HostAP WPA Workshop

27. Dezember 2004

Jan Fiegert, <jan.fiegert@gmx.de>

Einleitung / Motivation

- 802.11 ist eine Gruppe von Standards zu Funkvernetzung.
- 802.11b beinhaltet ein RC4 basiertes Verfahren zur Verschlüsselung des Datenverkehrs.
- Diese hat sich mittlerweile als völlig unbrauchbar heraus gestellt.
- Abhilfe ist nötig und möglich.

Mögliche Alternativen:

- ☐ Verschlüsselung auf Applikationsebene.
- ☐ Tunneling duch ein anderes Protokoll.
- ☐ Einrichtung eines VPN.
- ☐ Wi-Fi Protected Access (WPA).
- ☐ Warten auf 802.11i.

Welche Probleme hat WEP?

- Fehlerhaft implementierter RC4 Algorithmus.
- Fehlen einer brauchbaren Authentifizierung.
- Neuartige kryptographische Attacken, die diese Schwächen nutzen.
- Tools die diese implementieren.

WPA Kurzübersicht

- WPA umschifft die Schwächen der RC4 Implementierung in WEP.
- Bestehende Hard- und Firmware kann weiterverwendet werden.
- Überbrückt die Zeit bis 802.11i.

WPA -Kurzübersicht

- Wi-Fi Protected Access (WPA)
- WPA kombiniert Authentifizierungs-verfahren und mit einer verbeserten Verschlüsselung.
- Bei der Authentifizierung kommt 802.1x zum Einsatz.
- Die Verschlüsselung wird durch RC4 und TKIP realisiert.

802.1x Teilnehmer

- Authenticator:
  - regelt den zugang zum Netz
  - solange ein Client nicht authentifiziert ist, werden nur Pakete zur Authentifizierung zugelassen.
  - im Erfolgsfall wird danach jeglicher Verkehr zugelsassen

802.1x Teilnehmer

- Supplicant:
  - Client seitige Komponente
  - Implementiert Schlüsselaustausch und Authentifizierung
  - Existiert für alle gängigen Betriebsysteme.

802.1x Teilnehmer

- Authentication Server:
  - bekommt vom Authenticator Anfragen weitergeleitet
  - erlaubt oder verweigert Zugang zum Netzwerk

Praktischer Teil!

Was wird benötigt?

- Linux Kernel 2.6.x
- HostAP Pakete (http://hostap.epitest.fi)
- freeRADIUS Server
- openssl und CA Software
- Prism2/2.5/3 basierte 802.11b Karte

Voraussetzungen schaffen

- Kernel Quellen anpassen und übersetzen. Kernel und Module installieren und in Betrieb nehmen.
- User Space software übersetzen und installieren
- zusätzlich benötigte Software installieren.

Kernel anpassen

- HostAP patches einspielen
- HostAP Treiber in die Quellen kopieren
- Kernel der verbauten Hardware entsprechend konfigurieren
- kleinere manuell Anpassungen vornehmen (fakultativ!)

User Space Programme

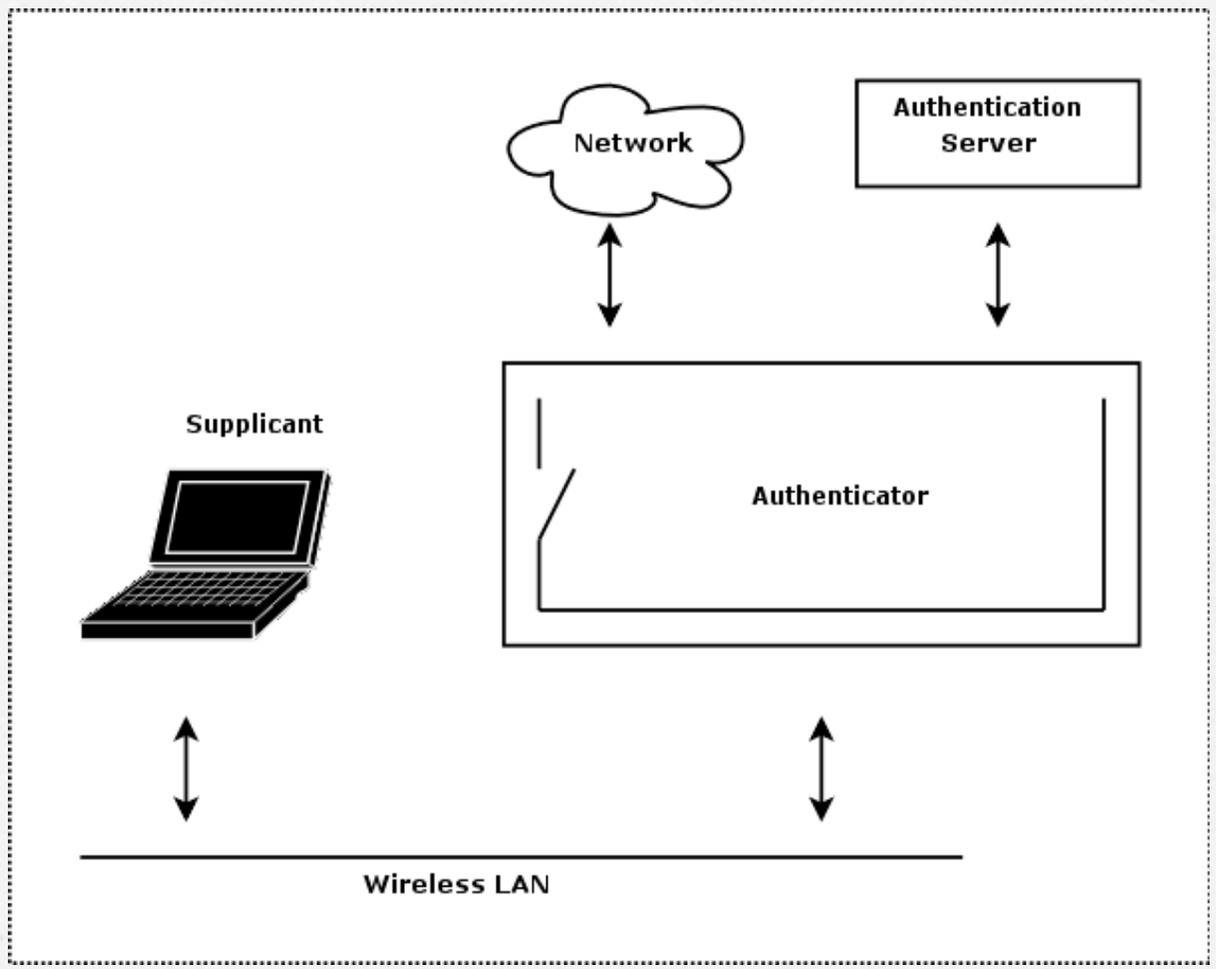
- [ ] hostapd übersetzen
- [ ] hostap-utils übersetzen
- [ ] Beide an geeignete Stelle im Pfad kopieren.

Aufgabenzuordnung 802.1x

- Der Authentication Server wird durch einen Radius Server implementiert

- hostapd dient als Authenticator

- Der Supplicant wird vom Client B.S. gestellt



PKI & Certificate Authority

- Der Access Point soll als EAP Verfahren EAP - TLS beherrschen
- Eine PKI ist dafür erforderlich
- Grundlage der PKI ist eine Certificate Authority (CA)
- Wenn möglich vorhandene PKI nutzen.

PKI in 5 Schritten

- Self Signed CA Certificate erstellen
- Zertifikat und Schlüssel für den Authentication Server erstellen
- Client Zertifikate für die Supplicanten erstellen
- beide von der CA unterschreiben lassen
- Zertifikate und benötigte Schlüssel exportieren

freeRADIUS Konfiguration

- [ ] EAP TLS Sektion suchen
- [ ] Server- und CA- Zertifikat sowie den privaten Server Schlüssel verwenden
- [ ] DH Konfiguration erstellen
- [ ] random file erstellen

freeRADIUS Konfiguration

- EAP TLS in Authorize- und Authenticate Sektion aktivieren
- hostapd agiert als Radius Client, er muss in der Benutzerverwaltung aktiviert werden.

hostapd Konfiguration

- allgemeine Einstellungen wie SSID, Logging und Debugging vornehmen
- Radius spezifische Konfiguration
- WPA Einstellungen (Verschlüsselung, Authentifizierung, Re- Keying usw.)

Netzanbindung

- Betrieb als Ethernet Bridge oder mit eigener IP Konfiguration
- Integration in die Infrastruktur der verwendeten Distribution
- weitere Sicherheitsmassnahmen

Ausblick

- Unterstützung weiterer Chipsätze
- Integration in den Standard Kernel
- Implementierung eines eigenen Authentication Servers
- Unterstützung weiterer EAP Verfahren.