Absicherung von WLANs

Kurzer Vergleich und Bewertung einiger Verfahren

IT-Symposium 2007
Nürnberg, 19. April 2007

Prof. Dr. -Ing. E. Eren
Fachhochschule Dortmund
University of Applied Sciences

Web: www.inf.fh-dortmund.de/eren
E-Mail: eren@fh-dortmund.de

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

Status-Quo bei der Absicherung von WLANs in Unternehmen

- WLANs in Unternehmen sind mittlerweile integraler Bestandteil der Netze.
- Doch Untersuchungen zeigen, dass die verwendeten Sicherheitsmechanismen nicht ausreichen.
- Unternehmen setzen sich damit Gefahren aus wie:
  - Mitschneiden von Datenverkehr im Netzwerk
  - Einschleusen von Daten wie auch von schadhaftem Code in das Netzwerk
  - Manipulation von Daten
  - Stören der Kommunikation und damit Verfügbarkeit des Netzes (DoS-Attacken)
  - Unterbrechen und Übernahme von bestehenden Verbindungen
  - Ausspähen von Benutzerdaten
  - Identifikation von Clients und damit Benutzern
  - Fälschen von WLAN-Acess Points (Rogue APs) und Simulation von Hotspots
  - Kompromittierung von Schlüsseln (WEP, WPA-PSK)
- Für Angriffe ist kein besonderes Know-how notwendig! Freie Tools im Netz machen es unversierten Angreifern möglich ...

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

Warum WEP nicht in Frage kommt …

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

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

Warum das einfache WPA nicht in Frage kommt …

- **Wi-Fi Protected Access (WPA):**
  - Zwar sind Vertraulichkeit (RC4-Verschlüsselung) und Datenintegrität (MIC) durch das TKIP-Verfahren gegeben, jedoch bietet dies nur eine Grundsicherheit auf der Bitübertragungsschicht.
    - **Problem:**
      - MIC nutzt einen schwachen Hash-Algorithmus beim MIC. Ein Angreifer kann irgendwann zufällig ein Paket mit der richtigen Prüfsumme senden, das vom Access Point akzeptiert und durchgelassen wird.

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

Warum das einfache WPA nicht in Frage kommt …

- **WPA:**
  - *WPA Personal (WPA-PSK):*
    - Einfachste Variante
    - für den Heimbetrieb ausgelegt, d.h. für Anwender ohne 802.1X-Infrastruktur.
    - Es kommt ein Pre-shared Key (PSK) zum Einsatz.
  - **Problem:**
    - Risiko von Wörterbuchattacken. I.d.R. wird ein einziger Pre-shared Key für alle Stationen einer SSID benutzt. Ein Angreifer kann diesen Schlüssel ableiten.
    - Außerdem bestimmt die Qualität der Passphrase (bei der Generierung des Schlüssels) die Sicherheit des Schlüssels.
    - Des Weiteren ist der administrative Aufwand in größeren WLANs nicht beherrschbar.

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

WPA kommt aber doch in Frage …

- **WPA mit 802.1X und EAP:**
  - Zugangssteuerung über 802.1X + EAP-Methode
  - *WPA Enterprise (WPA RADIUS):*
    - Es werden dynamische Schlüssel verwendet (Schlüsselaktualisierung)
    - Jeder Client erhält seinen individuellen Schlüssel.
    - Authentisierung erfolgt über EAP-Verfahren; i.d.R. ist es RADIUS.

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

WPA kommt aber doch in Frage …

- **WPA2 / IEEE 802.11i:**
  - Verschlüsselung und Integritätsprüfung mittels AES (CCMP).
  - 802.11i definiert mit dem sog. Robust Security Network (RSN) einen neuen Netzwerktypus (Regeln zur Ableitung und Verteilung von Schlüsseln).
  - Clients müssen die 802.1X-Prozedur sowie den Pairwise-Key-Handshake abschließen, bevor er Nutzdaten senden kann.
  - Es wirkt eine Vielzahl von Schlüsseln (Schlüsselhierarchie): Master Schlüssel zur Identitätsprüfung und temporäre Schlüssel für Sicherheitsprotokolle.
- **Vorteile:**
  - Im Vergleich zum „einfachen“ WPA deutlich sicherer.
  - CCMP ist wesentlich leistungsfähiger als TKIP (ein Schlüssel für Verschlüsselung und Integritätsprüfung).
  - 802.11i bietet u.a. geschützten Ad-hoc-Modus (Peer-to-Peer, d.h. ohne AP).

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

Handlungsempfehlungen … oder: Was sollte man beachten?

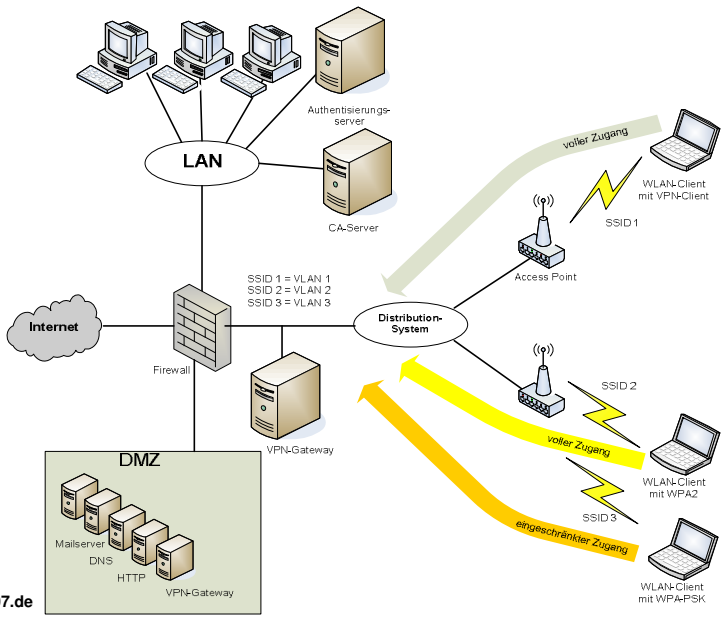
- Nicht nur von der „802.11i Security Task Group“ sowie dem „WiFi WPA“-Standard empfohlen:
  - **Gegenseitige Authentisierung**
  - **Dynamische Sitzungsschlüssel und Schlüsselmaterial:** EAP-Methode sollte Schlüsselmaterial zur Verfügung stellen.
  - **Nachrichtenintegrität:** Message Integrity Check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

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

Handlungsempfehlungen

- **802.11i:**
  - 802.11i stützt sich auf EAP, jedoch sind derzeit **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:** Mischbetrieb von 802.11i und schwachen Verfahren wie WEP möglich.
  - **SSID/VLAN-Mapping:**
    - Verschiedene SSIDs trennen Funkzellen logisch voneinander.
    - Pro SSID unterschiedliche Sicherheitslevel einstellbar.
    - Access Points leiten Clients entsprechend der SSID in verschiedene VLANs.

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren



Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

Welches EAP-Verfahren ist zu empfehlen?

- **Welches EAP-Verfahren?**
  - EAP-Variante genau auf individuelle Bedarfe abstimmen! (Trade-off zwischen Anwendungssimplizität und Sicherheit).
  - Die richtige Wahl ist eine infrastrukturelle Frage, insbesondere der Client-Unterstützung:
    - ***Wenn PKI vorhanden:***
      - EAP-TLS geeignet, jedoch hoher infrastruktureller Aufwand.
      - Sicheres Verfahren, wenn das AP-Zertifikat sicher zum Client übertragen wird oder durch eine CA überprüft wird.
    - ***Wenn keine PKI:***
      - EAP-TTLS/PEAP, besonders in heterogenen Netzen.
      - Benötigen lediglich Server-Zertifikat.
      - Sind abhängig von nachgelagerter Authentisierung.

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

Welches EAP-Verfahren ist zu empfehlen?

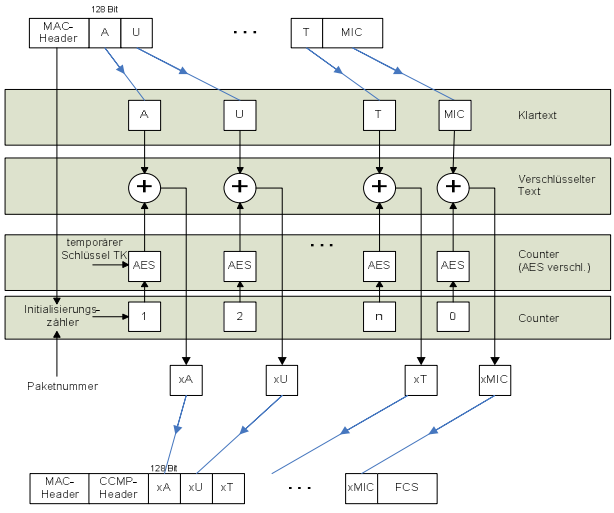
- **Welches EAP-Verfahren?**
  - **EAP-TTLS:**
    - EAP-TTLS ist wesentlich flexibler, da auch Authentisierungs-methoden ermöglicht werden, die EAP-Methoden nicht erreichen.
    - Einfacher zu implementieren als EAP-TLS.
    - Sicherheit wie bei EAP-TLS, jedoch nicht für hohe Sicherheits-anforderungen.
  - **PEAP:**
    - PEAP ist für die meisten Anwendungen sicher.
    - Mittlerer Planungs- und Implementierungsaufwand (jedoch gering, wenn mit EAP-MS-CHAPv2 kombiniert).
    - Unterstützt jedoch nur EAP-Methoden.

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

Welches EAP-Verfahren ist zu empfehlen?

- **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.

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

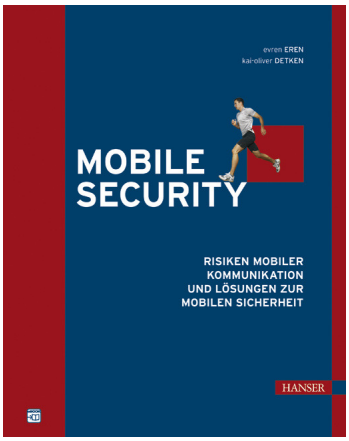


- Der Modus benutzt nicht die AES-Blockchiffre direkt, um Daten zu verschlüsseln, sondern verschlüsselt den sog. Counter (ein willkürlicher Zähler), und XOR-ed diesen mit den Daten.
- CCMP nutzt 128 Bit lange temporäre Verschlüsselungs-schlüssel (Teile des PTK), die innerhalb der 802.1X-Verhandlungsphase aus dem PMK abgeleitet werden.
- Auch kommt ein 48 Bit langer IV, die sog. Packet-Number (PN), zum Tragen.
- Zur Paketintegrität wirkt der MIC-Algorithmus mittels CBC-MAC (ein kryptographisch starkes Hashverfahren, der jedoch völlig unterschiedlich zum Michael-Verfahren bei TKIP ist).

Absicherung von WLANs – kurzer Vergleich und Bewertung einiger Verfahren

Vielen Dank für Ihre Aufmerksamkeit.

Haben Sie Fragen?
Sonst können Sie auch alles in diesem Bucg nachlesen ;-)



Evren Eren, Kai-Oliver Detken

Mobile Security – Risiken mobiler Kommunikation und Lösungen zur mobilen Sicherheit.

Carl Hanser Verlag.
ISBN 3-446-40458-9
München, Wien 2006