Wireless Security - Encryption

Joel Jaeggli
For
AIT Wireless and Security Workshop

Wireless link layer encryption

- Once people started puting data on the air the desire to protect that data became readily apparent.
- Multiple Goals
  - Restrict access to the wireless network
  - Protect the traffic from observation
  - Data integrity
  - Preclude man in the middle.

MAC filtering.

- Early approach
  - Preclude MAC address from associating with an AP
  - Provides no on-the-air protection
  - Does limit access to the network
    - But only to really stupid hackers

WEP

- Wired Equivalent Privacy
- And approach to shared key encryption that was supposed to provide equivalent to wired protection for wireless traffic
- Turns out it wasn't...
- Built in the era of watered down encryption due to export restrictions.
- It turned out that 64bit wep keys were a bit more vulnerable to factoring (40 bits or less) than previously thought. With the result that the key can be recovered in a matter of minutes.

WPA and WPA2

- WPA (Wifi Protected Access) was prepared by the IEEE as an immediate and intermediate setup to address the limitations in WEP.
- The full 802.11i standard when available was implemented by devices with WPA2 logo compliance
- Unfortunately there are a range of implementations.
  - Older devices that only support WEP,
  - Standard Windows XP machines that can support WEP or WPA
  - Systems with new drivers that support WPA2
  - ETC

TWO flavors of WPA/WPA2

- Enterprise
  - Uses an 802.1x authentication manager
- Personal
  - Supports the use of pre-shared keys.
  - One improvement over WEP is the use of Temporal Key Integrity Protocol (TKIP). Keys are changed dynamically as the system is used with the result that attacks against the keys used on the network become much more challenging.

WPA/WPA2 personal challenges

- The shared keys is known by other humans and generally has to be stored. So...
  - It can be lost and re-keying means distributing a new key
  - If you have the key you can create a rogue access point because there's no convenient way to authenticate the access point to the client.

WPA/WPA2 Enterprise

- WPA has an incomplete pre-standard implementation of the enterprise profile so WPA2 enterprise really should be the only serious consideration if pre-shared key is inadequate.
  - Cisco didn't help the situation any by implementing an early incomplete and not very secure variant in Cisco CCX (Cisco certified extensions) based on mschap called Cisco LEAP.
- WPA2 uses the IETF EAP (Extensible Authentication Protocol) for which there are an number of plugin authentication modules.

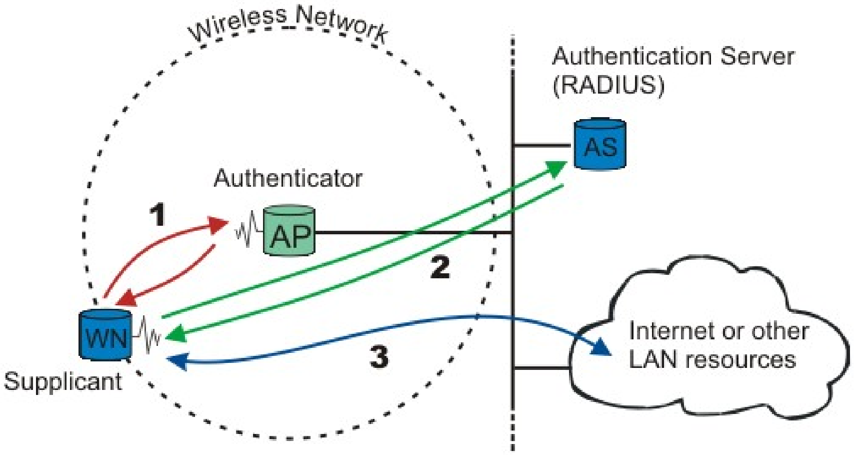
WPA2 eap methods

- Most relevant methods:
  - EAP TLS, based on a secure sockets layer key exchange. Allows for strong mutual authentication (client to network and network to client). Perversely while it may be the strongest method, it's seldom implemented because the certificate management and distribution is considered onerous (users certificated need to be installed on each system they use).

WPA2 EAP methods

- EAP PEAP
  - The protected extensible authentication protocol
  - Uses server side certificates to authenticate the server.
  - Authentication on the client side is done via mschapv2 (ie username and password)

802.1x EAP



1)The authenticator sends out the EAP-Request identity to the connecting supplicant the supplicant responds with the EAP-response packet

2) The authenticator forwards to the authenticating server. The authenticating server accepts the request, the authenticator sets the port to the "authorized" mode and

3) Normal traffic is allowed

WPA2 data

- In WEP and WPA once the shared key was defined the rc4 stream cipher was used to secure the data on the wire.
- With WPA2 the AES block cipher is now used.

EAP and FreeRadius

- One of the reference implementations of eap authentication is in Free Radius.
- Naturally that make it an attractive target for deployment as an authentication server.
- Leveraging a centralized store of authentication credentials can be an attractive way to deploy multiple services.
  - Might end up with a model such an ldap backend and a Free Radius front-end for authentication and perhaps accounting.

About the exercise.

- It is common for equipment where both ends are controlled by the same party (a network operator) for the equipment to be configured using a mutually shared secret. (tcp md5 for example, radius clients nad servers for another)
- We are going to configure both ends of our radio link to use the same wpa2-tkip shared secret.
- We're also going to lock the mac addresses on both ends of the link not so much as a security feature but rather to prevent the APs from roaming if another radio with the same ssid came online.

Bibliography

- EAP PEAP authentication setup on ubuntu http://ubuntuforums.org/showthread.php?t=478804
- EAP PEAP setup in freeradius wiki
- http://ubuntuforums.org/showthread.php?t=478804