wireless security strategies and challenges

David Morton
dmorton@u.washington.edu


Not related to wireless security…but I took this pic on campus and looking for excuse to show :)

Section one -
WEP, WPA & 802.1x

to encrypt or not to encrypt

- Encryption
  - WEP, WPA-PSK, 802.1x w/WPA
- Open, unencrypted wireless
  - Counter intuitive?

Why Unencrypted Wireless?

- University of Washington wireless is unencrypted.
- Treat all networks as untrusted, even wireless.
- Use application level encryption across all connections.
  - Ideally end-to-end (HTTPS/SSL, SSH, etc)
- Easiest to use and support

What about VPN?

- Good option - can protect wireless and some wired infrastructure.
- But... (there's always a but)
  - Often requires client and client config maint
  - All traffic may not be encrypted (split tunnel)
  - Most secure when term point is closest to dest
  - IP Addresses still viewable wirelessly

Wireless Encrypt - WEP

- WEP is broken.
- Don't use it-
  - Creates false since of security
  - Tools to break are easy and readily avail
  - Shared secret is easily discovered
  - It's hardly a secret when you have to tell everyone
- But...
  - Some devices don't support other encryption

Wireless Encrypt - WPA

- Wifi Alliance name for subset of 802.11i
- Primary flavors
  - WPA-PSK
  - 802.1x with WPA
  - WPA2 not yet widely adopted

WPA-PSK
(pre-shared key)

- WPA-PSK a "secret" is shared between client and access point
- WPA support is advertised in an IE (information element) of the access point's Beacon
- Wait, wasn't WPA-PSK hacked?
  - Yes, short passwords are vulnerable to dictionary attack (coWPAtty, et al)
  - short passwords easier to crack than WEP
  - mixed cased, numbers & symbols recommended

WPA-PSK
(pre-shared key)

- 802.11i recommends 20 character passphrase
- After initial auth, keys are automatically rotated
- WPA-PSK isn't a great solution > a few users
- Larger nets should use 802.1x with WPA

802.1x with WPA

(aka 802.1x)

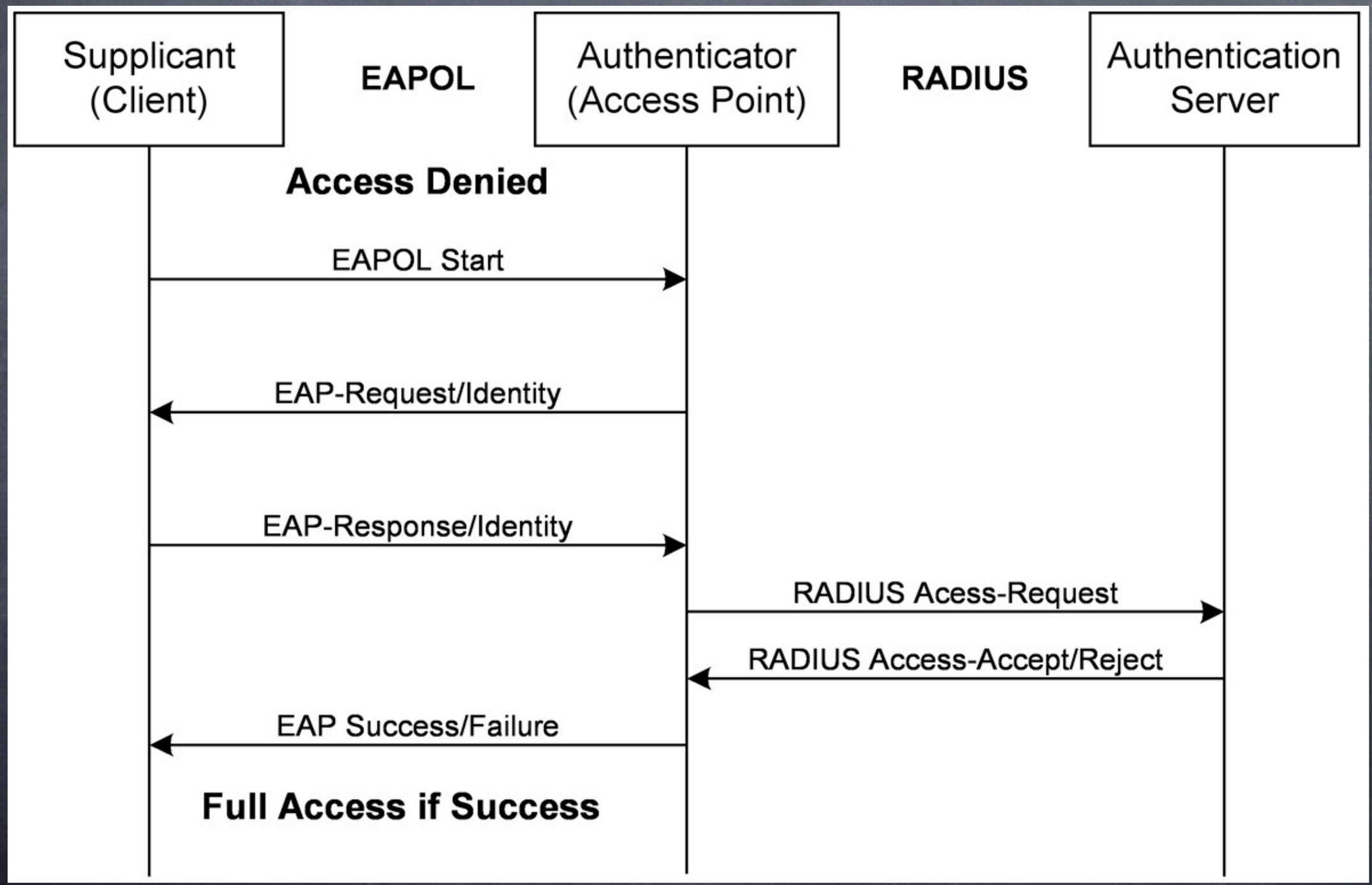
- Often referred to simply as 802.1x
  - full alphabet soup of a common deployment
    802.1x with PEAP v0/MSCHAP v2, WPA, TKIP (or AES), MIC with full funk style server cert check
- Yea, 802.1x can be complex
  - Requires client software (supplicant)
  - Choice of appropriate "EAP" type
  - Network upgrades possible
  - New Servers or server upgrades possible
  - Encryption, complexity harder to support

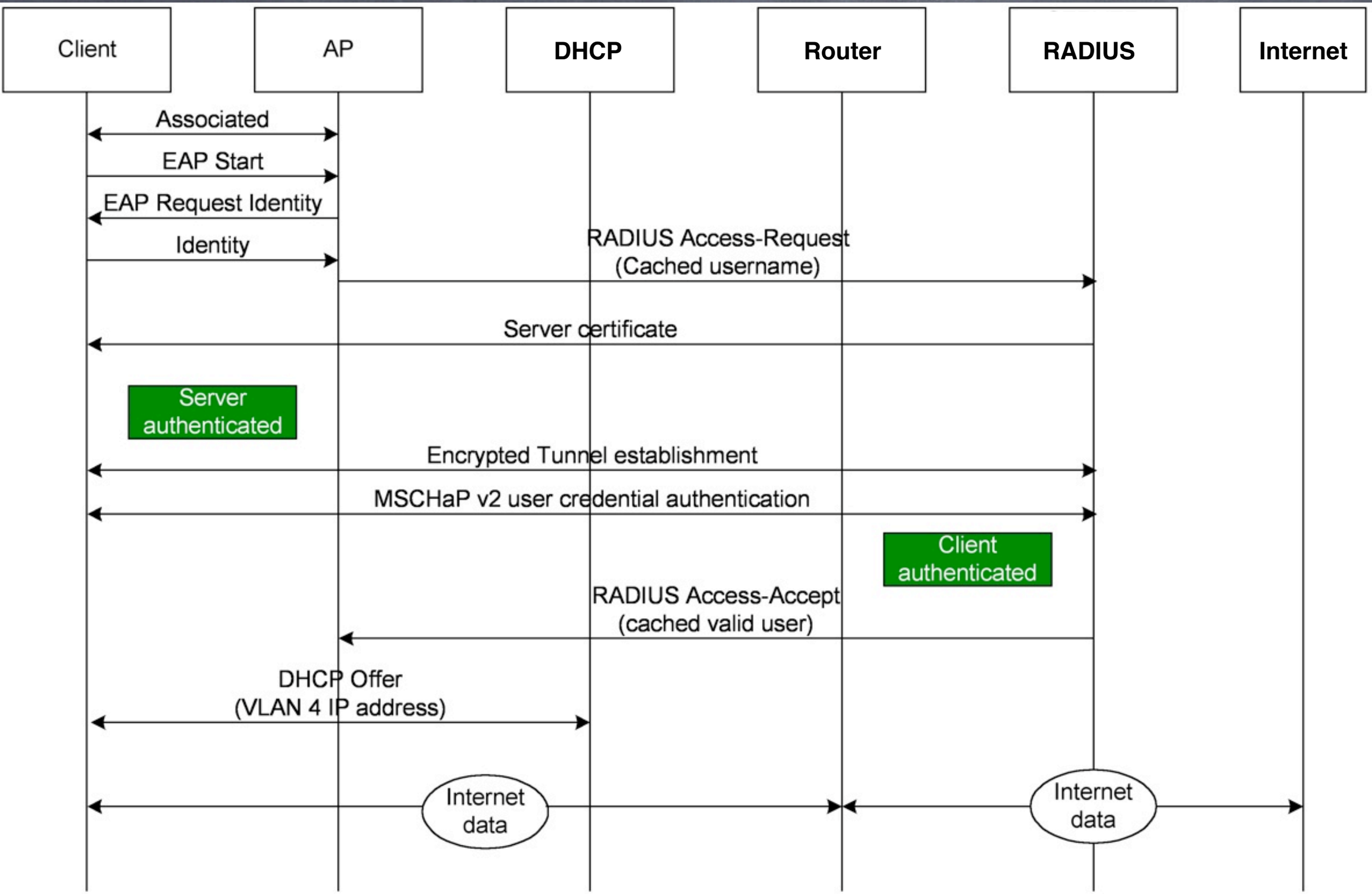
802.1x with WPA

(aka 802.1x)

- But, provides a fair amount of protection
  - No IP passed until properly authenticated
  - PEAP/TTLS pass authn in encrypted tunnel
  - RADIUS (used for authn) well understood & flexible
  - Federation and roaming well understood
  - NAC, health checks, VLAN assignment and other policies based solutions are all possible
  - Timers to force periodic re-authentication

802.1x basic call flow




Client
AP
DHCP
Router
RADIUS
Internet
Associated
EAP Start
EAP Request Identity
Identity
RADIUS Access-Request
(Cached username)
Server certificate
Server authenticated
Encrypted Tunnel establishment
MSCHaP v2 user credential authentication
Client authenticated
RADIUS Access-Accept
(cached valid user)
DHCP Offer
(VLAN 4 IP address)
Internet data
Internet data

802.1x future

- Some feel 1x is too complex, especially support
- Upcoming standards
  - 802.1ae - Link layer encryption
  - 802.1af - extension to 1x to support 802.1ae
  - Improved MIBs for management/support
- Higher Ed to benefit wider enterprise adoption

Section two -
challenges
(present and future)

Wireless offers unique challenges

- Shared media
  - Block wireless to wireless P2P (ie PSPF)
- Session hijack - unencrypted esp vulnerable
  - Sniff wireless to find IP and take it
  - Authorized ARP can help
- Cheap options for remote eavesdropping
  - my favorite is the 3-mile chinese spoon

Voice over Wifi (VoWLAN)

- You want encryption (you know you do)
  - 802.1x is good, as long as you don't move
    - Many clients 500ms to 10 seconds to roam and authenticate via 802.1x!
    - Delay budget provides only about 150ms
- Proprietary solutions for fast roaming exist
  - Cisco 'fast, secure roaming'
  - Typically no interop between vendors

Standards based? (VoWLAN)

- IEEE 802.11r - 18 or so months away
  - goal of sub 50ms handoff (no perceivable delay)
- In-between voice packets, evaluates and pre-authenticates to neighboring Access Point
  - will likely rely on 802.11e availability & QOS info
- Without 802.1x DOS is especially disruptive
  - imagine I turn on AP capabilities on my Mac
  - use the VoWLAN SSID
  - user roams to me, call dead

pdas, phones & handhelds

- encryption and connection options are often very limited
- newer mass market devices support WPA
- some may support 802.1x (Windows Mobile 2003/2005 support limited PEAP)
- older devices may only support WEP
- commercial products (notably Funk Odyssey works on many platforms and multiple EAP types)
- How does this affect your decisions?

outdoor and mesh

- Covering large areas with wifi poses some special challenges
- Location management is particularly difficult
  - triangulation (readings from 3-4 APs) used indoors
  - outdoor rarely has much overlapping coverage
- Capacity in high-density areas can be a problem
- As can rogue AP detection

wireless security strategies and challenges

Questions?

David Morton
dmorton@u.washington.edu