

Internet Security

Contents:

- Why Internet security
- Layered view of network security
- System security
- Other security applications

Why Internet Security

- More and more business activities are conducted over the Internet.
- More and more computers are connected to the Internet.
- More hackers (easy access to the Internet with lower cost).
- And we have a course about Information Technology in Electronic Commerce.

Network Security – Layered view

- Application layer security
 - Electronic mail security (PGP, S/MIME).
 - SET (Secure Electronic Transaction).
 - Many others.
- Transport layer security
 - SSL (Secure Socket Layer)
 - TLS (Transport Layer Security)
- IP Layer security
 - IPSec
- Data link and physical layer security
 - Provided by telephony.

Application Layer Security

- Electronic mail security – PGP (pretty good privacy)
 - Initially developed by Philip R. Zimmermann in 1991.
 - Uses a public key cipher to encrypt a session key.
 - Uses a secret key cipher with the session for data encryption.
 - Uses a public key ring and a private key ring for key management.
 - Users can choose to have confidentiality only, authentication only, or both.

PGP Cryptographic Functions

Explanation of symbols used in the next three figures:

K_s session key used in conventional (symmetric key) encryption

KR_a private key of user A

KU_a public key of user A

EP public-key encryption

DP public-key decryption

EC conventional encryption

DC conventional decryption

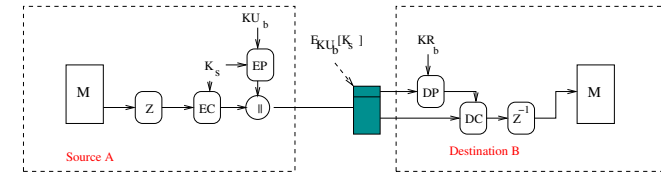
H hash function

\parallel concatenation

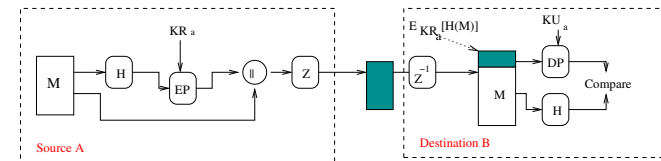
Z compression using ZIP algorithm

PGP Cryptographic Functions

➤ Confidentiality only.

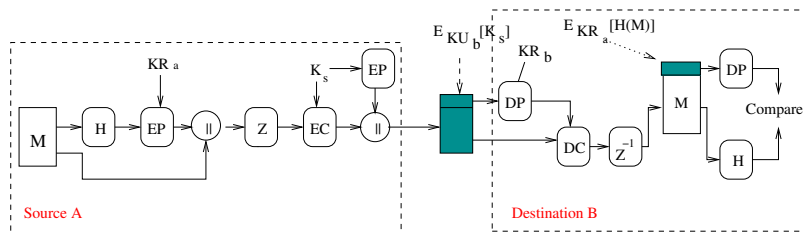


➤ Authentication only.



PGP Cryptographic Functions

➤ Confidentiality and Authentication.



Application Layer Security

➤ Electronic mail security – S/MIME (Secure Multi-Purpose Internet Mail Extensions)

- Security enhanced version of MIME Internet email standard.
- Targeting an industry standard.
- Compared with PGP, format more fixed (less flexibility).
- Utilizes X.509 protocol for key management.

➤ S/MIME versus PGP

- PGP is a protocol on top of normal email applications (SMTP), while S/MIME is security enhanced version of normal MIME.
- PGP is designed to be more flexible, while S/MIME tends to be more standard.
- PGP uses its own PKI while S/MIME uses X.509 as its PKI.

Application Layer Security

- Secure Electronic Transaction (SET)
 - Developed by MasterCard and Visa, with SETv1 emerging in 1996.
 - Primarily for protection of credit card transactions over the Internet.
- SET provides the following security services:
 - Confidentiality of information.
 - Integrity of data.
 - Cardholder account authentication.
 - Merchant authentication.

Transport Layer Security – SSL

- Secure Socket Layer (SSL) protocol
 - Designed and specified by Netscape, has been implemented by Netscape Communicators and Microsoft Internet Explorer.
 - Modified by Internet Engineering Task Force (IETF) as an Internet Standard, called **Transport Layer Security** (TLS).
- SSL services
 - Data encryption
 - message integrity
 - sever authentication
 - client authentication

SSL Sub-protocols

- Essentially two sub-protocols, used in every session:
 - SSL Record Protocol, provides security services for various higher layer protocols.
 - SSL Handshake Protocol, making connections to remote machine.
- Other associated sub-protocols, invoked during SSL connection, and may not be used in every session:
 - SSL Alert Protocol, notifying errors.
 - SSL Change Cipher Spec Protocol, changing session key.

IP Layer Security

- Provides general purpose security services.
- Both encryption and authentication can be provided.
 - Authentication Header (AH).
 - Encapsulating Security Payload (ESP).
- Encryption can apply to either the content only (transport mode), or the whole IP datagram (tunnel mode).
 - **Transport mode:** link-to-link encryption, vulnerable to traffic analysis attack.
 - **Tunnel mode:** end-to-end encryption, used to establish virtual private networks (VPNs).
- IPSec (v4 and v6) dominates IP layer security protocols.

System Security

- Firewall configuration and operating system security are all key factors to network security.
- Firewall services:
 - Service control
 - Direction control
 - User control
 - Behavior control
- Firewall types:
 - Screening Router: Service type (e.g. telnet or ftp) and service access point (IP address, port number) selection. Does not check content of datagram.
 - Proxy gateways: do what screening router does plus content checking, e.g. key word scanning, document virus scanning.

System Security

- Another type of system security threat is virus type of intruders.
 - viruses, trapdoors, logic bombs, Trojan horses, bacteria, Internet worms.
- Common features: – infection (reproduction); execution.
- Common behavior:
 - damaging the file system;
 - using the computing resources (CPU, RAM, Networks).
- Protection
 - viruses scanner;
 - using a secure operating system;

Other Network Security Protocols

- Secure HTTP (S-HTTP): security extension of HTTP.
 - Client/Server Authentication
 - Spontaneous Encryption
 - Request/Response Non-repudiation
- Secure Shell (ssh).
- Secure Copy (scp): transferring files between computers across the network.

Security Concerns

- Virus type of malicious attacks.
- Internet flooding attacks, terrorist attacks, and the kind.
- Password attacks (private key management).
- Security management (internal attacks).
- Mistrust.

Legal Issues

- Intellectual property.
 - Copyrights.
 - Trade marks.
- Criminal judgment and jurisdiction.
 - Laws may not yet be comprehensive enough to cover all the cases of criminal activities in e-commerce.
 - Laws may differ from country to country.
- Fair trading?
 - How can one ensure that fair trading will be achieved?
- Special applications: Internet voting (trust problems) and Internet gambling (legal and fair issues)