

Wireless Security



Hal Pomeranz

Deer Run Associates

hal@deer-run.com

Think About Network Architecture

- Two basic choices:
 - Wireless network is equivalent to internal LAN
 - Wireless network requires firewall/VPN access to internal resources
- Deciding factors:
 - "Visitors" needing regular access
 - Wireless architecture/hardware limitations
 - Wireless client limitations

Basic Wireless Security

- MAC Address Filtering
 - Useful on small networks
 - Can be a pain at the enterprise level
 - MAC addresses can be spoofed!
- Client Isolation
 - Can wireless clients attack each other?
- Antenna positioning
- Antenna power settings

Wireless Encryption Options

- Static WEP
 - Easy to configure, easy to crack
- WPA w/ Pre-Shared Keys (WPA PSK)
 - Roughly the same as WEP
- 802.11i (aka "WPA2", "Enterprise WPA")
 - Higher levels of security, pain to configure

About 802.11i

- Uses 802.11x network authentication:
 - Can use passwords, certificates, token cards...
 - Need a RADIUS server on the network
- AES for data encryption:
 - Replaces weaker RC4 from earlier standards
 - Session keys regularly regenerated to help prevent brute-force attacks

Lots of Different Pieces

- ❑ RADIUS Server
- ❑ Certificate Authority
- ❑ Loading Client Certificates
- ❑ Configuring Wireless Profiles on Clients
- ❑ Wireless AP Configuration

RADIUS Server Options

- Personally, I use FreeRADIUS (on Unix) but mostly for historical reasons
 - Active user support community
 - Fairly complex configuration
- List of other RADIUS Servers for Unix:
http://wiki.freeradius.org/Other_RADIUS_Servers
- Windows: use Microsoft IAS or Cisco ACS

FreeRADIUS Notes

- Critical files in `${INST}/etc/raddb`:
 - `radiusd.conf` – General server config
 - `eap.conf` – Wireless security config
 - `clients.conf` – Define APs, shared secrets
 - `users` – Text database for user accounts
- Can also store users in MySQL, LDAP, ...
- Use "`radiusd -x`" for debugging

Your Own Private CA

- Use OpenSSL to create your own root cert
- Use fake root cert to sign:
 - Certificate for RADIUS server
 - Per-user certificates
- FreeRADIUS supplies `CA.certs` script—this script is broken, use my version
- *Think very hard about certificate lifetimes before deployment!*

Loading Certificates (Windows)

- ❑ Copy root public key and user cert to client
- ❑ *Start...Run...mmc* (Microsoft Management Console)
- ❑ *File...Add/Remove Snap-in...* and add the "Certificates" snap-in
- ❑ Expand folders to "Trusted Root Certification Authorities"
- ❑ Right click, choose *All Tasks...Import*
- ❑ Use the wizard to import CA root public key
- ❑ Can also use *mmc* to import user cert, or just right-click user cert file and choose *Install PFX* which opens the same wizard
- ❑ *Do not* "enable strong private key protection" option on user cert

Oh heck, how about a demo instead???

Access Points and DD-WRT

- All (consumer grade) access points suck!
- It's mostly due to crappy, unstable firmware
- DD-WRT is free Linux-based firmware image that runs on many different access points:
 - Admin access via HTTP, HTTPS, and/or SSH
 - Built-in Firewall and [P|S]NAT support
 - PPTP and OpenVPN support
 - RIP/OSPF/BGP routing, VLANs, QoS, IPv6
 - SNMP, NTP & Samba clients, Kai, UPnP, SIPatH

DD-WRT Wireless Security

The screenshot shows the DD-WRT Wireless Security configuration page in Mozilla Firefox. The browser window title is "DD-WRT - Wireless Security - Mozilla Firefox". The address bar shows "https://airstation/WL_WPATable.asp". The page header includes the DD-WRT logo and "CONTROL PANEL". The main navigation menu has tabs for Setup, Wireless, Security, Access Restrictions, Applications & Gaming, Administration, and Status. The sub-navigation menu has tabs for Basic Settings, Radius, Wireless Security, MAC Filter, Advanced Settings, and WDS. The "Wireless Security" section is active, showing the "Wireless Encryption" settings. The "Security Mode" is set to "WPA2 RADIUS Only", "WPA Algorithms" is set to "AES", "RADIUS Server Address" is "192.168.1.10", "RADIUS Server Port" is "1812", "WPA Shared Key" is masked with asterisks and has an "Unmask" checkbox, and "Key Renewal Interval (in seconds)" is "3600". There are "Save Settings" and "Cancel Changes" buttons at the bottom. A "Help" section on the right provides information about the "Security Mode".

DD-WRT CONTROL PANEL

Firmware: DD-WRT v23 SP1 Final (05/16/06) std
Time: 13:20:12 up 2:25, load average: 0.07, 0.02, 0.00
WAN disabled

Setup **Wireless** Security Access Restrictions Applications & Gaming Administration Status

Basic Settings Radius **Wireless Security** MAC Filter Advanced Settings WDS

Wireless Security Help more...

Wireless Encryption

Security Mode: WPA2 RADIUS Only

WPA Algorithms: AES

RADIUS Server Address: 192, 168, 1, 10

RADIUS Server Port: 1812

WPA Shared Key: ***** Unmask

Key Renewal Interval (in seconds): 3600

Save Settings Cancel Changes

Done airstation

Useful URLs

- Software:

<http://www.freeradius.org/>

http://www.dd-wrt.com/wiki/index.php/Main_Page

- Good HOW-TO Article (parts 2&3 of 3):

<http://www.linuxjournal.com/article/8095>

<http://www.linuxjournal.com/article/8151>

- More info on XSupplicant (Unix Clients):

http://www.tldp.org/HOWTO/html_single/8021X-HOWTO/