Wireless Security Threats and Countermeasures

Wireless and Optical Communications Conference 2007

Steve Wang
Distinguished Member of Technical Staff
Alcatel-Lucent
Lilse, IL 60532
April 2007

AGENDA

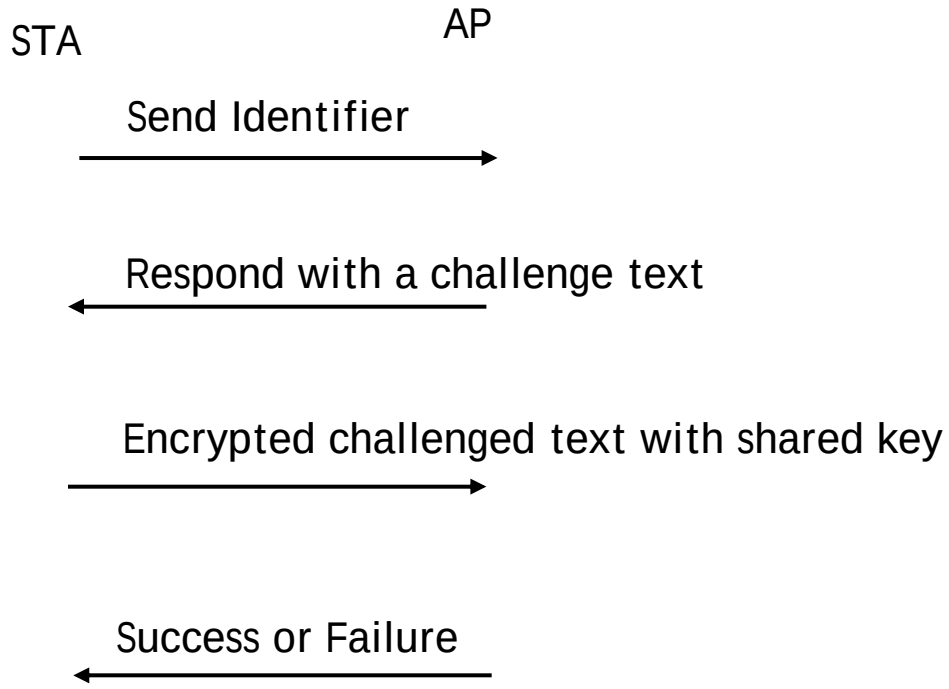
- Wireless System Security Issues
- Wireless LAN (Wi-FI) Security Architecture
- Wi-Fi Security Vulnerability and Countermeasures
- Wireless Broadband (WiMAX) Security Architecture
- WiMAX Security Vulnerability and Countermeasures
- Conclusion

Wireless System (Wi-Fi) Security Issues

- It was reported that Wireless access could bring organizations up to 22% of productivity
- But the deployment of Wi-Fi in the organization is well below the expectation. The major concern is SECURITY.
- Lack of physical boundary in a wireless network will provide a chance of parking lot attack.
- Service Set Identifier (SSID) Broadcast issues
- DHCP impacts security – Intruders could be assigned on the same network and access to your system much easily.
- Security was not well thought in the beginning of deployment and may require too much cost to update security on millions of devices in use after vulnerabilities are discovered.
- Denial of service attacks – Keep other users from accessing services by either producing enough strength of RF interference or sending continuous stream to occupy bandwidth – unlicensed spectrum.

WEP Security Architecture – Authentication and Encapsulation

Authentication:



Encapsulation:

Keystream = IV + Shared key encrypted with RC4

Plaintext with CRC-32 encrypted the keystream using exclusive OR operation. Prepend IV to the Cipher

WEP Security Architecture

- **Wired Equivalent Privacy (WEP) Security Goals and Security Architecture:**
  - **Confidentiality – prevent Casual eavesdropping**
  - **Access Control – Protect access to a wireless network and then to Internet.**
  - **Data Integrity – Prevent tamping with transmitted messages**
- **WEP relies on the secret key shared between a mobile station and an access point. It implements the following steps attempting to reach the goals:**
  - **Shared Key authentication by exchanging four management frames – no mutual authentication**
  - **Encryption using RC4 Stream Cipher via the keystream generated by the shared key and an Initialization Vector (24 bits)**
  - **Employ CRC-32 for checking integrity of messages**

Vulnerability of WEP

- Keystream generated by Initial Vector (IV) and the secret key is used for encryption, The two ciphers using the same keystream will make it computation possible to recover plain text. (XOR of two ciphers = XOR of two Plain text)
- CRC is designed to detect random errors in the message but not for a cryptography secure authentication code. It means that attackers can make modifications to the an encrypted message without fear of detection. Attackers may use it to modify destination IP address and re-direct packets to collect identity information.
- Once the keystream is detected, attackers can transmit frames to network at will. This is called active attack.
- Fixed authentication message and format allow attackers to determine the secret key much easily.
- Once shared keys are known, attackers can provide a false access point to intercept traffic and steal sensitive information. Tools are available (Airsnort and WEPcrack, .etc) to recover a secret key.

Countermeasures of WEP Vulnerability

- Some people has found out that many corporations are still using open authentication in their network. This should be changed.
- Avoid to use the same secret key for all users connecting to the access point, like SSID (company name) of the access point.
- Implement key management system to distribute keys. The WEP standard does not specify how this can be done.
- Every MPDU should use a new IV in order to reduce the chance of keystream reuse. Attackers might need to spend a great deal of effort to find instances of keystream re-use
- Substituting CRC with Message Authentication Code such as SHA1-HMAC, could prevent the ICV attack. But this may cause interoperability problem with millions of mobile stations in use.
- Implement more robust authentication protocol like 802.1x would fight with the authentication problem of WEP.

Security Architecture of Wireless Protected Access (WPA)

- WPA is a pre-standard of IEEE802.11i for enabled WEP devices. It provides two enhancements:
  - TKIP (Temporary Key Integrity Protocol) - Improved data encryption through the temporal key integrity protocol (TKIP). TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys haven't been tampered with.
  - User authentication, which is generally missing in WEP, through the Extensible authentication protocol (EAP). WEP regulates access to a wireless network based on a computer's hardware-specific MAC address, which is relatively simple to be sniffed out and stolen. EAP is built on a more secure public-key encryption system to ensure that only authorized network users can access the network.
- WPA2 implements 802.11i and use Advanced Encryption Standard (AES) encryption, key management, and IEEE 802.11x for Authentication. It supports both consumers (pre-shared key) and enterprises (802.11x Radius server) modes of authentication.

Vulnerability of WPA

- Michael Message Integrity (MIC) Key used as part of TKIP can be discovered via a known plaintext and MIC code. This technique is called inverting MIC.
- One way authentication of the supplicant (user) to the access point can expose the supplicant to the Man in the middle attack with an adversary acting as an access point to the client. Although EAP-TLS could provide strong mutual authentication but is not mandatory.
- Attackers can forge a EAP success message to a supplicant on the behalf of authenticator and start a simple Man in Middle attack to get all client's messages to pass through the attacker.
- Attackers can spoof MAC disassociate message to hijack the just established session due to loose coupling between 802.1x process and lower layer process and lack of message authenticity.
- WPA-PSK (pre-Shared Key) eliminates the strong authentication that comes with 802.1X services. The key can be exposed via a brute force attack.
- Vulnerable to DOS attack by triggering ongoing series of shutdown messages in BS due to a hacker who sends two bad MIC tag in quick succession.

Countermeasures of WPA Vulnerability

- Place the MIC code in a fixed location in the frame (before message body) so that it will not be exposed easily.
- Turn off countermeasure to shut down the Access Point after DOS is detected or send an alarm to inform security personnel to scan parking lot or neighboring areas to locate hackers.
- Add Message authenticity for management frames to avoid for hijacking sessions.
- Adding new EAP message authenticator to preserve the integrity of EAPOL message to avoid Man in Middle attack.
- Provide mutual authentications among supplicant, authenticator and authentication server (Radius).
- Employ longer than 20 characters of passphrases for pre-shared key to deter dictionary/brute force attack.

WMAX Security Architecture – IEEE802.11e 2005

- Create a privacy sub layer inside MAC protocol stack to provide access control and confidentiality of the data link.
- Security Association maintains the security state relevant to a connection. It contains cryptography information, IV, and key hierarchy, .etc.
- Each mobile station is identified with a X.509 certificate profile, which was provisioned by manufacturers.
- It uses Privacy Key Management (PKM) protocols to support security management exchanges between the BS and the MS for authentication and credential information of the MS.
- Both user and device authorization/authentication could be supported through a 802.1X model (ASN – authenticator, AAA – Authentication Server).
- Encryption protocol is AES with 128, 192 or 256 bits. WiMAX forum and some vendor (Intel) are pushing for 256 bits of AES encryption.

WiMAX Security Vulnerability – 802.16e 2005

- Physical layer attack is still possible, like battery drain attack and jamming/Scrambling of signals. But no standardization for fighting with the attack is available.
- Expanding larger physical coverage than Wi-Fi, WiMAX may be susceptible to more vulnerability. It increases chance of various security attack.
- No mutual authentication is performed between MS and BS so a rogue BS can play man-in-middle attack.
- Certificate based authentication can be compromised by a masquerading BS.
- Management frames are not encrypted and can be intercepted or modified for a replay attack.
- DOS attack by flooding BS with high numbers of messages to authenticate.
- Customers, service providers may lull into a false sense of WiMAX security – Should learn from the past Wi-Fi experience and not repeat the same mistake.

WiMAX Security Countermeasures

- Require Mutual authentication between Subscriber Stations and base stations to avoid Man in the middle Attack. It is suggested that a strong EAP (EAP-TLS/EAP-TTLS) based authentication be used between MS and BS.
- Employ a strong Message Authentication Code (MAC) for management messages.
- Turn on both user and device authentications if possible.
- Provide an Intrusion Detection System close to the wireless segment firewall to detect DOS attack.
- Segregate RAN network from other networks (core network, and internal network) using firewall to implement proper security policies on these firewalls.

Conclusions

- In the past 5 years, Wi-Fi has been deployed over millions of mobile stations, and its many vulnerabilities are uncovered.
- Sprint Nextel plans to roll out two WiMAX markets this year and rest of them by 2008. More vulnerability of WiMAX might be uncovered once the widespread of WiMAX deployment rollouts.
- The security of Wireless architecture only addresses link layer security, but the access right with authorization has become more important particularly for supporting variety of user populations. Multiple layers of security is required
- Access points, if possible, should be placed outside of enterprise's firewall so that attackers or guests will not allow to access to a company's internal network.
- In order to provide full security control regardless of vulnerability to be exposed by wireless networks, some existing security applications, like VPN, stateful firewalls, and VLAN, .etc may be used for added protections.
- MS needs encryption acceleration to handle AES processing demand. The capability in MS may not be available in the initial phase of large WiMAX deployment.
- Integration and interoperability of various security protocols, key management, .etc among certifying hardware is a big challenge.