Security in Layers & Attack Mitigation

Network Security Workshop

APNIC

Overview

- Protocols and Attack Vectors
- Layer 2 Attacks
- TCP Attacks
- Application-Layer Attacks
- Security Protocols

APNIC

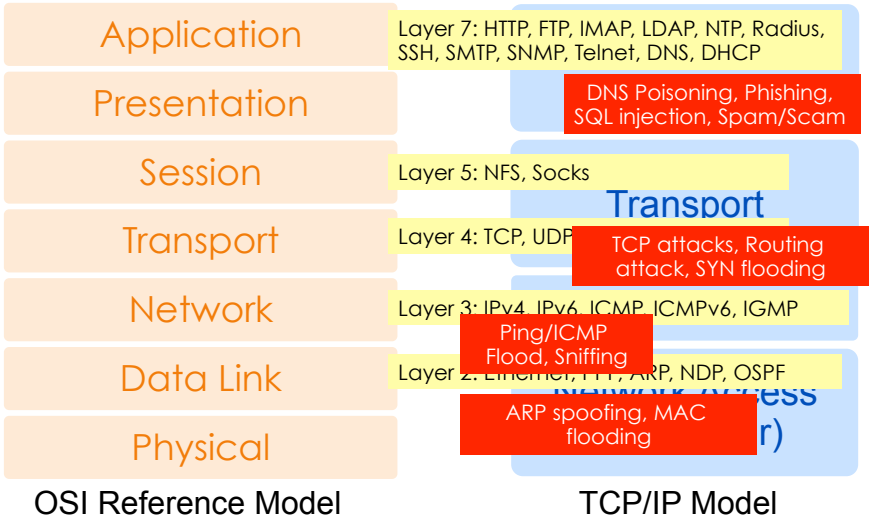
TOP SECURITY INCIDENTS OF 2014

1. Heartbleed OpenSSL Bug (April)
2. Shellshock Bash vulnerability (Sept)
3. POODLE in SSLv3 (Oct)
4. JP Morgan Chase system hacked (Oct)
5. Breach on Home Depot (and other retailers) (Oct)
6. Sony Hack (Nov/Dec)
   - Has an international impact

http://www.eweek.com/security/slideshows/top-10-security-incidents-and-vulnerabilities-of-2014.html

APNIC

Attacks on Different Layers



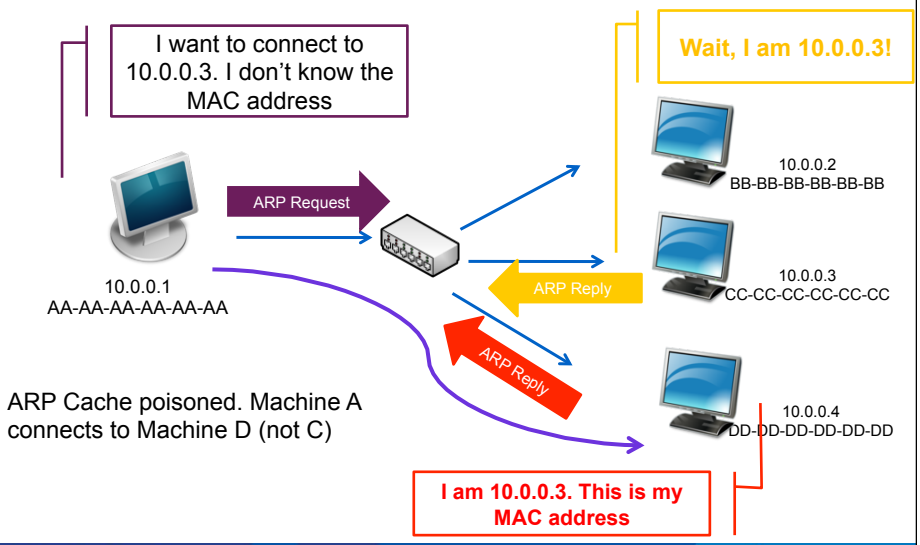
APNIC

Layer 2 Attacks

- ARP Spoofing
- MAC attacks
- DHCP attacks
- VLAN hopping

APNIC

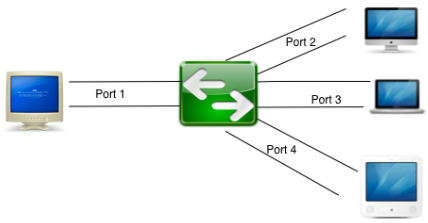
ARP Spoofing



APNIC

MAC Flooding

- Exploits the limitation of all switches – fixed CAM table size
- CAM = Content Addressable memory = stores info on the mapping of individual MAC addresses to physical ports on the switch.

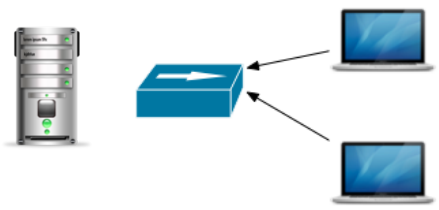


	Port 1	Port 2	Port 3	Port 4
00:01:23:45:67:A1	x			
00:01:23:45:67:B2		x		
00:01:23:45:67:C3			x	
00:01:23:45:67:D4				x

DHCP Attack

- DHCP Starvation Attack
  - Broadcasting vast number of DHCP requests with spoofed MAC address simultaneously.
  - DoS attack using DHCP leases
- Rogue DHCP Server Attacks

Server runs out of IP addresses to allocate to valid users

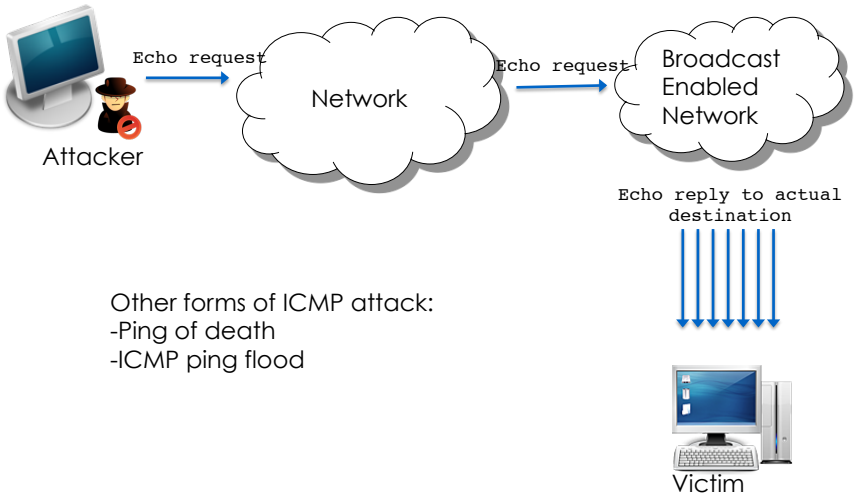


Attacker sends many different DHCP requests with many spoofed addresses.

Layer 3 Attacks

- ICMP Ping Flood
- ICMP Smurf
- Ping of death

Ping Flood



Other forms of ICMP attack:
-Ping of death
-ICMP ping flood

Routing Attack

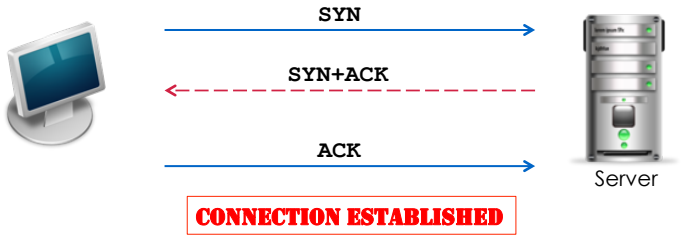
- Attempt to poison the routing information
- Distance Vector Routing
  - Announce 0 distance to all other nodes
    - Blackhole traffic
    - Eavesdrop
- Link State Routing
  - Can drop links randomly
  - Can claim direct link to any other routers
  - A bit harder to attack than DV
- BGP attacks
  - ASes can announce arbitrary prefix
  - ASes can alter path

TCP Attack

- SYN Flood – occurs when an attacker sends SYN requests in succession to a target.
- Causes a host to retain enough state for bogus half-connections such that there are no resources left to establish new legitimate connections.

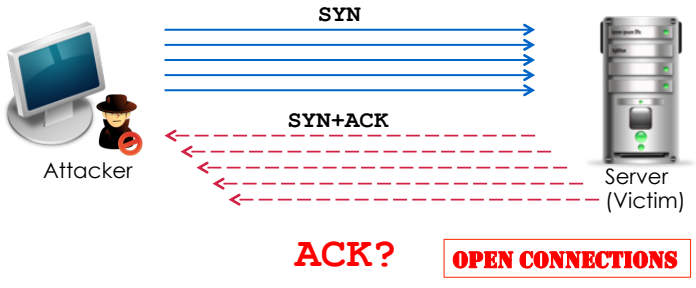
TCP Attack

- Exploits the TCP 3-way handshake
- Attacker sends a series of SYN packets without replying with the ACK packet
- Finite queue size for incomplete connections



TCP Attack

- Exploits the TCP 3-way handshake
- Attacker sends a series of SYN packets without replying with the ACK packet
- Finite queue size for incomplete connections



Application-Layer Attacks

- Target applications or services at Layer 7
  - Increasingly common in recent years
- Sophisticated, stealthy and difficult to detect and mitigate
  - "slow and low"

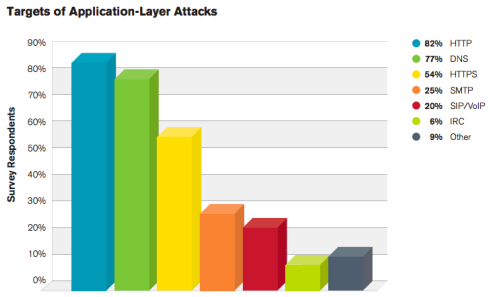


Figure 24 Source: Arbor Networks, Inc.

Source: Arbor Networks WISR 2014

APNIC

Application-Layer Attacks

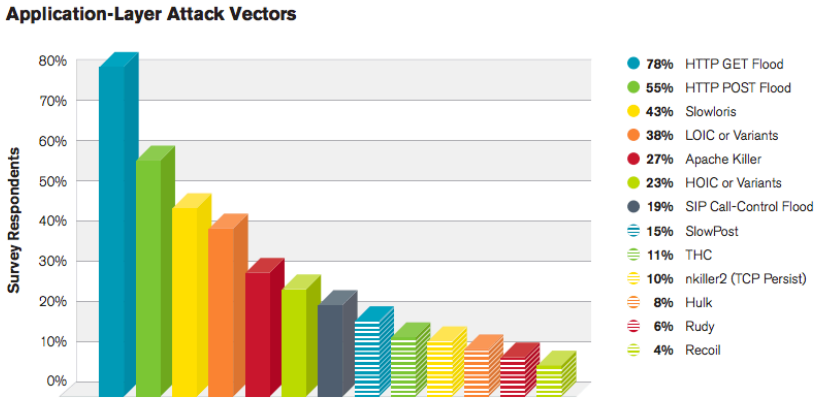


Figure 27 Source: Arbor Networks, Inc.

Source: Arbor Networks Worldwide Infrastructure Security Report Volume 2014

APNIC

Layer 7 DDoS Attack

- Traditional DoS attacks focus on Layer 3 and Layer 4
- In Layer 7, a DoS attack is targeted towards the applications disguised as legitimate packets.
- The aim is to exhaust application resources (bandwidth, ports, protocol weakness) rendering it unusable
- Includes:
  - HTTP GET
  - HTTP POST
  - Slowloris
  - LOIC / HOIC
  - RUDY (R-U-Dead Yet)

Layer 7 DDoS: Slowloris

- Incomplete HTTP requests
- Properties
  - Low bandwidth
  - Keep sockets alive
  - Only affects certain web servers
  - Doesn't work through load balancers
  - Managed to work around accf_http

Application Layer Attacks

- Scripting vulnerabilities
- Cookie poisoning
- Buffer overflow
- Hidden field manipulation
- Parameter tampering
- Cross-site scripting
- SQL injection

Check the OWASP Top 10 Web Application Security Risks

DNS Changer

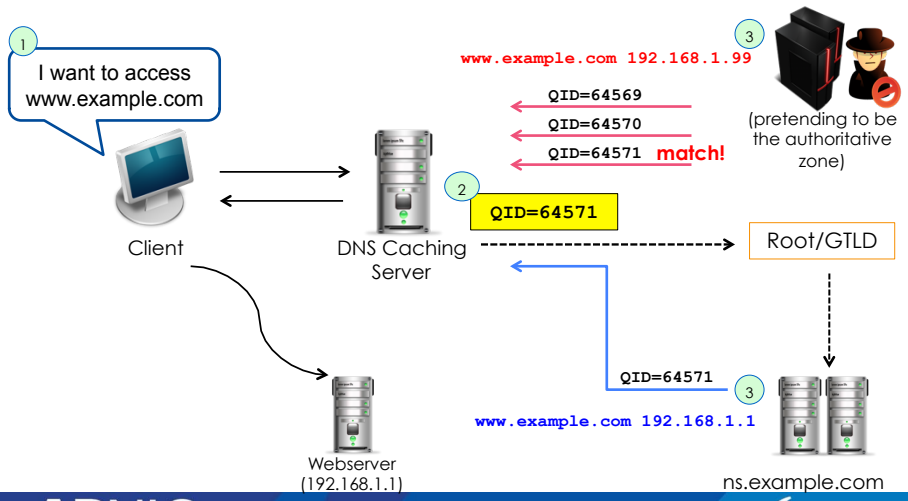
- “Criminals have learned that if they can control a user’s DNS servers, they can control what sites the user connects to the Internet.”
- How: infect computers with a malicious software (malware)
- This malware changes the user’s DNS settings with that of the attacker’s DNS servers
- Points the DNS configuration to DNS resolvers in specific address blocks and use it for their criminal enterprise
- For more: see the NANOG presentation by Merike

DNS Cache Poisoning

- Caching incorrect resource record that did not originate from authoritative DNS sources.
- Result: connection (web, email, network) is redirected to another target (controlled by the attacker)

APNIC

DNS Cache Poisoning

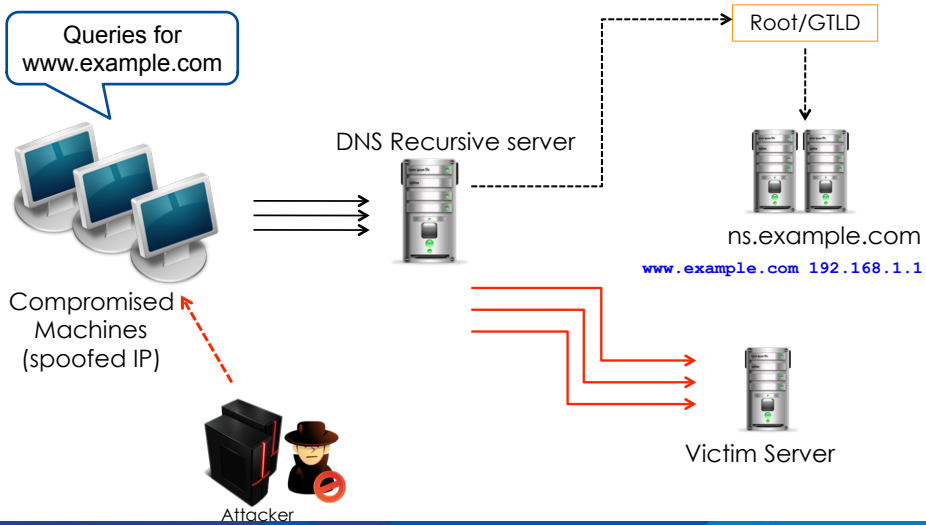


APNIC

DNS Amplification

- A type of reflection attack combined with amplification
  - Source of attack is reflected off another machine
  - Traffic received is bigger (amplified) than the traffic sent by the attacker
- UDP packet's source address is spoofed

DNS Amplification Attack



Common Types of Attack

- Ping sweeps and port scans - reconnaissance
- Sniffing – capture packet as they travel through the network
- Man-in-the-middle attack – intercepts messages that are intended for a valid device
- Spoofing - sets up a fake device and trick others to send messages to it
- Hijacking – take control of a session
- Denial of Service (DoS) and Distributed DoS (DDoS)

Wireless Attacks

- WEP – first security mechanism for 802.11 wireless networks
- Weaknesses in this protocol were discovered by Fluhrer, Mantin and Shamir, whose attacks became known as “FMS attacks”
- Tools were developed to automate WEP cracking
- Chopping attack were released to crack WEP more effectively and faster
- Cloud-based WPA cracker
  - https://www.wpacracker.com/

Man in the Middle Attacks (Wireless)

- Creates a fake access point and have clients authenticate to it instead of a legitimate one.
- Capture traffic to see usernames, passwords, etc that are sent in clear text.

Botnet

- Collection of compromised computers (or 'bot')
- Computers are targeted by malware (malicious software)
- Once controlled, an attacker can use the compromised computer via standards-based network protocol such as IRC and HTTP
- How to become a bot:
  - Drive-by downloads (malware)
  - Go to malicious websites (exploits web browser vulnerabilities)
  - Run malicious programs (Trojan) from websites or as email attachment

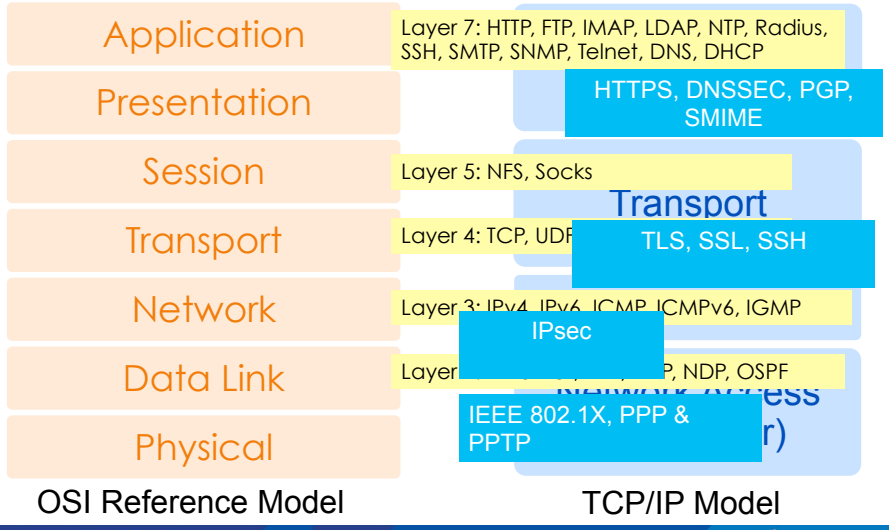
Password Cracking

- Dictionary attacks
  - Guessing passwords using a file of 1M possible password values
    - Ordinary words and people's names
  - Offline dictionary attack when the entire password file has been attacked
  - Use random characters as password with varying upper and lower case, numbers, and symbols
- Brute-force attacks
  - Checking all possible values until it has been found
  - The resource needed to perform this attack grows exponentially while increasing the key size
- Social engineering

Pharming and Phishing

- Phishing – victims are redirected to a fake website that looks genuine. When the victim supplies his account and password, this can be used by the attacker to the target site
  - Typically uses fraud emails with clickable links to fake websites
- Pharming – redirect a website's traffic to another fake site by changing the victim's DNS settings or hosts file

Attacks on Different Layers

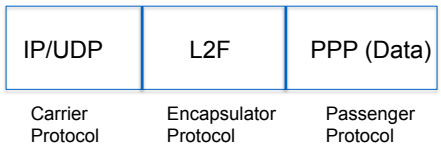


Link-Layer Security

- Layer 2 Forwarding (L2F)
- Point-to-Point Tunneling Protocol (PPTP)
- Layer 2 Tunneling Protocol (L2TP)

Layer 2 Forwarding Protocol

- Created by Cisco Systems and replaced by L2TP
- Permits the tunneling of the link layer – High-level Data Link Control (HDLC), async HDLC, or Serial Line Internet Protocol (SLIP) frames – of higher-level protocols



Point to Point Tunneling Protocol

- Initiated by Microsoft but later became an informational standard in the IETF (RFC 2637)
- Client/server architecture that allows PPP to be tunneled through an IP network and decouples functions that exist in current NAS.
- Connection-oriented

Layer 2 Tunneling Protocol

- Combination of L2F and PPTP
- Published as RFC 2661 and known as L2TPv2
- L2TPv3 provides additional security features and the ability to carry data links other than PPP
- The two end-points are L2TP Access Concentrator (LAC) or L2TP Network Server (LNS)

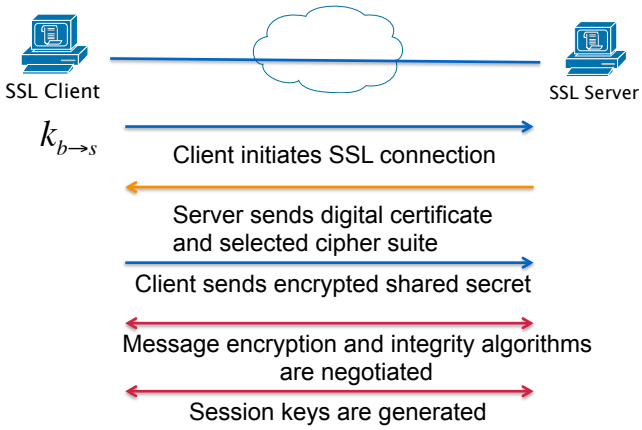
Transport Layer Security

- Secure Socket Layer (SSL)
- Secure Shell Protocol
- SOCKS Protocol

SSL/TLS

- TLS and SSL encrypts the segments of network connections above the Transport Layer.
- Versions:
  - SSLv1 – designed by Netscape
  - SSLv2 – publicly released in 1994; has a number of security flaws; uses RC4 for encryption and MD5 for authentication
  - SSLv3 – added support for DSS for authentication and DH for key agreement
  - TLS – based on SSLv3; uses DSS for authentication, DH for key agreement, and 3DES for encryption
- TLS is the IETF standard which succeeded SSL.

SSL Handshake



Advantages of SSL

- The connection is private
  - Encryption is used after initial handshake to define a secret key
  - Encryption uses symmetric cryptography (DES or RC4)
- Peer's identity can be authenticated using asymmetric cryptography (RSA or DSS)
- The connection is reliable
  - Message transport includes message integrity check using a keyed MAC. Secure hash functions (SHA or MD5) are used for MAC computation.

Applications Using SSL/TLS

Protocol	Defined Port Number	SSL/TLS Port Number
HTTP	80	443
NNTP	119	563
LDAP	389	636
FTP-data	20	989
FTP-control	21	990
Telnet	23	992
IMAP	143	993
POP3	110	995
SMTP	25	465

SSL POODLE Vulnerability

- A vulnerability in SSLv3.0 CVE-2014-566
- Note that SSL 3.0 (RFC101) is an obsolete protocol and has been replaced by TLS
- But many TLS implementations are still backwards compatible with it
- Implement TLS_FALLBACK_SCSV if SSLv3 cannot be disabled

APNIC https://www.openssl.org/~bodo/ssl-poodle.pdf

OpenSSL and Heartbleed

- OpenSSL is a popular open-source implementation of SSL and TLS protocols
- In April 2014, a serious vulnerability CVE-2014-160 was found in OpenSSL, as a result of improper input validation in the TLS/DTLS “hearbeat” extension (RFC6520)
- This leads to leak of memory content, thus allowing attackers to steal data (secret keys, usernames/passwords, messages) from clients and servers

APNIC http://heartbleed.com/

Secure Shell Protocol (SSH)

- Protocol for secure remote login
- Provides support for secure remote login, secure file transfer, and secure forwarding of TCP/IP and X Window System traffic
- Consists of 3 major components:
  - Transport layer protocol (server authentication, confidentiality, integrity)
  - User authentication protocol (authenticates client to the server)
  - Connection protocol (multiplexes the encrypted tunnel into several logical channels)

Application Layer Security

- HTTPS
- PGP (Pretty Good Privacy)
- SMIME (Secure Multipurpose Internet Mail Extensions)
- TSIG and DNSSEC
- Wireless Encryption - WEP, WPA, WPA2

HTTPS

- Hypertext Transfer Protocol Secure
- Widely-used, message-oriented communications protocol
- Connectionless oriented protocol
- Technically not a protocol in itself, but simply layering HTTP on top of the SSL/TLS protocol
- Encapsulates data after security properties of the session
- Not to be confused with S-HTTP

Note: A website must use HTTPS everywhere, otherwise it is still vulnerable to some attacks

Pretty Good Privacy (PGP)

- Stands for Pretty Good Privacy, developed by Phil Zimmerman in 1995
- PGP is a hybrid cryptosystem
  - combines some of the best features of both conventional and public key cryptography
- Assumptions:
  - All users are using public key cryptography and have generated private/public key pairs (using RSA or El Gamal)
  - All users also use symmetric key system (DES or Rijndael)
- Offers authentication, confidentiality, compression, e-mail compatibility and segmentation

Questions