Erfahrungsbericht Wireless 802.1x am USZ

Agenda

- Übersicht über das Spital
- Ausgangslage
- Anforderungen bezüglich Wireless
- Problemstellung und Lösungsvarianten
- Testerfahrungen
- Aussichten weitere Nutzung von Zertifikaten

Kennzahlen des USZ

- **Kennzahlen des USZ**
  - 6100 Mitarbeitende
  - 42 Kliniken und Institute
  - 52 Bettenstationen
  - 160'000 Patientinnen und Patienten ambulant
  - 30'000 Personen stationär

Ausgangslage

- **Am USZ werden seit 2001 erste Wirelessinstallationen betrieben**
- **In den darauffolgenden Jahren vereinzelte Installationen mit Cisco APs und LEAP.**
- **Wunsch nach einer herstellerunabhängigen und sichereren Lösung**
- **Vorschlag des Einsatzes von EAP-TLS mit 802.1x**
- **EAP-TLS wird von allen Windowsclients ab Win2k unterstützt**
- **Am USZ werden mehrheitlich Win2k Clients eingesetzt**

Ausgangslage

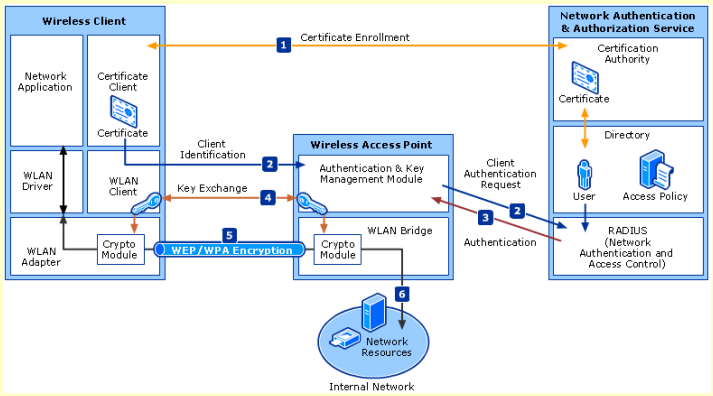
- Von Seiten Microsoft wurde zum Teil die Aussage vertreten, dass EAP-TLS nur mit WinXP und Vista sinnvoll funktioniert.
- Damit EAP-TLS verwendet werden kann, braucht es Zertifikate.
- Sinnvollerweise werden diese über das ADS verteilt.
- Dies wiederum impliziert sinnvollerweise eine PKI die im ADS eingebunden ist.
- Von Seiten USZ wurde ein Anbieter gesucht, der uns im Bereich Zertifikatsverteilung und Integration in Wireless mit Win2k Unterstützung bieten konnte.
- Keyon erklärte sich bereit uns diesbezüglich zu unterstützen.

Anforderungen bezüglich Wireless

- Einbindung der Win2k Clients mit 3. Herstellertreiber (Intel Centrino, Cisco, etc.)
- Verwendung der 3. Herstellertreiber sowie Betriebsystemtreiber von WinXP.
- Möglichst problemloses Roaming zwischen den APs.

Problemstellung und Lösungsvarianten

- Aufbau der 802.1x Infrastruktur



Problemstellung und Lösungsvarianten

- Testaufbau im Labor
- Ertüchtigung des AD für die Nutzung zusätzlicher Felder für Zertifikate
- Einbindung des Zertifikatservers in das AD
- Einbindung des IAS als Radiusserver für die Radiusclients (APs, Wirelessswitch)

UniversitätsSpital Zürich
Erfahrungsbericht Wireless 802.1x am USZ
A. Senn 8.5.2007

Problemstellung und Lösungsvarianten

- **Verwendung der Zertifikate**
  - Ursprünglicher Ansatz alleinige Verwendung von Gerätezertifikaten
  - Konnte nicht realisiert werden, da ein Standarduser keine Berechtigung auf den Zertifikatsspeicher hat
  - Somit Verwendung von Geräte- und Benutzerzertifikaten

Problemstellung und Lösungsvarianten

- **Zertifikat – Autoenrollment von Microsoft**

Zertifikat / Windows	User	Computer
XP	✓	✓
Vista	✓	✓
2000	✗	✓

UniversitätsSpital Zürich
Erfahrungsbericht Wireless 802.1x am USZ
A. Senn 8.5.2007

Problemstellung und Lösungsvarianten

- **Manuelle Zertifikats-Vergabe für Windows 2000**
  - Zertifikatsanfrage auf Client durch Benutzer manuell durchführen mittels Zertifikatsspeicher von Windows
  - Installation des Zertifikats durch den Benutzer
  - Nachteil:

    Für die manuelle Zertifikats-Vergabe muss sich der Benutzer per LAN in seinen Benutzer-Account einloggen.

Problemstellung und Lösungsvarianten

- **Zusammenfassung**
  - Windows 2000 unterstützt 802.1x EAP-TLS
  - USZ Komponenten 802.1x EAP-TLS fähig
  - Benutzer Zertifikat notwendig
  - Benutzer Zertifikats-Vergabe für Windows 2000 möglich
  - Keine Anpassungen an USZ Infrastruktur

UniversitätsSpital Zürich
Erfahrungsbericht Wireless 802.1x am USZ
A. Senn 8.5.2007

Testerfahrungen

- **Testerfahrung mit den Win2k Clients (primär Wlan)**
- **Testerfahrung mit den WinXP Clients (primär Wlan)**
- **Aufbau der produktiven Umgebung.**

Weitere Aussichten

- **Aussichten weiterer Nutzung von Zertifikaten**
  - Authentisierung am Lan über 802.1x
  - Aufbau einer PKI -> Identity Management Projekt

Besten Dank für die Aufmerksamkeit