D·A·CH Security 2006

Gemeinsame Arbeitskonferenz

GI · OCG · BITKOM · SI · TeleTrusT

Düsseldorf, 28. bis 29. März

WLAN Sicherheit – von WEP bis CCMP

Fachhochschule Dortmund
University of Applied Sciences

Prof. Dr.-Ing. Evren Eren
Fachhochschule Dortmund
Web: www.inf.fh-dortmund.de/eren
E-Mail: eren@fh-dortmund.de

DECOIT

Dr.-Ing. Kai-Oliver Detken
DECOIT GmbH
Web: www.decoit.de
E-Mail: detken@decoit.de

WLAN-Standards

Standard	Beschreibung
802.11a	54 MBit/s WLAN im 5-GHz-Band
802.11b	11 MBit/s WLAN im 2,4-GHz-Band
802.11c	Wireless Bridging
802.11d	World Mode, Anpassung an regionsspezifische Regulatoren
802.11e	Quality-of-Service (QoS) und Streaming-Erweiterung für 802.11a/g/h
802.11f	Roaming für 802.11a/g/h mit dem Inter Access Point Protocol (IAPP)
802.11g	54 MBit/s WLAN im 2,4-GHz-Band
802.11h	54 MBit/s WLAN im 5-GHz-Band mit Dynamic Frequency Selection (DFS) und Transmit Power Control (TPC)
802.11i	Authentifizierung/Verschlüsselung für 802.11a/b/g/h (AES und 802.1X)

WLAN Sicherheit – von WEP bis CCMP

Status-Quo bei WLAN

- WLANs werden im privaten Bereich und in Unternehmen jedweder Couleur eingesetzt. Im Heimbereich sind ca. 70 % der WLAN-Netze ungesichert.
- Sicherheitsmechanismen wie WEP und teilweise WPA nicht ausreichend.
- Wardriving und Warchalking sind zu einem Sport geworden.
- **Gefahren:**
  - Mitschneiden von Datenverkehr im Netzwerk
  - Einschleusen von Daten wie auch schadhaftem Code in das Netzwerk
  - Manipulation von Daten
  - Stören der Kommunikation und damit Verfügbarkeit des Netzes
  - Unterbrechen und Übernahme von bestehenden Verbindungen
  - Ausspähen von Benutzerdaten
  - Identifikation von Clients und damit Benutzern
  - Fälschen von WLAN-Acess Points und Simulation von Hotspots
  - Kompromittierung von WEP-Schlüsseln
- Für Angriffe kein besonderes Know-how notwendig! Es gibt freie Tools im Netz.

Schwachstellen bei WEP

- **Kein Schlüsselmanagement**
  - Schlüssel ...
    - ist statisch
    - existiert nur einfach
    - muss „von Hand“ verteilt und eingetragen werden
    - wird sehr selten oder überhaupt nicht gewechselt
  - Offenbarung eines Schlüssels, z.B. durch Verlust eines Clients oder mittels frei verfügbarer Angriffs-Tools, kompromittiert das gesamte WLAN.
- **Keine Benutzeridentifikation und -Authentisierung**
- **Keine zentrale Authentisierung und Autorisierung**

Alternative Sicherheitsmechanismen und Verfahren

- **Wi-Fi Protected Access (WPA):**
  - Zugangssteuerung über 802.1X + EAP-Methode
  - Vertraulichkeit und Datenintegrität durch TKIP (RC4-Verschlüsselung). TKIP bietet Grundsicherheit auf der Bitübertragungsschicht. Kombiniert mit 802.1X ist es relativ sicher.
    - **Problem:** MIC nutzt einen schwachen Hash-Algorithmus. Ein Angreifer kann irgendwann zufällig ein Paket mit der richtigen Prüfsumme senden, das vom Access Point akzeptiert und durchgelassen wird.
  - *WPA Personal (WPA-PSK):* Einfachste Variante; für den Heimbetrieb ausgelegt. Für Anwender ohne 802.1X-Infrastruktur. Es kommt ein Preshared Key zum Einsatz.
    - **Problem:** Risiko von Wörterbuchattacken. I.d.R. ein Preshared Key für alle Stationen einer SSID. Angreifer kann Schlüssel ableiten. Qualität der Passphrase bestimmt die Sicherheit des Preshared Keys. Administrativer Aufwand in größeren WLANs nicht beherrschbar.
  - *WPA Enterprise (WPA RADIUS):* Dynamische Schlüssel für jedes versendete Paket. Für jeden Benutzer ein Schlüssel. Authentisierung über EAP-Verfahren, oft RADIUS.

Alternative Sicherheitsmechanismen und Verfahren

- **802.11i / WPA2:**
  - Verschlüsselung und Integritätsprüfung durch CCMP (AES als Verschlüsselungsverfahren).
  - Im Vergleich zu WPA deutlich sicherer. CCMP ist wesentlich leistungsfähiger als TKIP, da ein und derselbe Schlüssel zur Frame-Verschlüsselung und Integritätsprüfung benutzt wird.
  - WPA2 hat diverse Untersuchungen und Prüfungen von Kryptoanalytikern bestanden und entspricht dem Stand der Technik.
  - 802.11i bietet geschützten Ad-hoc-Modus, Secure Fast Handoff und Pre-Authentication, sicheres De-Authentication and Disassociation.

Handlungsempfehlungen

- Folgende Punkte sollten beachtet werden (u.a. von „802.11i Security Task Group“ sowie dem „WiFi WPA“-Standard empfohlen):
  - **Gegenseitige Authentisierung**
  - **Dynamische Sitzungsschlüssel und Schlüsselmaterial:** EAP-Methode sollte Schlüsselmaterial zur Verfügung stellen.
  - **Nachrichtenintegrität:** Message Integrity Check (MIC) bei TKIP (WPA) sowie CCMP (WPA2).
  - **Zentrale Authentisierung und Autorisierung:** Zentralisierter AAA-Mechanismus muss Benutzer einzeln identifizieren und authentisieren. (Policy-basierter Netzwerkzugang abbildbar)
  - **Schnelles Re-Keying:** Re-Keying fordert Clients auf, Schlüssel zu aktualisieren (z.B. periodisch).
  - **Session-basierte Verschlüsselung:** Kombination von 802.1X, EAP-TLS und RADIUS erlaubt pro Verbindung und Sitzung verschlüsselten Datenverkehr mit dynamischen Schlüsseln.

Handlungsempfehlungen

- **Welches EAP-Verfahren?**
  - EAP-Variante genau auf individuelle Bedarfe abstimmen! (Trade-off zwischen Simplizität in der Anwendung und Sicherheit). Richtige Wahl ist eine infrastrukturelle Frage, insbesondere der Client-Unterstützung.
  - *Wenn PKI vorhanden:* EAP-TLS geeignet, jedoch hoher infrastruktureller Aufwand. Sicheres Verfahren, wenn das Authenticator-Zertifikat sicher zum Supplicant übertragen wird oder durch eine CA überprüft wird.
  - *Wenn keine PKI:* EAP-TTLS/PEAP, besonders bei einem heterogenen Netzwerk. Brauchen nur Server-Zertifikat; sind abhängig von nachgelagerter Authentisierung.
    - EAP-TTLS wesentlich flexibler, da auch Authentisierungsmethoden ermöglicht werden, die EAP-Methoden nicht erreichen. Einfacher zu implementieren als EAP-TLS. Sicherheit wie bei EAP-TLS, jedoch nicht für hohe Sicherheitsanforderungen.
    - PEAP für die meisten Anwendungen sicher. Mittlerer Planungs- und Implementierungsaufwand (jedoch gering, wenn mit EAP-MS-CHAPv2 kombiniert). Unterstützt nur EAP-Methoden.

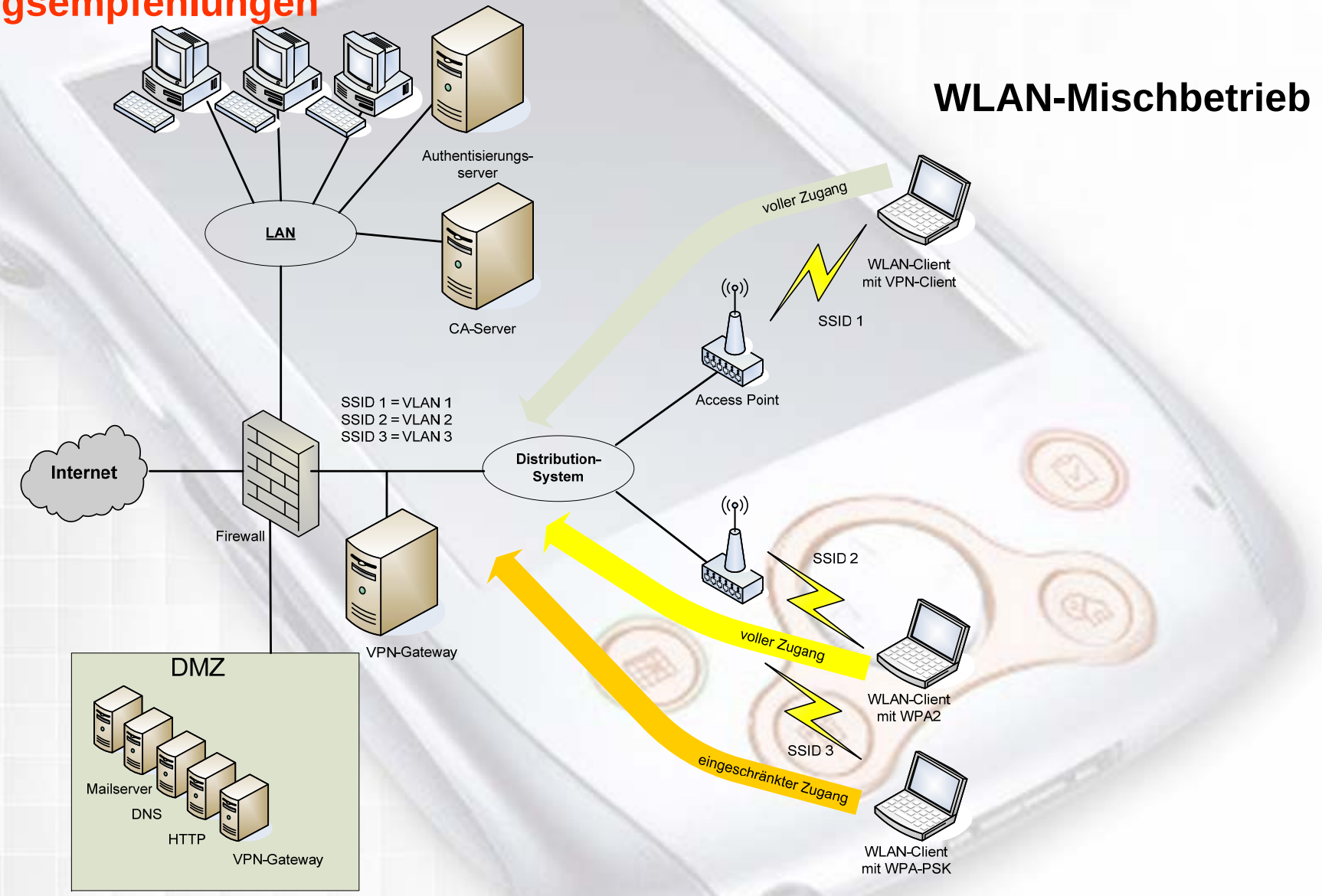
Handlungsempfehlungen

- **Welches EAP-Verfahren?**
  - *Alternative zur "gegenseitigen Authentisierung":* EAP-Methoden, die mit zwei Tunneln (äußerer und innerer Tunnel) arbeiten und im inneren Tunnel schwächere Authentisierungsverfahren schützen, z.B. EAP-PEAP.
  - **Geeignete Grundlage: 802.1X + EAP:**
    - Einheitliche Authentisierungsmethodik mittels EAP.
    - Flexibel in der Zugangstechnik, da AAA-Infrastruktur nicht nur für WLAN, sondern auch für LAN und VPN einsetzbar.
    - Änderungen der Authentisierungsmethode haben kaum Auswirkungen auf Client und Netzwerkinfrastruktur.

Handlungsempfehlungen

- **802.11i:**
  - 802.11i abwärtskompatibel zu WPA; Aufrüsten per Firmware möglich.
  - 802.11i stützt sich auf EAP, jedoch sind nur EAP-TLS, PEAP und EAP-TTLS zu empfehlen.
- **Mischbetrieb von WPA und 802.11i:**
  - Sicherheitstechnisch problematisch. Verschlüsselung entweder per TKIP (WPA) oder AES-CCMP (WPA2). TSN-konforme Access Points erlauben Mischbetrieb von 802.11i und schwachen Verfahren wie WEP.
  - SSID/VLAN-Mapping empfehlenswert; mit verschiedenen SSIDs Funkzellen logisch voneinander trennbar (pro SSID unterschiedliche Sicherheitslevel). Access Point leitet Benutzer entsprechend SSID in verschiedene VLANs).

Handlungsempfehlungen



Vielen Dank für Ihre Aufmerksamkeit.

Ihre Fragen …