Keamanan Sistem Komputer

Wireless Network Security, DoS, DDoS

SECURITY NEWS

October 17th 2010, Chicago, Illinois

seek4media

50% of all Wi-Fi networks capable of being hacked in 5 seconds

A study conducted recently has found that nearly 50 percent of Wi-Fi networks could be hacked. The study conducted in six cities and derived that out of 40,000 Wi-Fi network nearly 20,000 did not have passwords assigned to them.

It is estimated that nearly 82 percent of the people thought their network was secure, though the harsh reality is that nearly 25 percent of the private networks had no password. What has made the study scarier is that hackers were able to hack through secure networks.

Hackers like Jason Hart believe that today it is easy for hackers to get into another user's system and access their information, emails and social sites apart from online banking. They could also create a social identity of their own.

http://www.seek4media.com

SECURITY NEWS

October 22, 2010

Google Street View Car Cameras Grab Emails & Passwords

Google collected e-mails, passwords, and URLs while the company was snapping images for its Street View service, it admitted in a blog.

"In some instances, entire e-mails and URLs were captured, as well as passwords," Google's senior vice president of engineering and research, Alan Eustace, wrote in a blog post

Eustace said that "**most of the data is fragmentary**," and the company will delete the information "as soon as possible."

This collection of data, Google states, happened while **mistakingly running a piece of code from an experimental project** which ran alongside a program Google intended on using to amass data on **WiFi hotspots** to provide location-based services.

Eustace said that Google had not "**analyzed in detail the mistakenly collected data**, so they did not know for sure what the disks contained."

The company said that its director of privacy, Alma Whitten, will help "build effective privacy controls" into Google products and practices.

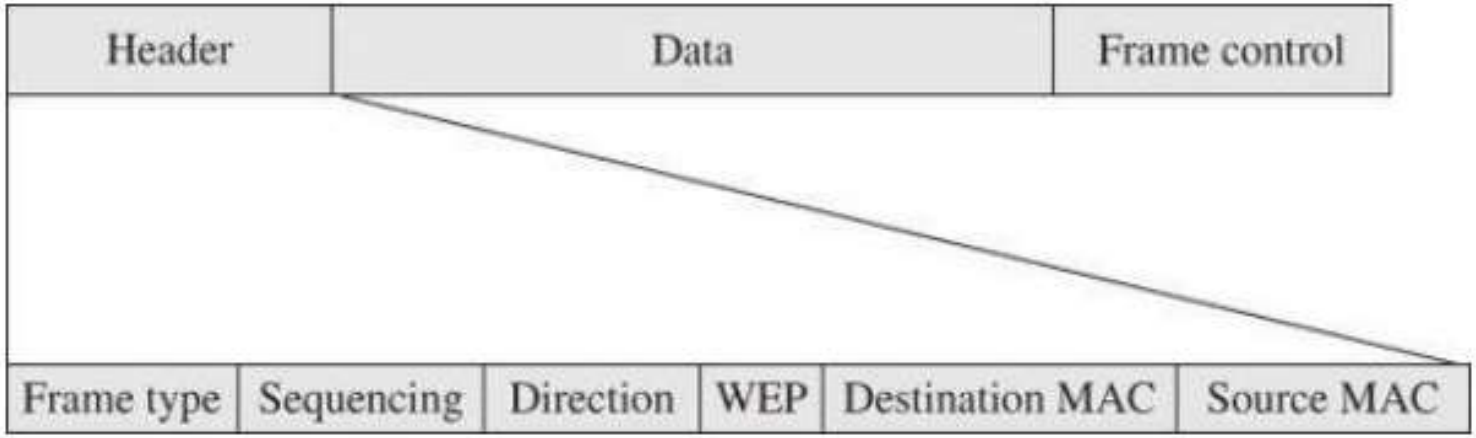
http://www.slashgear.com

Wireless Network

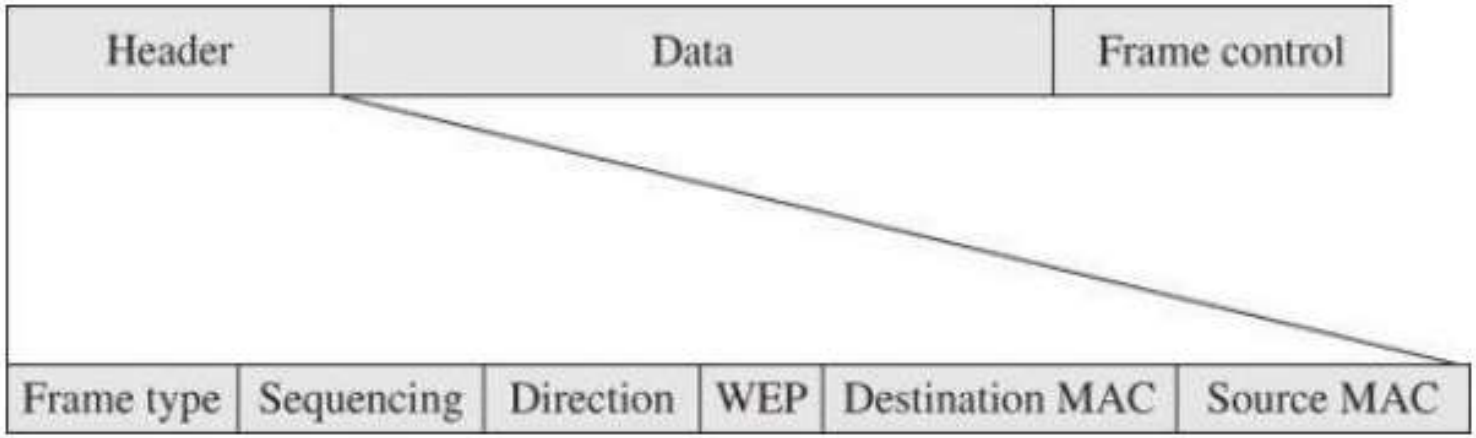
- Wireless communication will never be as secure as wired, because the exposed signal is more vulnerable.
- A wireless network consists of:
  - Access point or router that receives, forward and transmits data
  - One or more devices that communicate with the access point
- Each device must have a NIC, which identifies itself by a supposedly unique MAC address.
- Wireless signal degrade because of interference from intervening objects as well as distance.

Wireless Network

- Each WiFi data unit, called frame, contains three fields: MAC header, payload, and FCS (frame check sequence)



Wireless Network



- Frame type: control, **management**, data.
- Management frames are the most important, they control the establishment and handling series of data flows.

Wireless Network

The most significant management frame types:

- Beacon: beacon signal advertises a network accepting connection
- Authentication: NIC requests a connection by sending an authentication frame. To terminate an established connection, a deauthentication frame is used.
- Association request and response: NIC requests an access point to establish a session. To terminate a session, a deassociation request is used.

Wireless Network

- SSID (Service Set Identifier) is the identification of an access point; it is a string of up to 32 characters chosen by the access point's administrator.
- The SSID is the identifier the access point broadcasts in its beacon, and the ongoing link ties an associated NIC's communication to the given access point.

Vulnerability in Wireless Network

- Confidentiality; If data signals are transmitted in the open, certainly unintended recipients may be able to get the data.
- Integrity; The sources of problems could be nonmalicious sources (reception problem caused by weather, etc) or a direct, malicious attacks to change the content of the communication.
- Availability; Involves three potential problems:
  - Component of wireless communication stops working because of hardware fails
  - Availability is loss of some but not all access, typically manifested in slow or degraded service.
  - The possibility of rogue network connection.

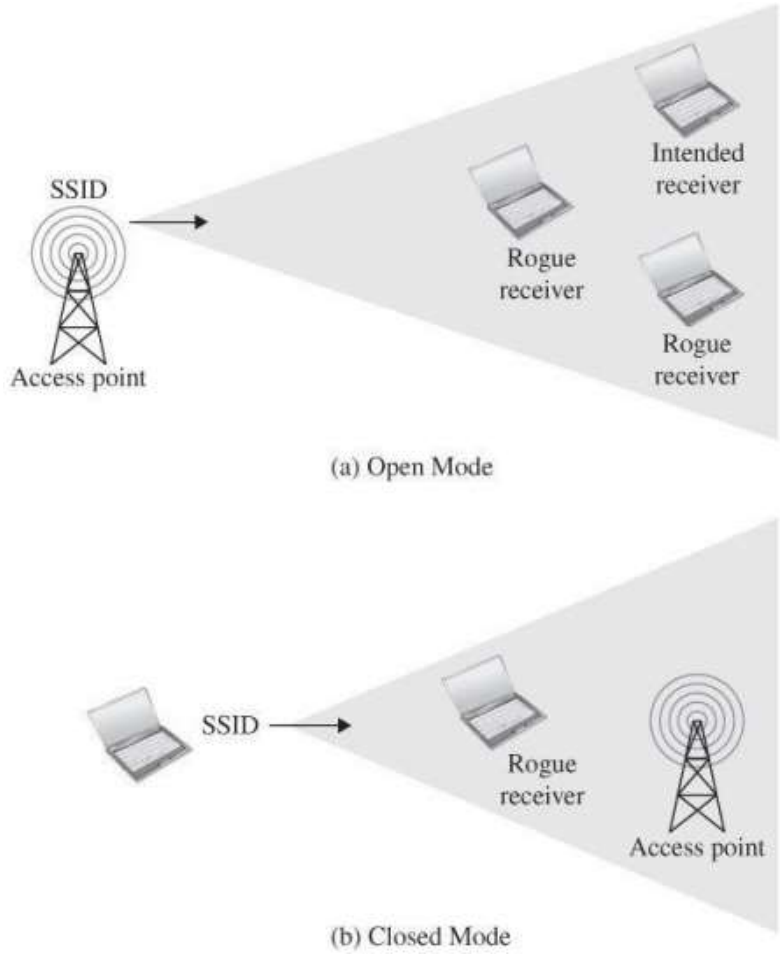
WiFi Protocol Weaknesses

<u>Picking up the beacon</u>

- Open mode: access point continually broadcasts its SSID
- Closed mode (stealth mode): a client continually broadcasts a request to connect to a given SSID

Operating in closed mode seem to be a successful way to prevent unauthorized access but leaves the client exposed.

In open mode, client effectively becomes a beacon, sending a continuing series of messages “I am MAC address mmm, looking for SSID sss. Are you sss?” From those messages a rogue host can learn the expected values needed to impersonate an access point.



WiFi Protocol Weaknesses

- SSID in all frames

  After the initial handshake, all data frames contain the same SSID, so sniffing any one of these frames reveals the SSID. A better protocol design would have been for the access point and the associating device to establish a shared data

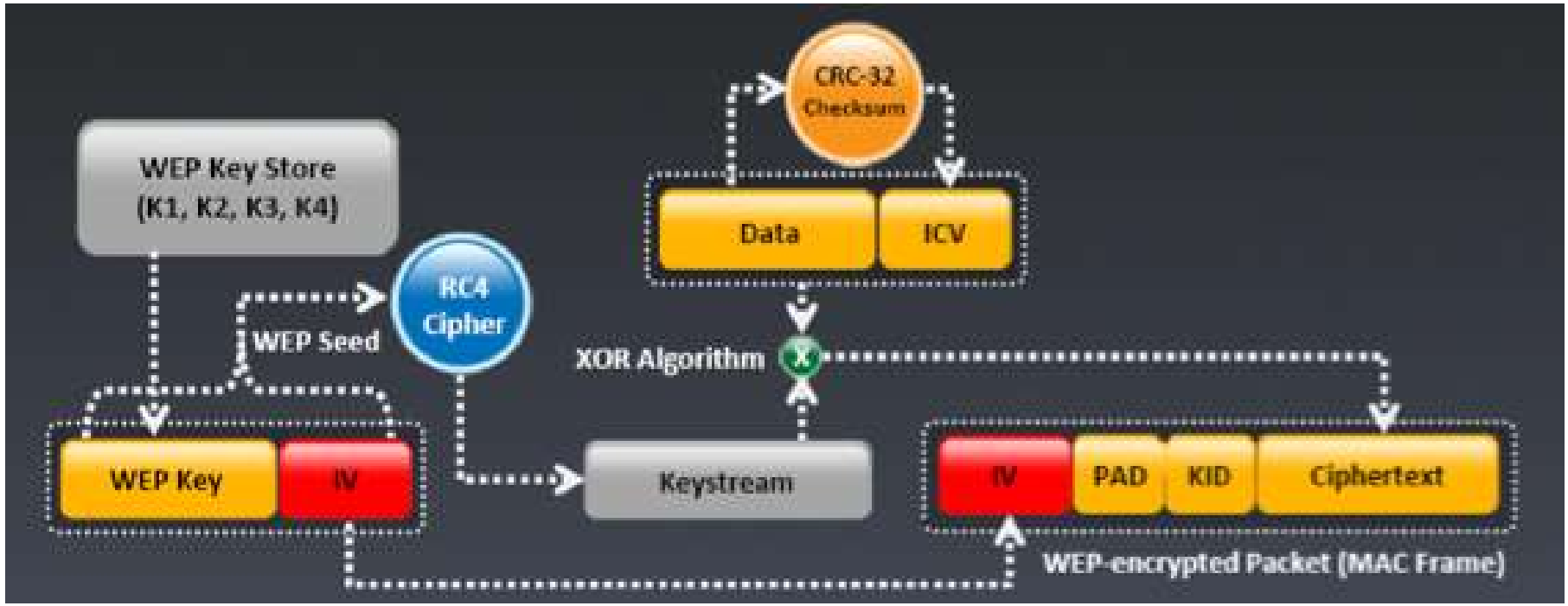
- Changeable MAC address

  Changing the NIC's MAC address can lead to a larger attack called MAC spoofing in which one device impersonates another.

WEP (Wired Equivalent Privacy)

- WEP was intended as a way for wireless communication to provide privacy equivalent to conventional wire communications.
- Weaknesses in WEP were identified as early as 2001, and the weaknesses are now so severe that WEP connection can be cracked with available software in a few minutes.

How WEP Works



WEP Security Weaknesses

- Weak encryption key
- Weak encryption algorithm
- Initialization vector collisions
- Fault integrity check
- No authentication

How WEP Works

- 32-bit Integrity Check Value (ICV) will be calculated for data frame
- Data frame will be padded with ICV
- Generate 24-bit Initialization Vector (IV) and sum it with WEP encryption key
- Combination of IV and WEP key will be used as input to RC4 and the result will used as keystream
- The keystream, data, and ICV will be XOR’ed and made chipher text
- IV will be added with cipher text and ICV for getting a MAC Frame

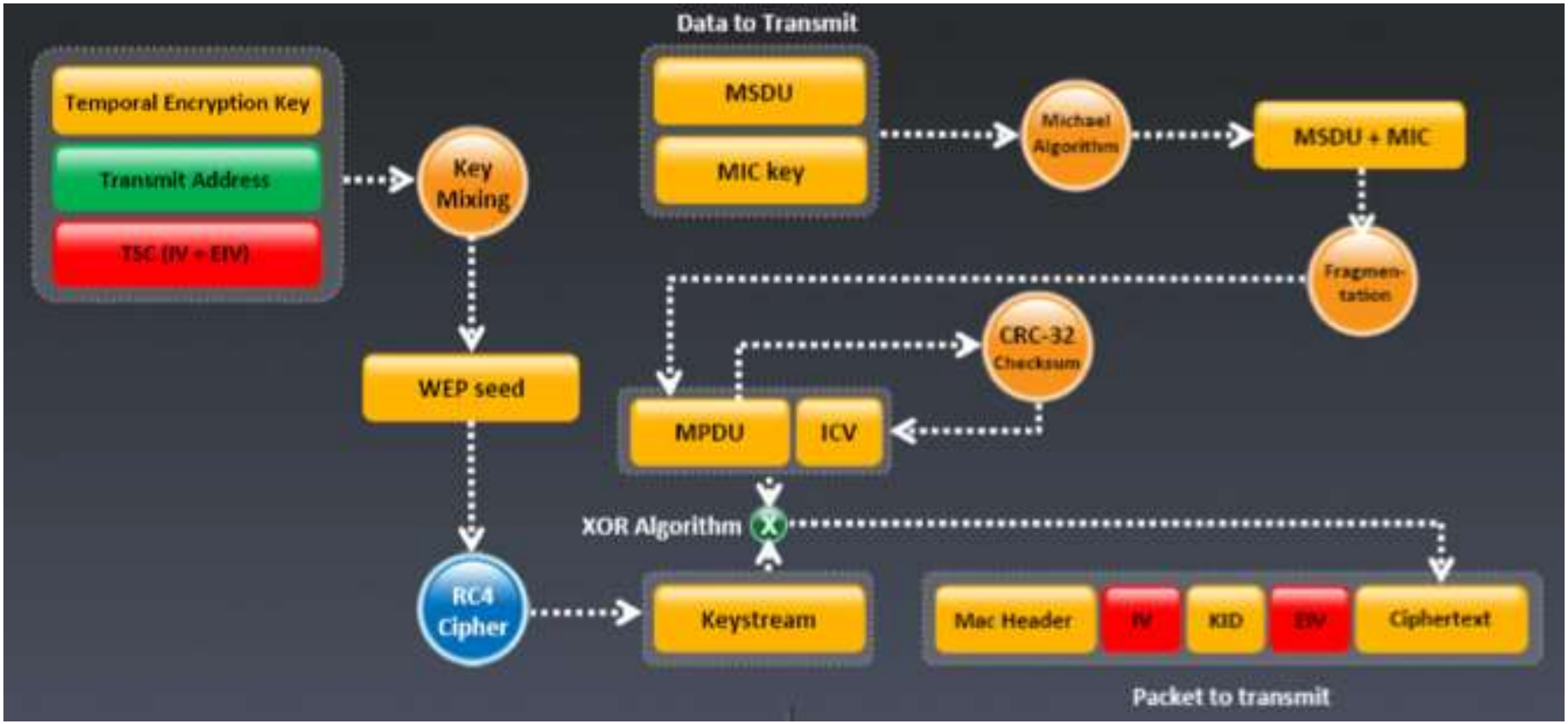
WPA (WiFi Protected Access)

- WEP uses short, infrequently changed encryption keys, it requires no authentication, and its integrity is easily compromised. So WEP Security is **unacceptable**.
- A stronger protocol suite -> WPA

WPA Strengths over WEP

- Non-static encryption key
- Authentication
- Strong encryption
- Integrity protection
- Session initiation

How WPA Works

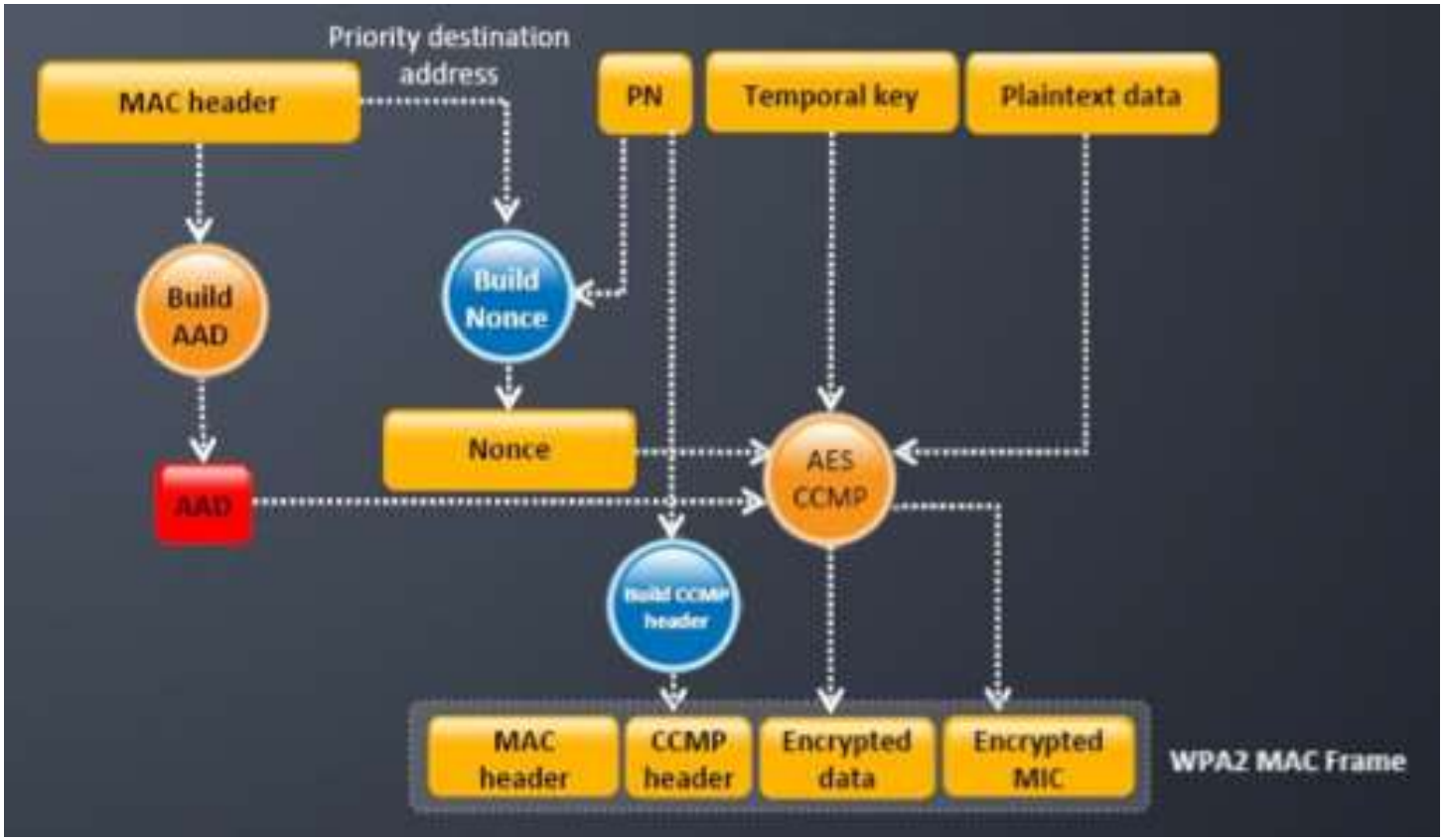


Attacks on WPA

- Man-in-the-middle
- Incomplete authentication
- Exhaustive key search

But WPA is adequately secure, since the vulnerabilities do not affect most users or WPA.

How About WPA-2



WEP vs. WPA vs. WPA2

Encryption	Attributes			
	Encryption Algorithm	**IV Size**	**Encryption Key Length**	**Integrity Check Mechanism**
WEP	RC4	24-bits	40/104-bits	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	Michael Algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	AES-CCMP

WEP	Should be replaced with more secure WPA and WPA2
WPA, WPA2	Incorporates protection against forgery and replay attacks

How To Break WEP

- Start your wireless device and run it into monitor mode with specific channel in Access Point
- Testing “injection capability” from wireless device to Access Point
- Use aireplay-ng to create fake authentication to Access Point
- Run Wi-Fi sniffing application such as airodump-ng or Cain & Abel with BSSID filter to get unique IV
- Run Wi-Fi packet encryption application such as aireplay-ng to run ARP request replay mode to inject packet
- Use Cain & Abel or aircrack-ng to crack and extract encryption key from IV

Bagaimana Membobol WPA/WPA2?

- WPA PSK :
  - Menggunakan password yang ditentukan oleh user untuk inisialisasi TKIP dimana tidak dapat di-crack packet yang sudah dilindungi oleh kunci tetapi kunci yang ada dapat di brute-force menggunakan dictionary attack
- Brute-Force WPA Keys :
  - Dapat menggunakan aplikasi seperti aircrack, aireplay, atau KisMac untuk mem-brute-force WPA key

Bagaimana Membobol WPA/WPA2?

- Offline Attack :
  - Dapat dilakukan saat berada didekat AP, serangan ini dapat dilakukan dengan sangat cepat, serangan ini bertujuan untuk mendapatkan autentikasi WPA/WPA2 handshake, dengan sukses mendapatkan paket yang tepat, kunci WPA dapat di-crack secara offline
- De-Authentication Attack
  - Memaksa client yang terkoneksi untuk terputus, dan kemudian meng-capture paket reconnect dan autentikasi dengan menggunakan airplay, akan didapatkan data autentikasi ulang dalam beberapa detik, dan dapat dilakukan serangan dengan menggunakan Dictionary Brute Force

Bertahan Dari WPA Cracking?

- Passphrases : untuk men-crack WPA dapat dilakukan dengan men-sniff password yang terasosiasi dengan “handshake”; jika password yang digunakan rumit, maka WPA hampir tidak mungkin dapat di-crack
- Passphrase Complexity : gunakan passphrase acak yang tidak ada dalam kamus; mininum 20 karakter, dan diganti secara rutin
- Client Settings : Hanya gunakan enkripsi AES/CCMP; setting di sisi client harus tepat (validasi server, alamat server harus benar, dsb.)
- Additional Control : Gunakan teknologi VPN, seperti Remote Access VPN, Extranet VPN, Intranet VPN, dsb.; Implementasi Network Access Control (NAC) atau Network Access Protection (NAP) untuk mengkontrol konektifitas pengguna.

DoS (Denial of Service)

- This kind of attack is devastating to a commercial firm that depends on computing for customer interaction, as well as back-end functions like inventory management and scheduling.
- The source of a DoS attack is typically difficult or impossible to determine with certainty.
- DoS can occur from excessive volume, a failed application, a severed link, or hardware or software failure.

DoS – How Service is Denied

Three root threats to availability:

- Insufficient capacity; overload
- Blocked access
- Unresponsive component

Attacker will try to actualize any of these threat types by exploiting vulnerabilities against them.

Network Flooding

- Flooding occurs because the incoming bandwidth is insufficient or resources—hardware devices, computing power, software, or table capacity—are inadequate.

Network Flooding Caused by Malicious Code

- Ping of death
- Smurf
- Echo-chargen
- SYN flood

Network Flooding by Resource Exhaustion

- Switching from one application to another, called context switching, requires time and memory,
- With too many processes, a system can enter a state called thrashing, in which its performance fails because of nearly continuous context switching.

Addressing Failure

- DNS spoofing; attackers intercepting and replying to a query before the real DNS server can respond.
- Rerouting routing; one node's redirecting a network so that all traffic flows through the attacking node.
- Source routing and address spoofing; source routing is a process where the sender can specify some or all the intermediate points. A vicious use of source routing is to force data to flow through a malicious router or network link.

DNS Attacks

- Session hijack; the attacker allows an interchange to begin between two parties but then diverts the communication. In session hijack the attacker literally steals an established TCP connection by rewriting source and destination addresses.
- DNS cache poisoning; subvert the addressing to cause a DNS server to redirect clients to a specified address. In cache poisoning an incorrect name-to-address DNS conversion is placed and remains in a translation cache.

Physical Disconnection

- Transmission failure; line cut or network noise makes a packet unrecognizable or undeliverable.
- Component failure; age, factory flaws, power surges, heat, and tampering can affect hardware such as routers, circuit boards, switches, storage devices, etc.

DDoS (Distributed Denial of Service)

- Distributed denial-of-service attacks change the balance between adversary and victim by marshalling many forces on the attack side.
- To mount a DDoS attack, attacker has to:
  - Conscript an army compromised machines to attack a victim.
  - Plants a Trojan hose on a remote machine not to cause any harm but to make it participate in the attack.
- The attacker repeat the process with many target computers in which each compromised systems then becomes what is known as zombie.
- After a victim is chosen, the attacker sends a signal to all the zombies to launch the attack.

Scripted DoS Attacks

- DDoS are a serious problem because they are easily launched from scripts.
- DDoS attack tools first appeared in mid-1999.
- The tools available now has everything needed: identifies its zombie, installs the Trojan horse, and activates zombie to wait for an attack signal.
- Compromised zombies to augment an attack are located by scanning random computers for unpatched vulnerabilities.

Bots

- The army in DDoS attack is a network of compromised machines ready, willing, and able to assist with the attack.
- Zombies (or bots) are machines running pieces of malicious code under remote control.

Botnets

- Networks of bots used for massive DoS attack, implemented from many sites working in parallel against a victim.
- Also used for spam and other bulk email attacks.
- A network of bots requires a command hierarchy, and the bot headquarters is called a command-and-control center.
- Botnet command-and-control center instructs specific machines to target a particular victim at a given time and duration.

Malicious Autonomous Mobile Agents

- Working largely on their own, can infect computers anywhere they can access, causing denial of service as well as other kinds of harm.
- The developer who sets up the process and establish scheme for updates is sometimes called an inoculation agent.

Autonomous Mobile Protective Agents

- Agents that is modified to look normal to its siblings but in fact to spread a counterinfection.
- For example, a modified agent might look for other hostile agents and pass them an “update” that in fact disabled them.

Cryptography in Network Security

- Symmetric encryption, used for bulk encryption of large quantities of data, perfectly fits network traffic.
- Asymmetric encryption, excels at establishing a trustworthy relationship between two parties, which also applies naturally in a networking situation.

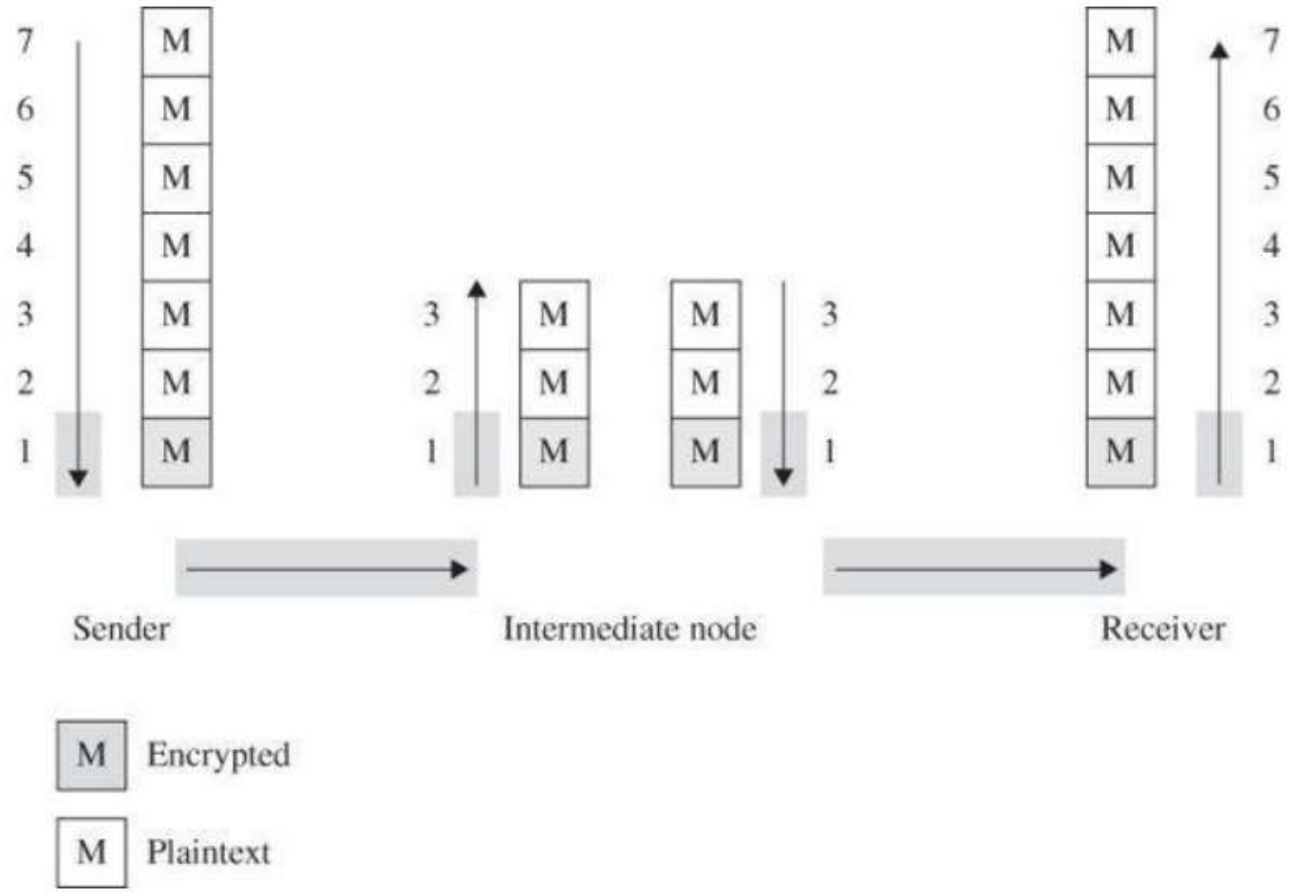
Network Encryption

- Encryption protects only what is encrypted. Cannot protect against malicious attack that intercepts data before the point of encryption.
- Designing encryption algorithm is best left to professionals.
- Encryption is no more secure than its key management. If an attacker can guess or deduce a weak encryption key, the game is over.
- Encryption is not a panacea or silver bullet. A flawed system design with encryption is still a flawed system design.
- In network application, encryption can be applied either between two hosts (called link encryption) or between two applications (called end-to-end encryption).

Network Encryption (Link Encryption)

- Data are encrypted just before the system places them on the physical communications link.
- Decryption occurs just as the communications arrives at and enters the receiving computer.
- In the intermediate node, encryption must be removed in order to determine where next to forward the data, so the content is exposed.
- Link encryption covers a communication from one node to the next on the path to the destination.
- This encryption mode is especially appropriate when the transmission line is the point of greatest vulnerability.

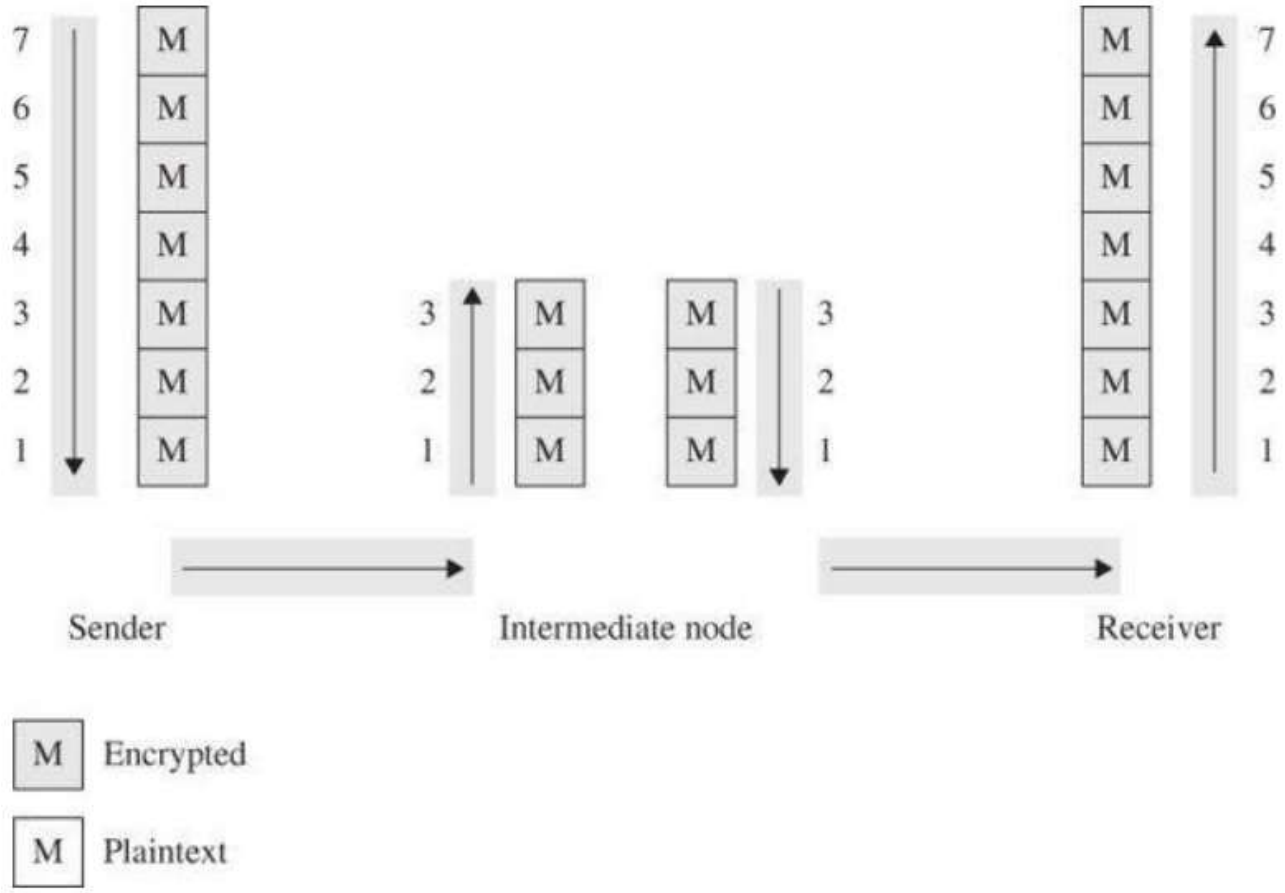
Network Encryption (Link Encryption)



Network Encryption (End-to-End Encryption)

- Provides security from one end of a transmission to the other.
- The encryption can be applied between the user and the host by a hardware device, or alternatively by software running on the host computer.
- In either case, the encryption is performed at the highest levels.
- The message is transmitted in encrypted form throughout the network.
- End-to-end encryption covers a communication from origin to destination.

Network Encryption (End-to-End Encryption)



Browser Encryption

- SSH Encryption; involves negotiation between local and remote sites for encryption algorithm and authentication.
- SSL and TLS Encryption; covers communication between a browser and the remote web host.
  - Cipher Suite; client and server negotiate encryption algorithms for authentication, session encryption, and hashing.
  - SSL Session; client request SSL session, server responds with its public key certificate so the client can determine the authenticity. Client returns a symmetric session key encrypted under the server's public key. Both server and client compute the session key and switch to encrypted communication using the shared session key.

Onion Routing

- In both link and end-to-end encryption, the addressing data were exposed, so someone monitoring traffic between points A and B would know the volume of traffic communicated.
- Onion routing model uses a collection of forwarding hosts, each of whom knows only from where a communication was received and to where to send it next.
- The most popular uses are covert email and private web browsing.
- Onion routing prevents an eavesdropper from learning source, destination, or content of data in transit in a network.

IP Security Protocol (IPsec)

- IPsec implements encryption and authentication in the internet protocols.
- Encapsulated security payload contains descriptors to tell a recipient how to interpret encrypted content.
- IPsec can enforce either or both confidentiality and authenticity.