A2x
Trefzer Consulting

Sicherheit in drahtlosen Netzwerken

Erstellt durch: Benedikt Trefzer

Webseite: http://www.a2x.ch

Datum: 2.3.2006

Inhalt

A2x
Trefzer Consulting

- WLAN Bedrohungen
- Schutzmöglichkeiten und Wertung
  - MAC/IP Authentifizierung
  - Verstecken der SSID
  - WEP
  - WPA und WPA2
  - VPN
- Beispiel Volksschule (A2x Gateway GW100)

Spezifika WLAN

A2x
Trefzer Consulting

- Ein drahtloses Netz kann nicht physisch abgeschirmt werden (nicht wie bei Kabel).
- Im Umkreis eines Senders ist jeglicher Verkehr sichtbar.
- ein drahtloses Netzwerk lässt sich nicht verstecken.

Netznutzung durch Dritte

A2x Trefzer Consulting

- Kostenfolge durch Bandbreitennutzung
- Dritte Nutzen Anonymität aus
  - für Copyrightverletzungen (Bsp. Mp3 Download)
  - für Hackerangriffe
  - Up-/Download verbotener Inhalte (Bsp. Pornografie)
  - Freisetzen von Viren
  - Versenden von Spam
  - etc.

Abhören und Manipulieren

A2x
Trefzer Consulting

- Ausspähen von
  - Passwörter (Mail etc.)
  - Dokumenten
- Manipulation von Verbindungen
  - Einschleusen von Viren oder anderem Schadcode
  - Man in the middle Attack

Denial of Service

A2x
Trefzer Consulting

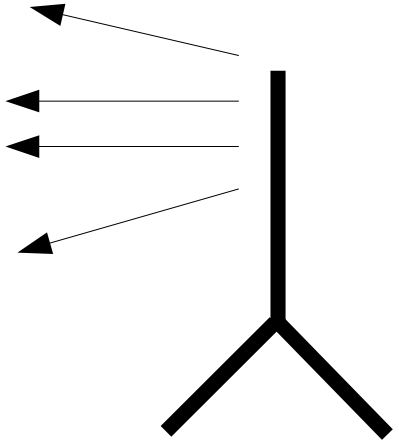
- Denial of Service durch
  - erzeugen von grossem Verkehrsvolumen mit falschem Schlüssel -> AP antwortet
  - übernehmen von IP/MAC eines Benutzers
  - Frequenzstörungen
  - etc.
- Eine DoS Attacke ist zumeist einfach lästig und verursacht dadurch Kosten.

Rechtliches (DE)

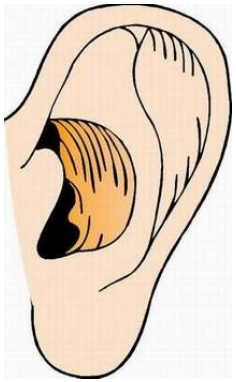
- Access Points unterliegt dem Teledienstgesetz
- Im Internet ist nur die IP-Adresse des Besitzers sichtbar
- Rechtswiedriges Verhalten der Nutzer fällt als erstes auf den Besitzer
- Zu beweisen, dass ein Dritter einen Verstoss begangen hat ist schwierig

Bedrohungen

Wireless Netz



Nutzung durch Dritte



Abhören

Denial of Service

Authentifizierung MAC/IP

A2x
Trefzer Consulting

- Durch Zugriffskontrollisten werden nur bestimmte Hardwareadressen (MAC) oder IP Adressen zugelassen.
- Eigentlich mehr eine Firewall Funktionalität des Access Points
- Problem:
  - ifconfig ethX hw ether ab:cd:ef:gh:ij:kl
  - IP Adresse lässt sich mindestens so leicht anpassen !

Verstecken der SSID

A2x
Trefzer Consulting

- SSID := Name des drahtlosen Netzwerkes
- Ohne den Namen eines Netzwerkes zu kennen, ist eine Verbindungsaufnahme nicht möglich.
- ABER: Verhindert das Entdecken eines WLAN's nicht wenn Daten ausgetauscht werden
- Aufstöbern versteckter WLAN's ist möglich
- Nachteil: Benutzerfreundlichkeit leidet, da mehr konfiguriert werden muss

Wired Equivalent Privacy (WEP)

A2x
Trefzer Consulting

- Standard-Verschlüsselung für WLAN (eingeführt 1999 mit den ersten WLAN)
- Bietet eine einfache Datenverschlüsselung (XOR-Verknüpfung mit pseudozufälligem Bitstrom).
- Benutzerzugriff durch WEP Schlüssel.

Wired Equivalent Privacy (WEP)

A2x Trefzer Consulting

- Probleme:
  - Alle Benutzer müssen denselben Schlüssel verwenden
  - Wenn der WEP Schlüssel bekannt ist, ist aller Verkehr unverschlüsselt
  - Durch Abhören des verschlüsselten Verkehrs lässt sich der WEP Schlüssel errechnen
  - Wenn kein Verkehr, lässt sich Verkehr durch den Angreifer erzeugen
  - => Ein WEP Schlüssel lässt sich innerhalb kurzer Zeit (2-3h) knacken

WPA

- Vorwegnahme von Teilen von WPA2 nachdem festgestellt wurde das WEP unsicher ist.
- Je Verbindung wird ein Schlüssel ausgehandelt
- Benutzerbasierte Authentifizierung möglich (Mit Radius Server)
- Übergangslösung

WPA2 (802.11i)

A2x
Trefzer Consulting

- Neuer Standard seit Juni 2004
- neues Verschlüsslungsverfahren (AES)
- Benutzerbasierte Authentifizierung möglich (mit Authentifizierungsserver, teilweise im AP enthalten)
- Eingehende kryptologische Prüfungen während der Entwicklung

WPA2 (802.11i)

- Aber
  - ältere Hardware ist ausgeschlossen
  - Benötigt spezielle Software auf dem Client
    (Verfügbar für Linux, Mac OS X >10.3, Windows 2003, XP und 2000 (mit patch))
  - ältere Betriebssysteme sind ausgeschlossen

VPN

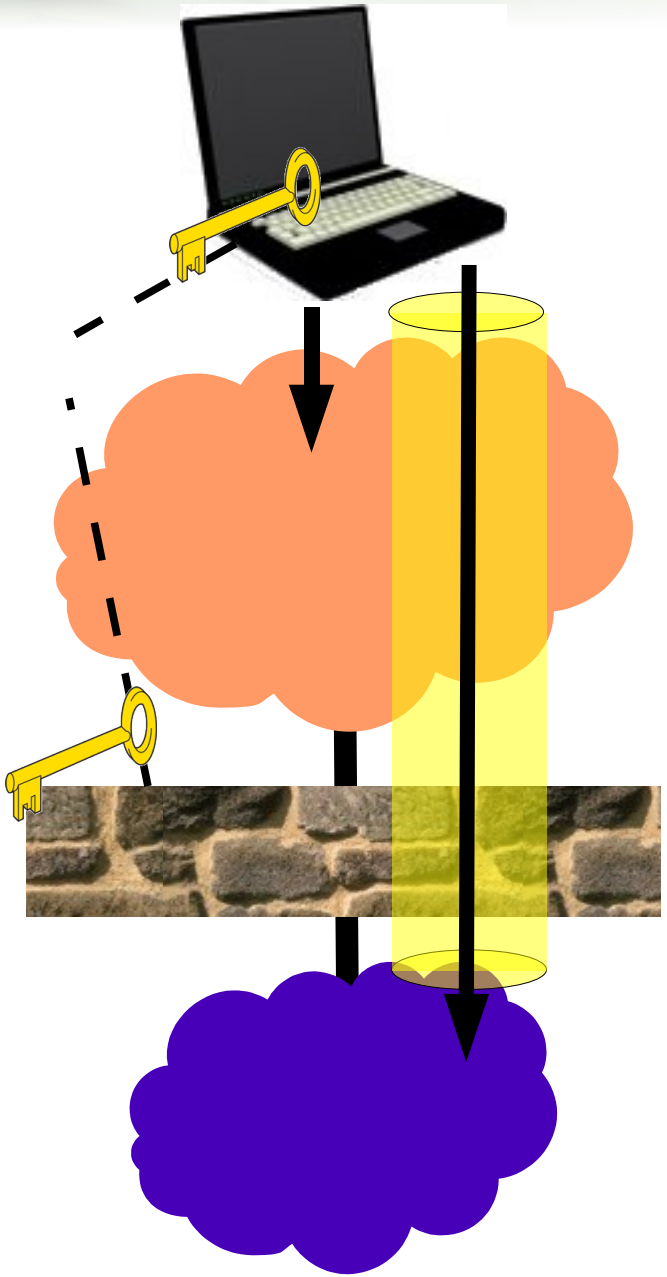
A2x
Trefzer Consulting

- Definition: Virtuelles Netz, bestehend aus Rechner aus verschiedenen Teilnetzen. Die Übertragung innerhalb des VPN erfolgt meist verschlüsselt.
- Beispiele für VPN: Ipsec, OpenVPN, Cisco etc.

VPN Funktionsweise

A2x Trefzer Consulting

1. Netzverbindung aufbauen
2. Authentisierung am VPN Gateway
3. Aufbau eines Tunnels
4. Verbindung ins sichere Netz via Tunnel



VPN

A2x
Trefzer Consulting

- Durch die Verwendung einer VPN Verbindung über Wireless erreichen wir:
  - Authenthifizierung
  - Verschlüsselte Verbindung dadurch
    - kein Abhören
    - keine Manipulation bestehender Verbindungen

VPN

- Bedingt Installation einer Client Software (Dadurch Betriebsystemabhängkeit)
- Benötigt VPN Server
- Unabhängig von Netzhardware (egal ob Ethernet, Tokenring oder Wireless)
- Hohe Sicherheit durch ausgereifte Lösungen

Zusammenfassung

Nutzung durch Dritte

Abhören

Denial of Service

	Nutzung durch Dritte	Abhören	Denial of Service
Authentifizierung MAC	rot	rot	rot
Verstecken SSID	rot	rot	rot
WEP	gelb	gelb	rot
WPA	grün	grün	rot
WPA2	grün	grün	rot
VPN	grün	grün	rot

Beispiel Volksschule

A2x Trefzer Consulting

- Ausgangslage:
  - mehrere Access Points vorhanden (WEP Schlüssel ist „schule“)
  - Schulclients mit Internetzugriff (ADSL)
  - Netzdrucker
  - Externe Referenten benötigen Internet Zugang
  - Wenig Informatik KnowHow
  - Bisher ist das WLAN völlig offen !

Volksschule Bedrohungen

A2x
Trefzer Consulting

- Das Netz wurde mehrfach Anonym genutzt.
  Der hohe Traffic legt nahe, dass ein Filesharer am Werk ist.
- LehrerInnen versenden Zeugnisnoten, Klausuren etc. mittels Email.
- Bereits hat jemand 10000 Seiten Papier mit „*Ich bin der Beste*“ bedruckt.

Lösungmöglichkeiten

A2x Trefzer Consulting

- Verzicht auf Wireless ist nicht möglich
- Umrüsten auf WPA oder WPA2
  - nur durch Hardwareänderung (Kosten !)
- VPN über das Wireless LAN (OpenVPN) und Webauthenthifikation für Referenten
  - realisiert auf einer Appliance

Gateway GW100

A2x
Trefzer Consulting

- Einfache Appliance mit ausreichender Sicherheit
- VPN (OpenVPN) Zugriff für Wireless Clients
- Webbasierte Authenthifikation für Gastnutzer
- Schutz aus dem Internet durch NAT based Firewall

Netztopologie neu

Trefzer Consulting

Wireless

Zugriff nur nach Authentifikation oder VPN

Internet

Intranet

Direkter Zugriff auf Internet

Für Drucker Server etc.

Demo GW100

A2x
Trefzer Consulting

GW100 Anschlüsse

- LAN0 (Internet): Keine offenen Ports, Rechner in den anderen Netzen können nicht erreicht werden (NAT)
- LAN1 (Clients WLAN) Zugriff auf Internet und Intranet nur nach Authenthifizierung (Webbased oder VPN).
- LAN2 (Intranet) Server, Durcker etc. Zugriff auf Internet frei.

Referenzen

- „Entwicklung einer einfachen Authentifizierungslösung für WLAN-Netze in kleinen Schulumgebungen“ Semesterarbeit von Markus Heule [http://campus.ph-solothurn.ch/SIS/FunknetzAuthentisierungsLoesungFuerSchulen]
- „Kabellose Vernetzung von Computern an Schulen“ von Yvan Grepper, Beat Döbeli [http://www.swisseduc.ch/informatik/berichte/wireless/]
- Wikipedia [http://de.wikipedia.org] (Stichworte: WPA, WPA2, WEP)
- C't 2004/21 Seite 214: Jenseits von WEP
- OpenVPN [http://openvpn.net]