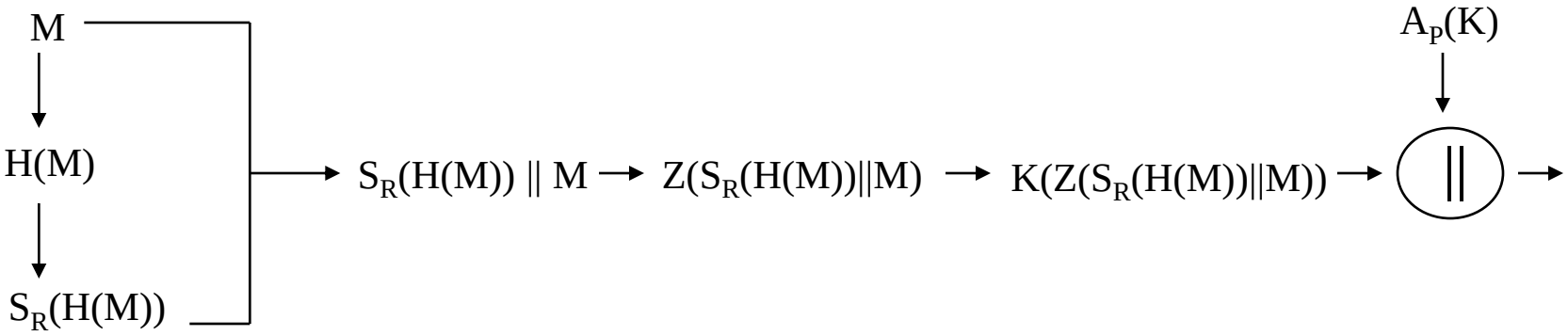
- Email's ubiquitous popularity in virtually facets of human interactions has given rise to the need for message confidentiality and authentication. Currently, the two most popular technology solutions capable of meeting these needs are PGP (Pretty Good Privacy) and S/MIME (Secure Multipurpose Internet Mail Extension).
- Several email clients, such as Microsoft Outlook Express, Qualcomm's Eudora, or Netscape Communicator, currently employ PGP and/or SMIME. PGP is typically used for personal messages, whereas S/MIME is typically used in commercial products.
- PGP was created by Phil Zimmermann and is available as freeware or a commercial product (with vendor support) for several operating systems including: Windows, Unix, and MacOS.
- PGP provides the following privacy-related services:
  - encryption
  - digital signature
  - email compatibility
  - compression
  - segmentation/reassembly

Security Services

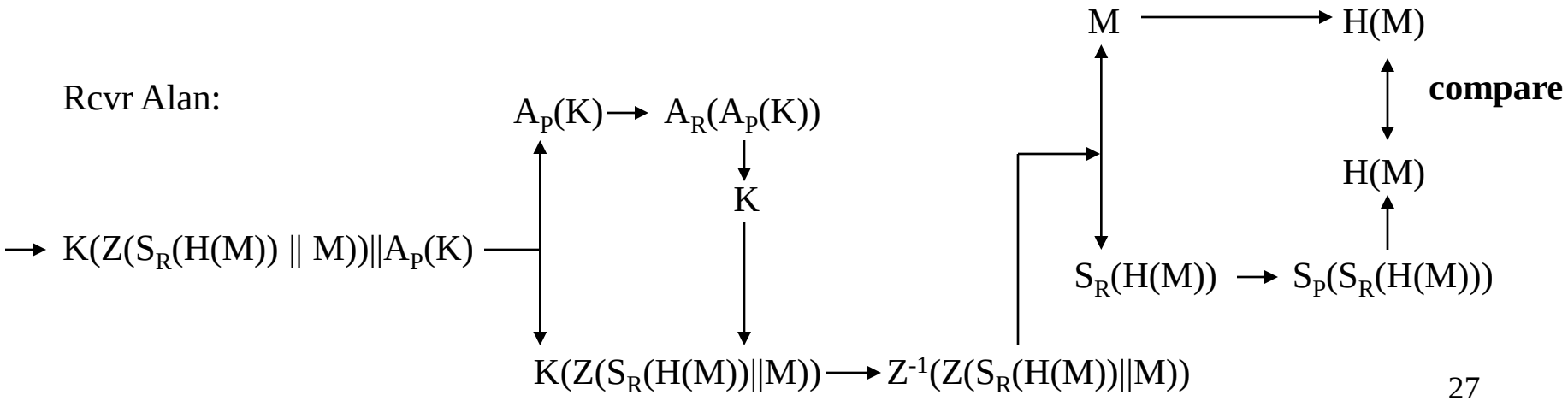
Email Security - continued

PGP Services, M = message, H= hash function, Z = ZIP, K = session key (conventional)

Xmit Sally:



Rcvr Alan:

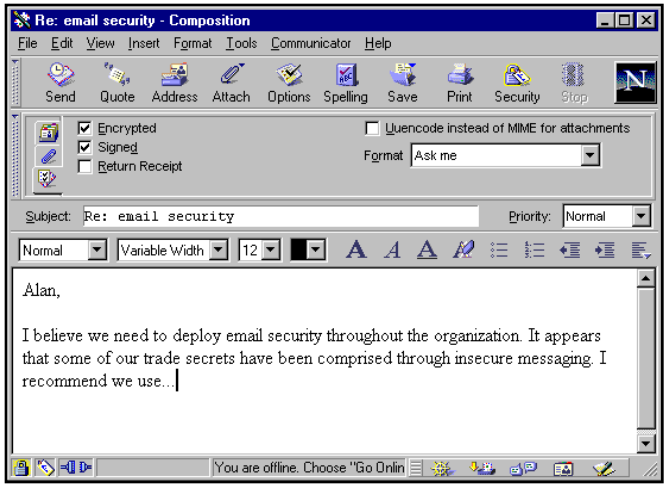


Security Services

Email Security - continued

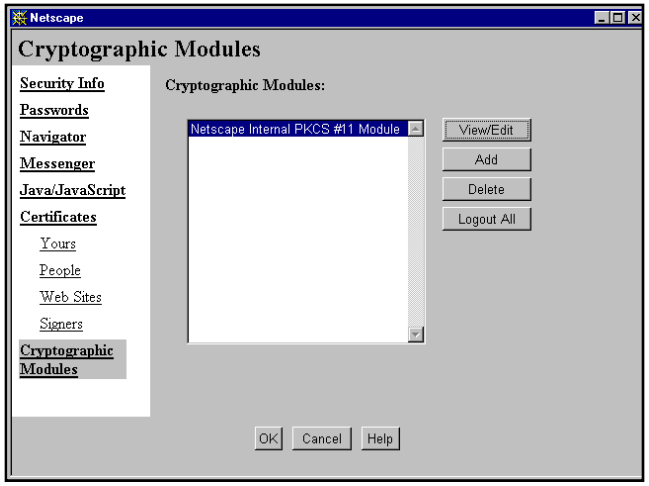
Netscape Communicator Message Security

a

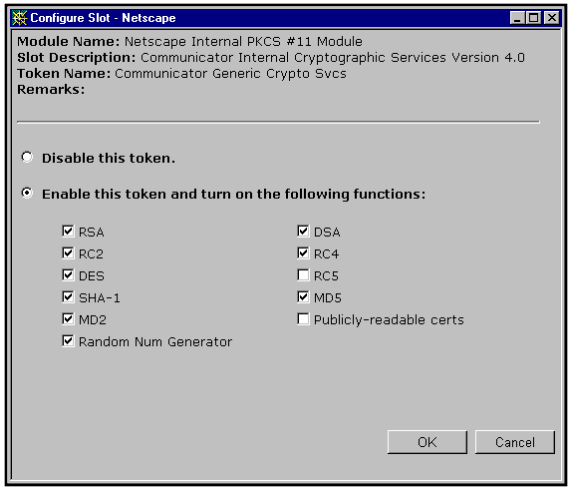


b

c



d

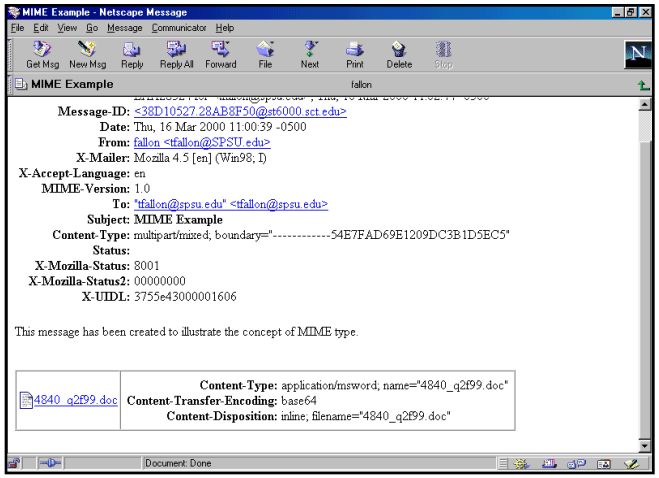


Security Services

Email Security - continued

- S/MIME is an encryption and authentication enhancement to the MIME format used in Internet-based email systems. It is very similar to PGP.
- The transport protocol, SMTP (Simple Mail Transfer Protocol), is only capable of transmitting and receiving ASCII-based messages. Therefore, one of the primary functions of MIME is the conversion of other formats into ASCII upon transmission and back into its original state upon reception.
- MIME defines several different Content Types, such as “multipart/mixed” and “text/enriched,” which can be transported within the envelope of an Internet message, along with the original message.

MIME enhanced message



Security Services

Email Security - continued

- S/MIME provides the following security services:
  - clear-signed data
  - signed data
  - enveloped data
  - signed and enveloped data
  - S/MIME employs the use of X.509 certificates for public key authentication

Web Security

Security Threats

- Active and passive attacks are possible against web servers, browsers, and the data traffic between them. Such attacks can be categorized by the type of threat they pose and the countermeasures that may be deployed against them. They are:
  - Denial of Service
    - countermeasure: use of firewalls and network analysis (detection), hard to prevent
  - Confidentiality
    - countermeasure: use of encryption and firewalls
  - Integrity
    - countermeasure: use of cryptographic checksums
  - Authentication
    - countermeasure: use of digital signatures, message encryption, and certificates
- Fortunately, the following advanced technologies are capable of providing the aforementioned countermeasures: IPSec, S-HTTP (Secure HTTP), S/MIME, SSL (Secure Socket Layer), Transport Layer Security (Transport Layer Security), SET (Secure Electronic Transactions), and firewalls.

Web Security

S-HTTP (Secure HTTP)

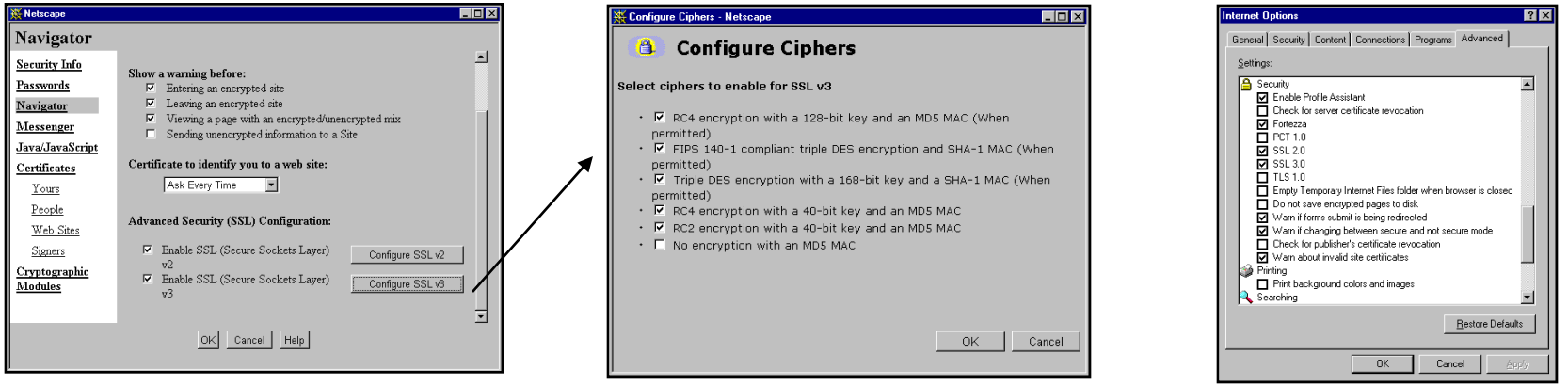
- S-HTTP is a secure, but independent, version of HTTP that provides secure message-oriented communications, such as an encrypted web-based form, between web clients and servers.
- S-HTTP has provisions for encryption and authentication using either the CMS (Cryptographic Message Syntax) or MOSS (MIME Object Security Services) security standards, which employ RSA or DSA for digital signatures generation and DES or RC2 for encryption. Public key authentication is also supported via the use of certificates.
- Implementing security requires the use of S-HTTP-enabled clients and servers. However, in the event that either side does not support S-HTTP, regular HTTP-based communication will still occur.

Web Security

SSL (Secure Socket Layer)

- SSL is a multi-protocol Internet standard which provides security services to TCP and its payload.
- Although SSL was designed by Netscape Communications Corp. (now AOL), and is, therefore, implemented within Navigator, it is also implemented within Internet Explorer.
- The IETF has formed a TLS (Transport Layer Security) working group to develop a common Internet-based version of SSL. TLS is very similar to SSLv3.0.

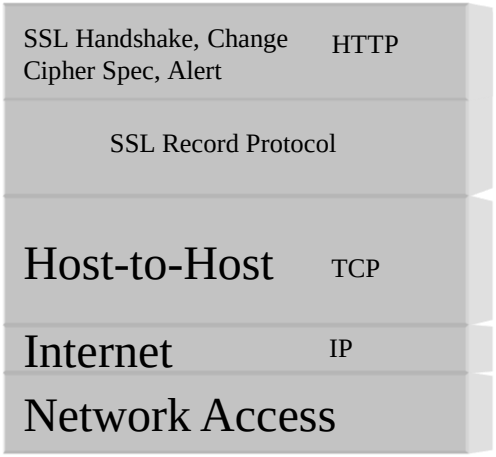
Netscape Navigator and Microsoft I.E. SSL Configuration



SSL (Secure Socket Layer) - continued

- The four SSL subprotocols (see previous figure) are:
  - Handshake Protocol
  - Change Cipher Spec Protocol
  - Alert
  - Record Protocol

SSL and the TCP/IP model



Web Security

Java and ActiveX Issues

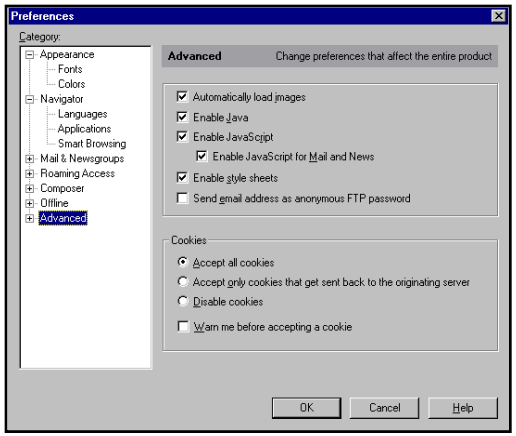
- The Java programming language (developed by Sun MicroSystems, Inc.) was designed with security in mind. Although related to C++, several features that enable a program to access systems resources have been removed.
- Using a Java compiler, such as javac, one can create stand-alone applications or miniature applications, referred to as applets, that can be transmitted over the Internet to a Java-enabled web browser.
- The creation and implementation stages of an applet are: 1) source code is created with a text editor (filename.java), 2) source is complied into Java bytecode, or applet, using a Java compiler (filename.class), 3) applet is embedded into a web page with certain parameter specifications, 4) web page is downloaded into requesting browser, 5) the applet is verified and run by a Java bytecode interpreter, referred to as a Java Virtual Machine (JVM).
- Although applets are, for the most part, secure, JVMs may not be. Other than memory, JVMs prevent applets from accessing other system resources unless if an appropriate applet signature is provided and verified.

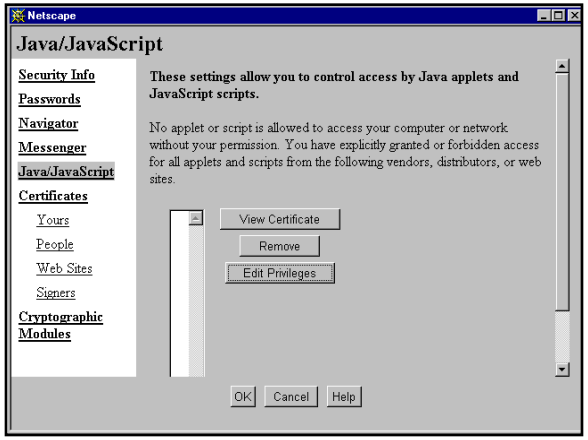
Web Security

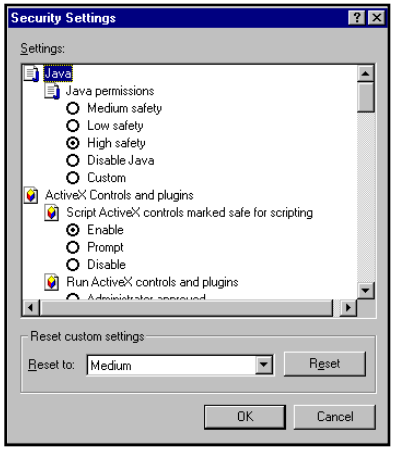
Java and ActiveX Issues - continued

- ActiveX (developed by Microsoft) is a component-based programming environment in which programmers create ActiveX controls in languages such as Microsoft Visual Basic or C.
- Controls are basically "canned" programs that provides the user with some sort of control mechanism, such as a media player or slide-lever, which is embedded within a web page.
- Unlike Java Applets, controls are optionally downloaded to the user's hard drive for subsequent use. Like applets, ActiveX controls can be digitally signed for security purposes.

Netscape Navigator and Microsoft I.E. Java/ActiveX Configuration





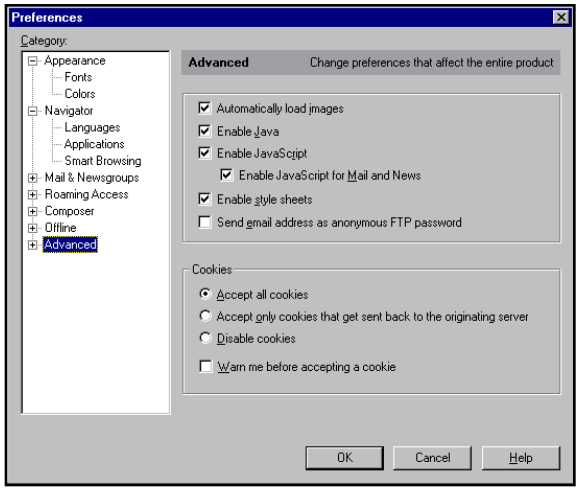


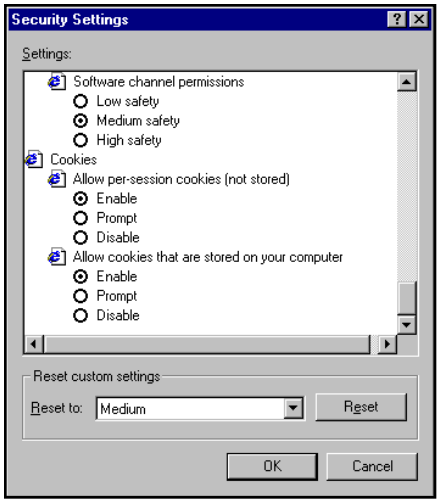
Web Security

Cookies

- Cookies are bits of data that may be written to a user's hard drive from a visited web site. Cookies are typically used to store web site specific information (such as user name, password, credit card numbers, links visited most often, etc.) so that the user won't have to enter the information upon subsequent visits. Although such information provides greater surfing efficiency, it can also be used for unscrupulous means, such as tracking a user's habits for reasons of exploitation.
- Netscape Navigator and Internet Explorer have provisions to disable or modify the behavior of cookies.

Netscape Navigator and Microsoft I.E. Cookie Configuration





Firewalls

- A firewall is a security mechanism used to protect an organization's external or internal network borders. They are usually implemented on computers possessing a secure operating system (referred to as a trusted system), such as Windows NT or Unix configured for such duties.
- Firewalls are generally capable of providing several important security features including: a single point for audit and alarm generation, bi-directional access restrictions, internal and external user authentication, VPN (e.g. using IPSec), NAT (Network Address Translation) and protection from several known attack strategies.
- Firewalls can not protect internal networks and computer systems from all forms of malicious behavior. Additional external connections (such as dialup lines), attacks originating internally, and virus protection issues are generally not supported by firewalls.
- Firewalls are categorized by the manner in which they operate as either packet-filtering, application-level gateway, or circuit-level gateway.
- A bastion host is a trusted system used to aid a firewall(s) in the defense of an internal network's perimeter. Bastion hosts may be configured to require additional authentication of user requests, more extensive auditing of data traffic, and the implementation of multiple, independent proxies.

Firewalls

Packet-filtering

- Implemented using routers or trusted systems, such as a PC running a secured Linux operating system, packet-filtering firewalls operate by applying a set of rules to each incoming and outgoing packet.
- Filtering rules are based upon the information contained within either the IP address and/or IP protocol fields (IP header), and/or the port number fields (TCP or UDP header).
- The appropriate field(s) within each packet is/are compared to each rule within the set of rules until a match is found, where upon it is forwarded or discarded; several rule sets may exist.
- If no specific rule applies, then the default rule, which is placed at the bottom of the set, will be applied to the packet. Default rules either explicitly discard or forward all packets. Usually, the "discard all" default rule is employed.

SMTP rule set for packet-filtering firewall

action	source	src port	destination	dst port	flags
forward	[internal]	*	*	25	
forward	*	25	*	*	ACK
discard	*	*	*	*	*

Firewalls

Application-level Gateway

- Commonly referred to as a proxy server, an application-level gateway is essentially a relay agent that that behaves as the proxy for a legitimate, internal application; I.e, client requests don’t directly interact with the application.
- After the user’s request has been authenticated, TCP segments containing application-related data are relayed to and from the internal system running the application. Applications for which proxy agents have not been implemented are inaccessible to external request.
- Although application-level gateways are usually more secure than packet-filtering firewalls, they are also generally slower, due to the greater amount of processing required.

Firewalls

Circuit-level gateway

- Generally implemented on a stand-alone system, circuit-level gateways operate by establishing two separate TCP connections, internal and external, after the user's request has been properly authenticated. Once the "circuit" is established, data segments (TCP and UDP) are allowed to traverse the firewall. Security is enforced by determining which connections to establish.
- A typical circuit-level firewall scenario would involve the use of a proxy server for incoming traffic and a circuit-level configuration for outgoing traffic. It is assumed that internal users are trusted, and, therefore, can freely select which external applications to use, whereas, external users are generally not trusted, and, therefore, must be restricted to applications permitted by the organization.

Firewalls

Example

Typical screened host firewall configuration