Migrating from WEP to WPA/WPA2

Joshua Wright

Aruba Networks

jwright@arubanetworks.com

Start sending questions to “q@sans.org”!

Introduction

- Identifying the need to move to WPA/WPA2
- Defining WPA/WPA2
- Planning a migration
- Configuring hardware
- Configuring clients
- Monitoring the network

Is WEP That Bad?

- Key is recoverable from cipher text
- No replay protection
- Attacker can inject arbitrary frames into WEP networks
- DWEP implementations often lack key rotation
- Weak ICV allows plaintext recovery

Organizations cannot assume any level of security or privacy when relying on WEP

The Challenge

- Upgrading to WPA/WPA2 is not trivial
  - New infrastructure (hardware/software), upgrades
  - Client configuration tasks
  - AP reconfiguration
  - Testing, troubleshooting
- Many legacy devices only support WEP
  - Few options other than to isolate vulnerable networks, devices

What is WPA?

- WiFi Protected Access, defined by the WiFi Alliance, 802.11i specification
- Improves security of legacy devices
- Designed to work with majority of devices designed only for WEP
- Replaces WEP with TKIP algorithm
  - Uses RC4 for encryption
- Stopgap security, not intended for long-term use

What is WPA2?

- Recommended encryption mechanism for wireless networks
- Defined by WFA, IEEE 802.11i
- Includes many benefits of WPA
  - Uses AES/CCMP for encryption
  - Accommodates pre-authentication for faster roaming, secure transition
- Only works with newer hardware

WPA-PSK vs. WPA-Enterprise

- WPA-PSK intended for consumer networks
  - Uses pre-shared key for authentication to the wireless network
  - Vulnerable to offline dictionary attacks
- WPA-Enterprise intended for enterprise networks
  - Requires EAP authentication, certs

coWPAtty

- Designed to illustrate weakness in simple passphrase selection

```
mercury:~/cowpatty $ ./cowpatty -d words.db -r wpapsk-linksys.dump -s linksys
cowpatty 2.5 - WPA-PSK dictionary attack. <jwright@hasborg.com>

Collected all necessary data to mount crack against passphrase.
Starting dictionary attack.  Please be patient.
key no. 100000: Mennonite
key no. 200000: accommodee

The PSK is "adequately-capitalized".

210644 passphrases tested in 2.78 seconds:  75661.57 passphrases/second
mercury:~/cowpatty $
```

Pentium 4 2.8 GHz

Planning a Migration

- Purchasing policy
- Select an EAP type
- Establish or select a Certificate Authority
- Configure RADIUS authentication
- Establish transition network
- Client configuration options

Purchasing Policy

Continuing to purchase non-WPA2 certified hardware will perpetuate weak wireless security!

- Set a purchasing policy:
  - Require all wireless equipment to be WPA2 certified
  - Validate vendors: http://certifications.wi-fi.org/wbcs_certified_products.php)
  - Plan a hardware deprecation schedule for non-compliant equipment

Selecting an EAP Type

- Some EAP types should never be used
  - LEAP, EAP-MD5
- Selection of an EAP type depends on several factors
  - Dominant client operating system
  - Authentication database architecture
  - Availability of PKI infrastructure

EAP Options

- Windows-centric organizations benefit from PEAPv0
  - Disclosure of username with XP supplicant
- Alternate authentication mechanisms warrants TTLS
  - Tokens, OTP, two-factor, biometrics
- EAP/TLS very secure if PKI is available
  - Deployed with smart cards, very secure

“Simple” EAP Matrix

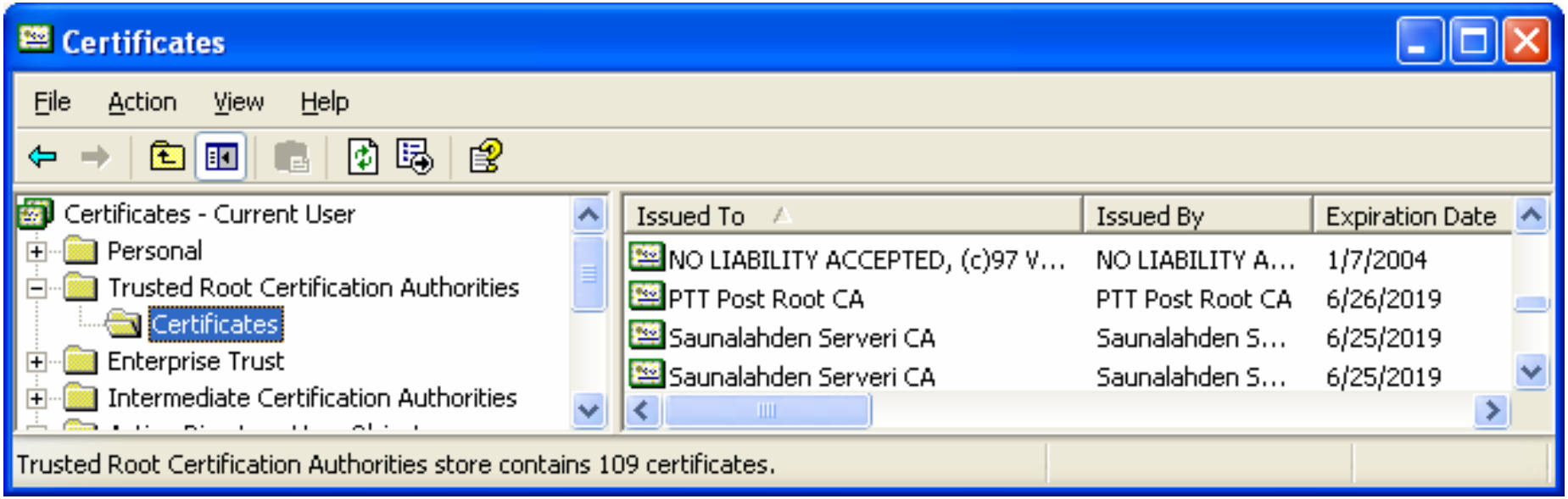
	Client Cert.	Server Cert.	Outer Protocol	Inner Protocol	Smart Card Support
PEAP-EAP/TLS	Yes	Yes	TLS	EAP/TLS	Yes
EAP/TLS	Yes	Yes	TLS	None	Yes
PEAPv2	No	Yes	TLS	Multiple	Yes
PEAPv1	No	Yes	TLS	EAP-GTC	Yes
EAP-FAST	Yes (PAC)	Yes (PAC)	TLS	EAP-GTC	Yes
TTLS	No	Yes	TLS	Multiple	Yes
PEAPv0	No	Yes	TLS	MS-CHAPv2	No
LEAP	No	No	MS-CHAPv2	None	No

Certificate Authorities

- Option 1: Deploy in-house CA
  - Often complicated to setup, manage
  - Requires more client configuration
  - Greatest flexibility, accommodates EAP/TLS
- Option 2: Purchase from commercial CA
  - Simplified installation, configuration
  - Must renew certificates before expiration
  - Cost-prohibitive for wide-scale deployment

Selecting a Commercial CA

- Select a vendor that is already trusted by clients
- Windows: Start → Run → certmgr.msc



Local Certificate Authority

- Select a tool for CA management
  - Windows CA Server, OpenSSL, Funk
- Windows CA server supports automatic enrollment
  - Useful with integrated AD
- OpenSSL flexible, available on all Unix OS's

Configure RADIUS

- EAP authentication requires RADIUS
- Windows IAS limited to PEAP, EAP/TLS, EAP-MD5
- FreeRADIUS, Funk SBR, Meetinghouse AEGIS support many EAP types
- Ensure interoperability/support for your current, planned authentication types
- Examine logging options, reporting!

Securing RADIUS

- Security of RADIUS relies on shared-secret
  - Susceptible to offline dictionary attacks
- Use strong passwords, do not re-use
- Consider Funk password amplifier

http://www.funk.com/Download/PassAmp.msi

Establish Transition Network

- Often impractical to cut-over all nodes in a short time
- Transition network for legacy and migrated client concurrency
- Multiple SSID/VLAN options available
  - Establish a "xyzsecure" SSID for transition
  - Vendor-specific, refer to documentation
- Carefully monitor both networks during transition, secure network exposed!

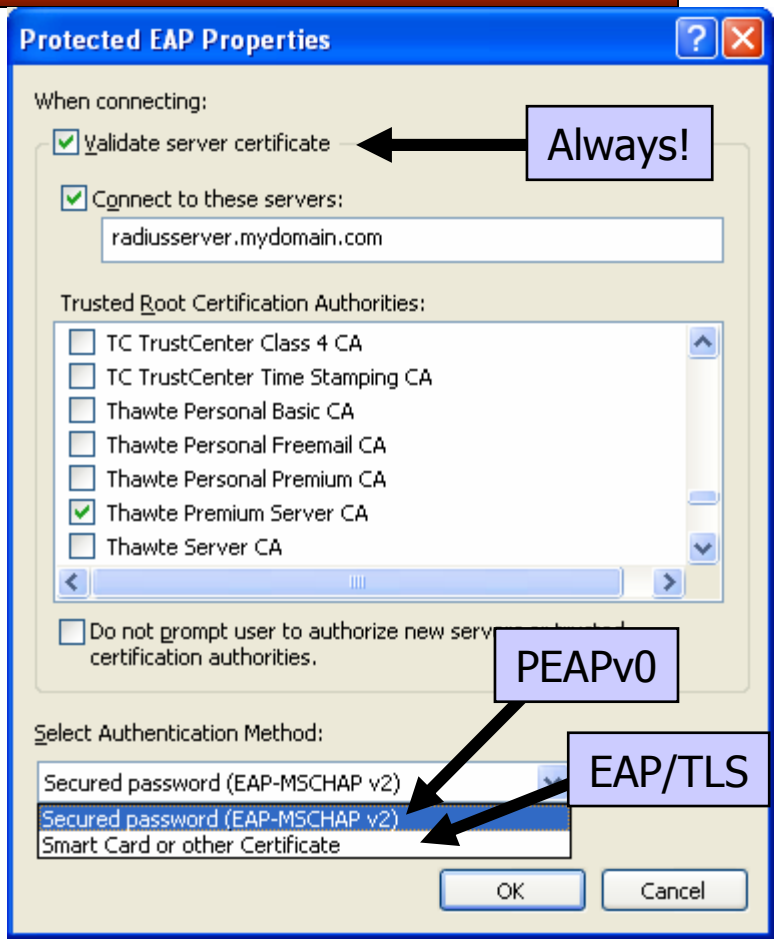
Configuring Clients - CA

- Local CA requires root certificate trust on client systems
- Options for distribution:
  - Windows AD GPO deployment
  - Manual copying, import
  - Automated install with IE

http://pkidev.internet2.edu/rootcerts/

Configuring Clients - EAP

- Ensure only the desired EAP type is configured on clients
- Require validation of server certificate!
- Specify RADIUS servers authorized to authenticate
- Select trusted root CA
- Consider third-party supplicant



Configuring Clients – SSIDs

- Restrict administrator access to local workstations whenever possible
- Limit permitted SSIDs for association
  - Windows XP enforcement with GPO
- Mandate personal firewalls for wireless users
- Home user policy with corporate laptops

Hotspotter - Client Attack Tool

- Simple tool for Linux systems
- Watches channel for probe requests
- Matches probe network to list of attack networks (e.g. “tmobile”)
- Configured soft-AP to become probed network (“Hi, I’m tmobile!”)
- Executes a script to attack client

Wireless clients require personal firewalls, patch management

Network Monitoring

- Strong encryption and authentication does not solve all!
  - Home users and vulnerable AP's
  - Hotspot users and vulnerable workstations
  - Wireless driver flaws, exploits
  - Rogue networks
- Consider deploying wireless IDS
- Add regular network monitoring to your regimen

http://www.sans.org/webcasts/show.php?webcastid=90561

Summary

- WPA/WPA2 provide strong encryption with EAP authentication
- Design a wireless policy for your organization
  - Define usage for organizational hardware, at home, office, hotspot
- Select EAP type based on infrastructure, authentication requirements
- CA and RADIUS options
- Temporary transitional network
- Client security needs

Questions?

Please send questions to "q@sans.org". Thank you!

-Joshua Wright
jwright@arubanetworks.com