Wireless Security and 802.1X

The pointy sharp cutting edge of 802.11

Agenda

- Trends in (wireless) LAN security
- 802.1X network architecture

Trends in LAN Security

Ow! The Cutting Edge of 802.11

- High density & high capacity networks
  - 802.11a is very helpful here
- Improving security while retaining usability to wired backbone
  - Admission control: Keep your infestations out of my network
- Differentiated access and policy implementation
  - Also differentiated service (e.g. voice)

Trends in LAN Security

- Movement of security to the edge
  - If port ≠ user, now what?
- Proliferation of access devices
  - Not just laptops any more
  - Need to protect network from devices
- Mobility
  - This is not just wireless—users have many networks
  - Cannot depend on always being connected to the infrastructure
- Differentiated access
  - Not only internal groups, but contractors

802.11 In Education

- Network is mostly open
  - Some network pockets need to be protected (e.g. registrar, finance networks)
- Network is balkanized
  - Cooperation between feudal lords (network administrators) may be impossible
- High degree of mobility
  - Session maintenance may be more important than in other environments
  - Corollary: political problems of networking may prevent it from happening
- Users may have a “real job”
  - Professional development students may need to VPN to work, for example

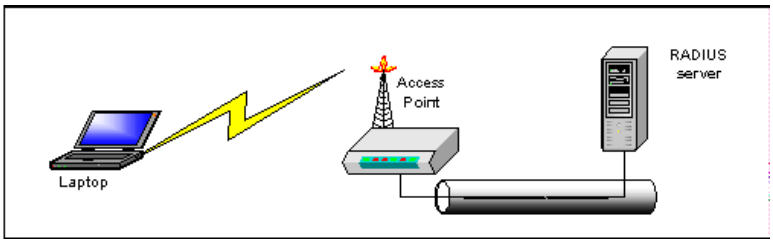
Why 802.1X?

- Establishing user identity can build a better network
  - Uses RADIUS, which is very flexible
  - Authorization: who you are controls what you can do
  - Applications: voice needs security integrated into handoff process, and low-latency encryption
- Does not require network redesign
  - Architecture does not have to be hierarchical
  - Can help build networks between warlords (network administrators)

802.1X Network Architecture

Physical Architecture

- Supplicant: End user device. Usually a computer, but may be printer, PDA, etc.
- Authenticator
  - Network device that blocks access until user authentication completes (more on this later)
  - May be AP for wireless networks, or switch on wired networks
- Authentication server: typically RADIUS



Authorization

- First, establish identity (authentication)
- Then, figure out what user is allowed to do (authorization)
  - The neglected second “A” in AAA
- With RADIUS, this is done with attributes
  - Assign users rights to resources and network access
  - Examples: VLAN number (see RFC 3580), session timeout, Access control lists/personal firewall
  - Many servers can rewrite attributes via proxy
- Any existing access control between networks is automatically applied to users

Back-end Databases & RADIUS

- No new wireless user accounts!
- Common back-ends
  - Active Directory/NT domain
  - LDAP
  - Kerberos
- May also be specialized for certain purposes
  - TACACS for routers, token cards for key resources
- Choosing the authentication protocol may depend on how password is stored
  - Yes, I am skipping over this

Large-Scale RADIUS

- Problems of large/distributed environments
  - Lots of APs
  - Different administrative zones (political boundaries get in the way)
- “Roaming” is possible by passing requests between two networks
  - Similar concept to mobile phone roaming (like the way that my T-Mobile USA phone is working right now)

RADIUS Star Architecture

- Multiple networks under separate administrative control
- Each network has a server
  - Some requests are handled locally
  - Unknown users are passed to other servers
  - Core server is an "identity router" for authentication requests
- We have a mini-version of this in the iLabs

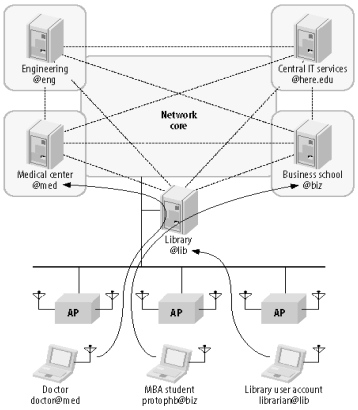


Figure used with permission from *802.11:TDG*, 2nd Ed

RADIUS Proxy Between Organizations

- Good for guest authentication
  - Ask visitor's employer to establish identity
  - Requires trust between organizations
- This is sometimes called "federated" authentication
  - Separately built & run networks
  - Users can use any member network
  - Generally no seamless roaming between two member networks

Federated Authentication

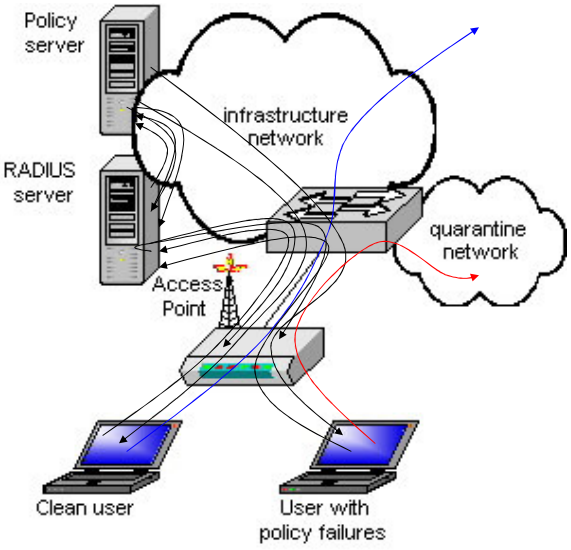
- Eduroam (http://www.eduroam.org/)
  - European-wide RADIUS star
  - Also hooked into Australia R&E network
  - United States core built at University of Utah
- Internet2 project for U.S. network
  - http://security.internet2.edu/fwna/
- General description of the technical issues:
  - http://www.oreillynet.com/pub/a/wireless/2005/01/01/authentication.html

Extended Authorization

- The Paris Hilton principle: users do not always deserve what they inherit
  - Basic authorization (e.g. VLAN) is static
- Limits on authorization may be useful
  - Area: guests are only allowed in the lobby
  - State of machine (integrity)
  - Software version or running applications
- Two part authorization
  - #1: You must be an authorized user
  - #2: You must **ALSO** meet our admission policy

Example: Policy Enforcement

- Users who pass policy check are placed on production network
- Users who fail are quarantined



Questions?