Agenda

- What is 802.1X?
- Why use 802.1X?
- Why not use 802.1X?
- Authentication
- Infrastructure
- Deployment
- Management
- Questions?
What is 802.1X

- IEEE Standard for Port-Based Network Access Control
- Provides authentication framework for LAN access
- Uses the Extensible Authentication Protocol (EAP)
- One of the components of 802.11i
802.1X

- Authenticator (Access Point)
- Supplicant (Laptop)
- Authentication Server (RADIUS Server)
- Internet
Why use 802.1X?

- **Strong Authentication**
  - User-based or machine-based
- **Enable scalable over-the-air encryption**
- **Assign network profile by AuthN**
  - Vlan, ACL, QoS
- **Contain SSID spoofing (wireless)**
Why not use 802.1X

- Common alternatives: Web, VPN, MAC
- Long dependency chain
  - Client: supplicant, EAP, encryption (hardware)
  - Network: AP/switch support
  - Middleware: RADIUS, authentication server
Choosing an EAP type

- X.509 Certificates
  - EAP-TLS
- Plaintext password (LDAP, Kerberos, OTP)
  - EAP-TTLS:PAP
- Windows hashed password
  - PEAP:MSCHAPv2
  - EAP-TTLS:MSCHAPv2

UserID format

- userid vs userid@realm
Authentication

- Guest login – 802.1X or other?
- AuthZ
  - Allow/deny
  - Access profile (ACL, vlan, ...)
- Credentials
  - Common
  - Dedicated
  - Merge of several sources
Infrastructure

- RADIUS Server
  - Open Solution’s Radiator
  - Funk Steelbelted RADIUS
  - Cisco ACS
  - Microsoft IAS
  - FreeRADIUS
- Multiple/Redundant RADIUS Servers
- RADIUS Transaction Rate
- Certificate for RADIUS Server
  - Purchase?
  - Self-signed?
- Logging, query tools
Infrastructure

- AP / Switch support for 802.1X
- Wired 802.1X migration support
  - MAC Based
  - Default VLAN
Deployment

- SSID name
- Broadcast SSID
- Multiple SSIDs
  - Open (current, guest, provisioning)
  - 802.1X
  - Client behavior
- Encryption: DynWEP, WPA, WPA2
  - Overloading SSID
- What about devices that don’t support 802.1X?
- Client configuration
- Which supplicant?
## Suppliants and Supported EAP Types

<table>
<thead>
<tr>
<th></th>
<th>EAP-TLS</th>
<th>EAP-FAST</th>
<th>LEAP</th>
<th>MD5</th>
<th>PEAP</th>
<th>EAP-TLS</th>
<th>PEAP-MSCHAPv2</th>
<th>EAP-TTLS</th>
<th>EAP-TTLS-MSCHAPv2</th>
<th>EAP-TTLS-MSCHAP</th>
<th>EAP-TTLS-MSCHAP CHAP</th>
</tr>
</thead>
<tbody>
<tr>
<td>WinXP/2000/Vista Native</td>
<td>X</td>
<td></td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MacOS 10.4 Native</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>wpa_supplicant</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Odyssey</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Aegis</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SecureW2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Note: X indicates support.
Management

- How quickly can you make changes on the wireless or wired network infrastructure?
- How do you encourage use of 802.1X in “dual mode” configurations?
- Can you disconnect authenticated users in your network hardware/software?
- Can you effectively troubleshoot a user connection problem?
IT Participation

- IT Management / Oversight
- Security Officer
- Security Ops
- Wireless Network Ops
- RADIUS Server Ops
- Authentication, Authorization Service Ops
- Customer Support
- Customer Communications
Checklist

- Network equipment (AP/switch) supports 802.1X (Wireless: WPA)
- EAP type decision
- RADIUS setup to AuthN, AuthZ
- Client-side experience known, documented, tested
- Tools to query logs for troubleshooting & security ops
- Process (tool?) to implement large scale network changes
- Communications plan to keep users apprised of changes
Questions?