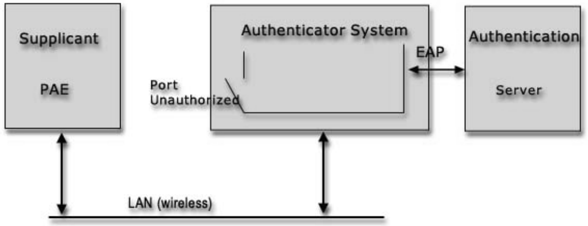
802.1X: Deployment Experiences and Obstacles to Widespread Adoption

Terry Simons
University of Utah; open1x.org
Terry.Simons@utah.edu

Jon Snyder
Portland State University
jon@pdx.edu

802.1X Adoption

- Ratified by IEEE in 2001
- Not exactly ubiquitous
- How many hotspots have you used that supported 802.1X? T-Mobile…
- What are the issues?
  - Client support
    - Often harder for users to configure
  - Vendor implementation
    - Particularly with accounting
  - Changing encryption standards



802.1X Deployment Experiences

- University of Utah
  - Urban campus, ~28k students
  - Very decentralized, scattered deployment
  - Initially deployed 802.11b with home-grown SSL captive portal
  - Cutover to 802.1X 5/19/2003
  - About 715 APs; cross-department authentication via RADIUS realms
  - Developers of Open1x (originally from UMD) and wEAP projects

University of Utah 802.1X Deployment

- Challenges
  - No control of client hardware/ software; laptops w/o CD-ROM
  - Decentralization makes it hard to standardize
  - Campus policy isn’t enforced
  - Multiple vendors: interoperability
  - Windows GINA/Zero Config
    - Funk, Meetinghouse disable some features, e.g. fast user switching

802.1X Deployment Experiences

- Portland State University
  - Urban campus with ~27k students
  - Initially deployed 802.11b in select campus locations using MAC address registration
  - Migrated to a captive portal as a stopgap until ready for 802.1X
  - Currently deploying 802.1X and expanding coverage area

PSU 802.1X Deployment

- Some challenges
  - No client control
    - Would really like a quick, easy installer for end users that sets up everything they need
  - Already deployed SSID with captive portal
    - Didn’t want to do a flash cutover
      - Using dual SSIDs deployed in parallel; new one requires 802.1X

PSU 802.1X Deployment

- EAP: Supporting TTLS and PEAP simultaneously
  - Prefer TTLS(PAP)
  - PEAP-MSCHAPv2 authentication gets proxied back to a Microsoft IAS RADIUS server as a regular RADIUS Access-Request
    - Thanks to the OSC folks for making Radiator able to do this—it’s great!
      - EAP_PEAP_MSCHAP_Convert

Lessons Learned: EAP

- Do your EAP homework
  - Pick an EAP type that provides keying material: ***Not*** EAP-MD5
  - Suggest either TTLS or PEAP for most organizations
    - TLS if you have and can support a PKI
      - Can be tough without client control

Lessons Learned: EAP

- PEAP-MSCHAPv2
  - EAP exchange within TLS tunnel
  - Supported by Microsoft clients (stores password in registry…)
  - Plain/MSCHAPv1 passwords on server
  - MiM attack can result in MSCHAPv2-hashed password
- EAP-TTLS
  - AVPs within tunnel (no 2nd EAP)
  - Susceptible to MiM with PAP inside

Deploying EAP-TTLS and/or PEAP

- Certificate verification
  - **Don’t** turn it off!
  - Use your own private CA; have it be the only one trusted by clients
  - OR, configure your 802.1X clients to verify a particular certificate name
    - If you can get away with a single exact name for the entire campus

Vendor EAP Issues

- Some vendors (e.g. Foundry) filter EAP types
  - Not exactly in the spirit of “Extensible” Authentication Protocol
- Not much authenticator involvement in the EAP exchange
  - Almost entirely between supplicant and authentication server
- So please, don’t filter EAP types!
  - Or at least make the filters configurable

Other Vendor Issues

- Dynamic WEP keying
  - Some vendors (e.g. Cisco, Trapeze, Airespace) use the Peer Key
    - Using the keying material as the key
  - This is Bad
    - Using the Peer Key as the unicast transmit key is less secure than sending the client a Peer-Key encrypted key

Lessons Learned: WPA

- Compatibility issues
  - Mac OS X does not associate to networks running in WPA Compatibility mode (multicast cipher is WEP)
    - Verified with Accton reference APs and Cisco 1200s
  - If you run in pure WPA mode, older cards not supporting WPA can’t associate

WPA Update

- 802.11i was ratified in June 2004
  - Uses AES (CCMP) rather than TKIP
  - The Wi-Fi alliance is testing for 11i-compatibility, under the name “WPA2”
- Linux WPA support evolving
  - No standard WPA calls; being added to Wireless Extensions 18
- Vendor support
  - Cisco plans support in Q4 2004.
- May want to wait for WPA2 if deploying

Lessons Learned: Client Caveats

- Certificate validation problems
  - System clock can be wildly wrong, especially on laptops (batteries)
  - Software prompts user for unknown certificate
    - Makes MiM easier
    - Client vendors: allow configuration such that unknown certificate is denied with error, rather than prompting user

802.1X Accounting Problems

- Acct-Session-Id
  - RFC 2866: “a unique Accounting ID to make it easy to match start and stop records in a log file. The start and stop records for a given session MUST have the same Acct-Session-Id.”
  - Can come out of order, so a **unique** Acct-Session-Id needs to be assigned to **every** session

802.1X Accounting Problems

- Acct-Session-Id is useless if ***every*** record for every session uses the same value
- If the client MAC address is used, you can't tell which Start and Stop records should be paired together
  - A random integer value that is unique to the session should suffice
    - The pair of NAS-IP-Address and Acct-Session-Id must always identify one accounting session

802.1X Accounting Problems

- Some Cisco devices format Acct-Session-Id this way:
  - ”10.1.2.3 username 06/10/04 14:22:03 00000007”
    - But they make sure that the Start and Stop records have matching Acct-Session-Id values, so it works
  - “00001878” is good too
- Proxim doesn’t do a good job here

802.1X Accounting Problems

- Call{ed,ing}-Station-Id
  - Called-Station-Id should be the MAC address of the NAS that is authenticating the user
  - Calling-Station-Id should be the MAC of the supplicant
- Some vendors really screw this up
  - Use IP addresses of NAS and RADIUS server, for example
- These attributes should be required
  - Hard to tell who had what IP without them

802.1X Accounting Problems

- Additional desirable accounting attributes
  - NAS-Port and NAS-Port-Type
    - Dictated by RFC2866
  - Authentication type
    - PEAP, EAP-TTLS, etc.
      - Some vendors do this in VSAs, but it should be standardized
  - SSID
    - Which SSID the user associated to

802.1X Accounting Problems

- Anonymous identities
  - With tunneled EAP types like PEAP and EAP-TTLS, outer EAP identity can be “anonymous”
    - Done so that a sniffer can’t see the true username
    - But makes accounting much more difficult

802.1X Accounting Problems

- Anonymous identity solutions
  - Access-Accept sent with inner user name: some devices will reply with this username in their accounting records (this is a hack)
  - Enforce inner=outer identities: RADIUS server could reject authentication if the outer and inner identities didn’t match
    - Radiator can do this via a hook

Summary: For 802.1X Deployers

- Use RADIUS accounting
- Consider creating a packaged installer for end users
- Have users verify server certificate
  - Make sure they install the root CA certificate, too
- Pick an EAP type and decide on WPA/WPA2 support
  - Rotate keys
- http://wireless.utah.edu/global/research/ap-reqs.html

Summary: For 802.1X Vendors

- DO NOT filter EAP types
- DO NOT use the Peer Key
- DO NOT force WPA to be enabled
- Support accounting!
- Use a unique Acct-Session-ID
  - One per session start/stop set
- Send proper Called-Station-ID and Calling-Station-ID
- Wish: have wired and wireless accounting formats be the same
- Client vendors: good debugging/logs!