Wireless LAN Security

Presented by Vikrant Karan

Why Wireless LANs?

- A WLAN allows end users to access e-mail, schedule meetings, and access files and applications on the corporate or university network from conference rooms, classrooms, coworkers' desks, and virtually anywhere on campus.
- User is a mouse-click away from key information and applications regardless of location in a particular facility.

Why Wireless LANs?

- WLANs overcome limitations created by older buildings, leased spaces, or temporary work areas.
- demand for continual network connections without having to "plug in," are driving the adoption of enterprise WLANs.
- With a WLAN, users are able to join or leave a network without plugging or unplugging a cable, thus creating user mobility.
- A study shows that productivity of users increase by 22% with wireless lan environment.

WLAN Security Concerns

- With the increased reliance on WLANs, businesses are increasingly more concerned about network security.
- With a WLAN, transmitted data is broadcast over the air using radio waves.
- This means that any WLAN client within an access point (AP) service area can receive data transmitted to or from the access point.
- With a WLAN, the boundary for the network has moved.

WLAN Security Concerns(Contd..)

- Easy Access: Wireless LANs are easy to find. All wireless networks need to announce their existence so potential clients can link up and use the services provided by the network. We have seen earlier that Beacon frames are used for this purpose according to 802.11 protocol.

WLAN Security Concerns(Contd..)

- Unauthorized Use of Service: Nearly all of the access points running with default configurations have not activated WEP (Wired Equivalent Privacy). This invites hacker to access the network.
- MAC Spoofing and Session Hijacking: 802.11 networks do not authenticate frames. Every frame has a source address, but there is no guarantee that the station sending the frame actually put the frame "in the air."

WLAN Security Concerns(Contd..)

- Traffic Analysis and Eavesdropping: Frame headers are always "in the clear" and are visible to anybody with a wireless network analyzer.
- Higher Level Attacks: Once an attacker gains access to a wireless network, it can serve as a launch point for attacks on other systems.

Wireless security

- security for WLANs focuses on access control and privacy.
- WLAN privacy ensures that only the intended audience understands the transmitted data.
- Traditional WLAN security includes the use of Service Set Identifiers (SSIDs), open or shared-key authentication, static WEP keys and optional Media Access Control (MAC) authentication.

SSID(old method)

- An SSID is a common network name for the devices in a WLAN subsystem.
- it serves to logically segment that subsystem.
- An SSID prevents access by any client device that does not have the SSID.
- an AP broadcasts its SSID in its beacon.
- an intruder or hacker can detect the SSID through sniffing. (A limitation of traditional wlan security)

IEEE suggestions

- two means of client authentication: open and shared-key authentication.
- Open authentication involves little more than supplying the correct SSID. Including MAC address information.
- With shared-key authentication, the AP sends the client device a challenge text packet that the client must then encrypt with the correct WEP key and return to the access point.

Shared key limitaiton

- It is not considered secure:
- a hacker who detects both the clear-text challenge and the same challenge encrypted with a WEP key can decipher the WEP key.
- While traditional WLAN security that relies on SSIDs, open or shared-keys, static WEP keys or MAC authentication is better than no security at all, it is not sufficient for the enterprise organization.

My proposal

- My proposal is to use 2 phase IPSec/IKE over wireless protocol.
- Elements involved in the proposal:
  - Find out the trusted element: The Access Point can only be considered as a trusted element in WLAN.
  - Please note that a compromised AP can lead to following problems:

Problems if AP is compromised

- Allows unauthorized users to access the WLAN
- Invalid billing information.
- Loss of privacy of a valid user.
- Unauthorized use of QoS if supported.

Brief overview of IPSec

- IPsec provides network-layer security that runs immediately above the IP layer in the protocol stack.
- It provides security for the TCP or UDP layer and above.
- It consists of two protocols, IPsec ESP and IPsec AH.

IPsec

- IPsec ESP provides confidentiality and message integrity, IP header not included.\
- AH provides only message integrity, but that includes most of the IP header.
- Since authentication of the IP header does not significantly improve security, I am proposing to use ESP with transform IDs defined in next slide.

WLAN Profile for IPsec ESP

- IPsec Transform Identifier (1 byte) is used by IKE to negotiate an encryption algorithm that is used by IPsec.
- As per now my finding reveal that following transform IDs are successfully used: ESP-3DES and ESP-NULL.

WLAN Profile for IPsec ESP

- The IPsec Authentication Algorithm is used by IKE to negotiate a packet authentication algorithm that is used by IPsec.
- Following authentication algorithm can be used: HMAC-MD5 and HMAC-SHA.

Key management protocol

- IKE as one of the key management protocols for IPsec:
- IKE key management can be completely asynchronous to signaling messages and should not contribute to any delays during communications setup.
- IKE is a peer-to-peer key management protocol. It consists of 2 phases.

IKE phases

- In the first phase: a shared secret may be negotiated via a Diffie-Hellman key exchange. This key exchange can then be used to authenticate the second IKE phase.
- The second phase negotiates another secret, used to derive keys for the IPsec ESP protocol.

WLAN profile for ESP

- First IKE Phase:
  - IKE Authentication with Signatures: both access point and wlan users can be authenticated with X.509 certificates and digital signatures.
  - IKE Authentication with Pre-Shared Keys: A pre-shared key can be entered in both access point and the users machine. This shared secret can be used for authentication purposes.
  - using pre-shared keys, the strength of the system is dependent upon the strength of the shared secret. Thus shared secret can be made as random as possible.

Second phase of IKE

- In the second IKE phase, an IPsec ESP SA is established, including the IPsec ESP keys and ciphersuites.
- First, a shared second phase secret is established, and then all the IPsec keying material is derived from it using the one-way function, e.g., diffie-hellman exchange.
- The second-phase secret is built from encrypted nonces that are exchanged by the twoparties thus establishing the SA’s.

My next goal

- Learn ns-2 simulator to run ipsec/ike configuration. If this functionality does not exist on ns-2 simulator, then I would like to implement this.
- Simulate one access-point and multiple users in as per wireless environment.
- Analyze the performance of WLAN traffic considering all the security measures.