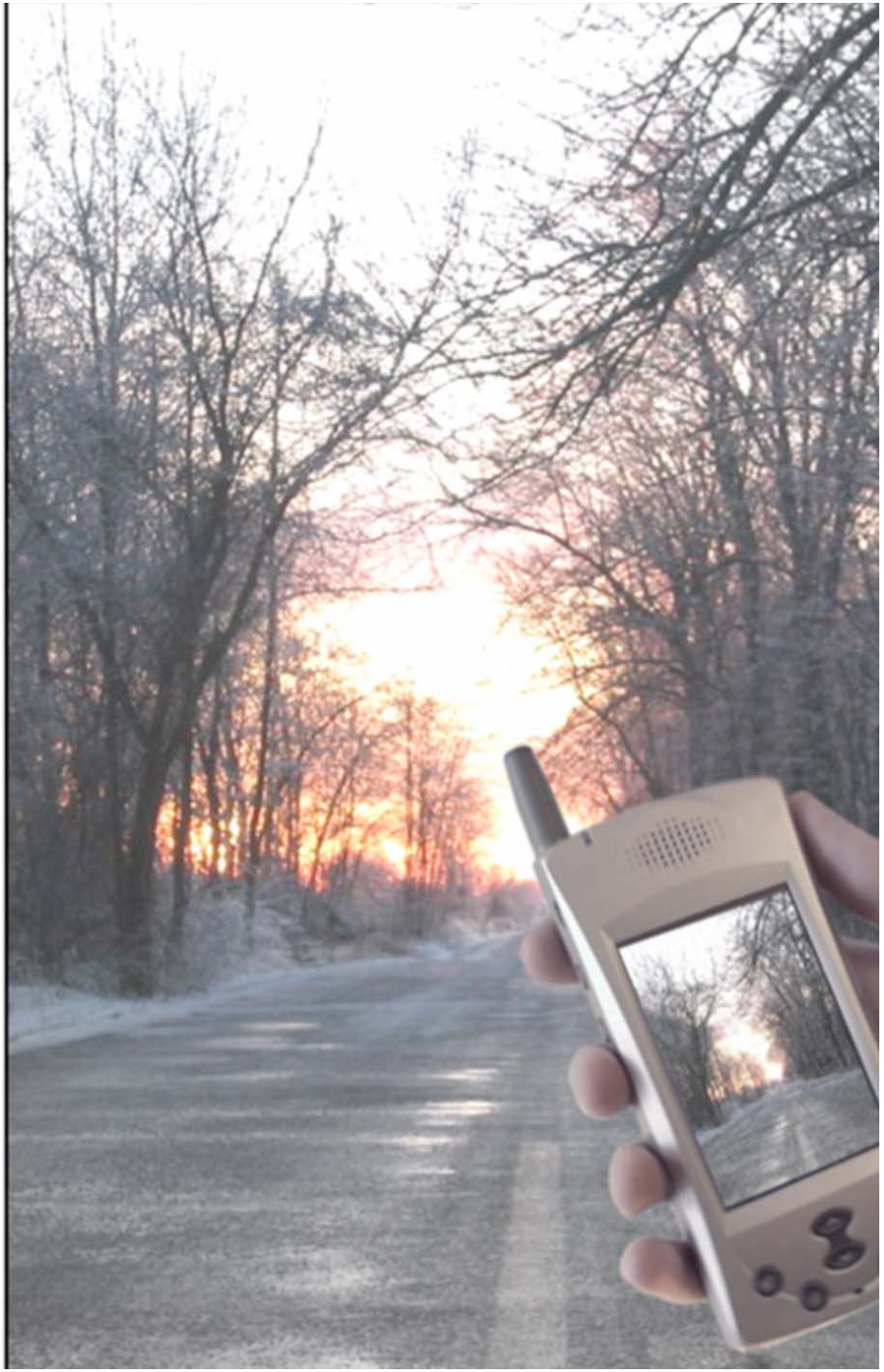
Robust Security Networks _ WLAN-Sicherheit mit IEEE 802.11i

Wireless Communication and Information 2006

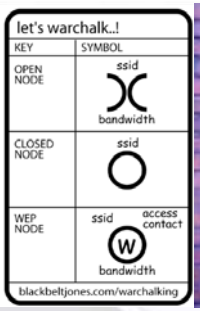
Berlin, 13. Oktober 2006

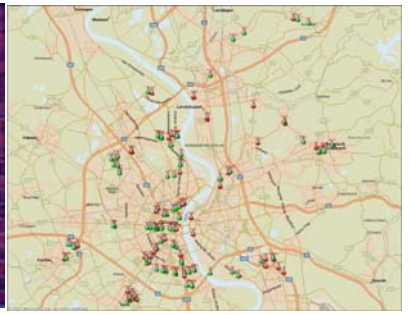
Prof. Dr. -Ing. Evren Eren
Fachhochschule Dortmund
Web: www.inf.fh-dortmund.de/eren
E-Mail: eren@fh-dortmund.de

Fachhochschule Dortmund
University of Applied Sciences



Robust Security Networks _ WLAN-Sicherheit mit IEEE 802.11i





Status-Quo WLAN

- WLANs werden im privaten Bereich und in Unternehmen jedweder Couleur eingesetzt.
- Heimbereich ca. 70 % und Unternehmensbereich ca. 30 % sind ungesichert!
- Sicherheitsmechanismen wie WEP und teilweise WPA sind nicht ausreichend.
- **Gefahren:**
  - Kompromittierung/Ermitteln von Schlüsseln
  - Mitschneiden von Datenverkehr im Netzwerk
  - Manipulation von Daten
  - Einschleusen von Daten wie auch schadhaftem Code in das Netzwerk
  - Stören der Kommunikation und damit Verfügbarkeit des Netzes
  - Ausspähen von Benutzerdaten zur Identifikation von Clients und damit Benutzern
  - Unterbrechen und Übernahme von bestehenden Verbindungen
  - Fälschen von WLAN Acess Points und Simulation von Hotspots
- Für Angriffe ist kein besonderes Know-how notwendig; freie Tools im Netz …

Robust Security Networks _ WLAN-Sicherheit mit IEEE 802.11i

WEP, einfachstes Verfahren _ Die Schwachstellen

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

Robust Security Networks _ WLAN-Sicherheit mit IEEE 802.11i

Alternative Sicherheitsmechanismen und Verfahren _ WPA (WPA1)

- Basiert auf drittem Draft von IEEE 802.11i; Subset von RSN.
- Zugangssteuerung über IEEE 802.1X + EAP-Methode(n).
- Vertraulichkeit / Datenintegrität durch TKIP (RC4-Verschlüsselung). Grundsicherheit auf Bitübertragungsschicht. Kombiniert mit 802.1X relativ sicher.
  - **Problem:** MIC nutzt einen kryptographisch 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).
  - **Problem:** I.d.R. existiert ein Preshared-Key für alle Stationen einer SSID. Risiko von Wörterbuchattacken. Angreifer kann Schlüssel ableiten. Sicherheit des Preshared-Keys hängt von Qualität der Passphrase ab. Administrativer Aufwand in größeren WLANs nicht beherrschbar.

- ***WPA Enterprise (WPA RADIUS):*** Dynamische Schlüssel für jedes versendete Paket. Für jeden Benutzer existiert ein individueller Schlüssel. Authentisierung über EAP-Verfahren, i.d.R. mittels RADIUS.

Robust Security Networks _ WLAN-Sicherheit mit IEEE 802.11i

Alternative Sicherheitsmechanismen und Verfahren _ IEEE 802.11i / WPA2

- Juni 2004 verabschiedet; WPA2 wird als Subset des Standards veröffentlicht.
- **RSN:** 802.11i definiert neuen Netzwerktypus: Robust Security Network (RSN). RSN ist ein Satz von Prozeduren, die festlegen, wie temporäre Keys von einem Master Key abgeleitet und verteilt werden.
- **Schlüsselhierarchie:** Es wirkt eine Vielzahl von Schlüsseln.
  - Vom *Pairwise Master Key* (PMK), der während der Clientauthentisierung im Client und Authentisierungsserver erzeugt wird, wird der *Pairwise Transient Key* (PTK) abgeleitet, welcher aus folgenden Schlüsseln besteht:
    - EAPoL Encryption Key *(verschlüsselt den Schlüsselaustausch)*
    - EAPoL MIC Key *(prüft die Integrität des Schlüsselaustausches)*
    - Temporal Key (Session-/MIC-Key) (*verschlüsselt den Datenverkehr*).
  - Für die Aushandlung des PMK zwischen Authentisierungsserver und Client kommt EAP zum Tragen.
  - Der PTK wird im Client und Access Point im 4-Wege-Handshake erzeugt.

Robust Security Networks _ WLAN-Sicherheit mit IEEE 802.11i

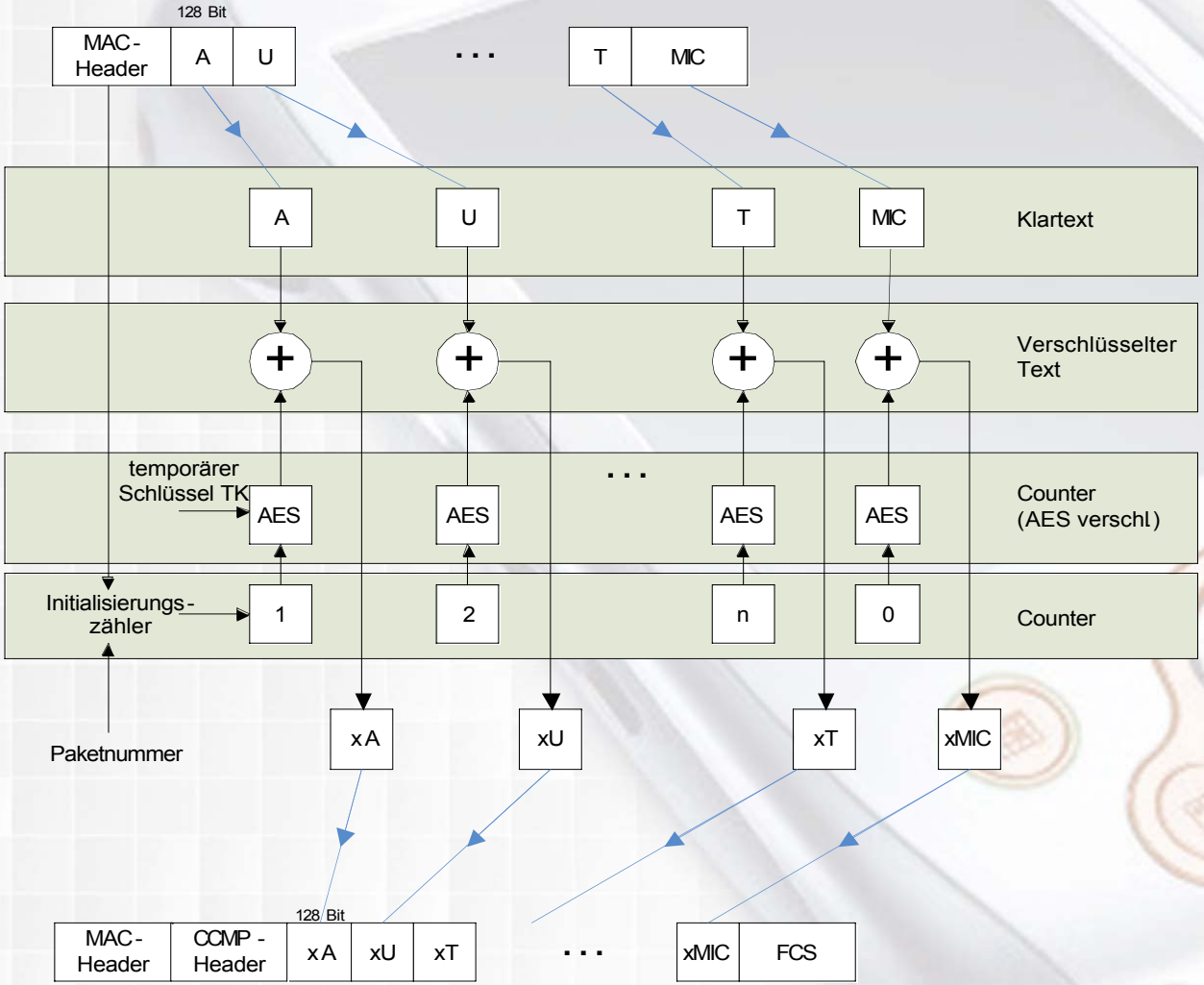
Alternative Sicherheitsmechanismen und Verfahren _ IEEE 802.11i / WPA2

- **Verschlüsselung und Integrität durch CCMP:**
  - Verschlüsselung und Integritätsprüfung erfolgen durch CCMP (Counter Mode with CBC-MAC Protocol).
  - Der „Counter Mode“ dient allein der Verschlüsselung.
  - Der CBC-MAC-Mechanismus ist zuständig für Datenintegrität.

- **Gegenseitige Authentisierung (802.1X und EAP):**
  - RSN setzt eine gegenseitige Authentisierung von Client und Authentisierungsserver voraus.
  - Dabei verwendet 802.11i zwischen Client und Access Point
    - 802.1X (EAPoL) um EAP-Nachrichten über WLAN zu kapseln.
    - EAP als Transportmechanismus für die Authentisierungsmethoden.
  - Bevor der Client überhaupt Nutzdaten senden darf, muss er zunächst die 802.1X-Prozedur sowie den 4-Wege-Pairwise-Key-Handshake (Einrichtung des PTK) abschließen.

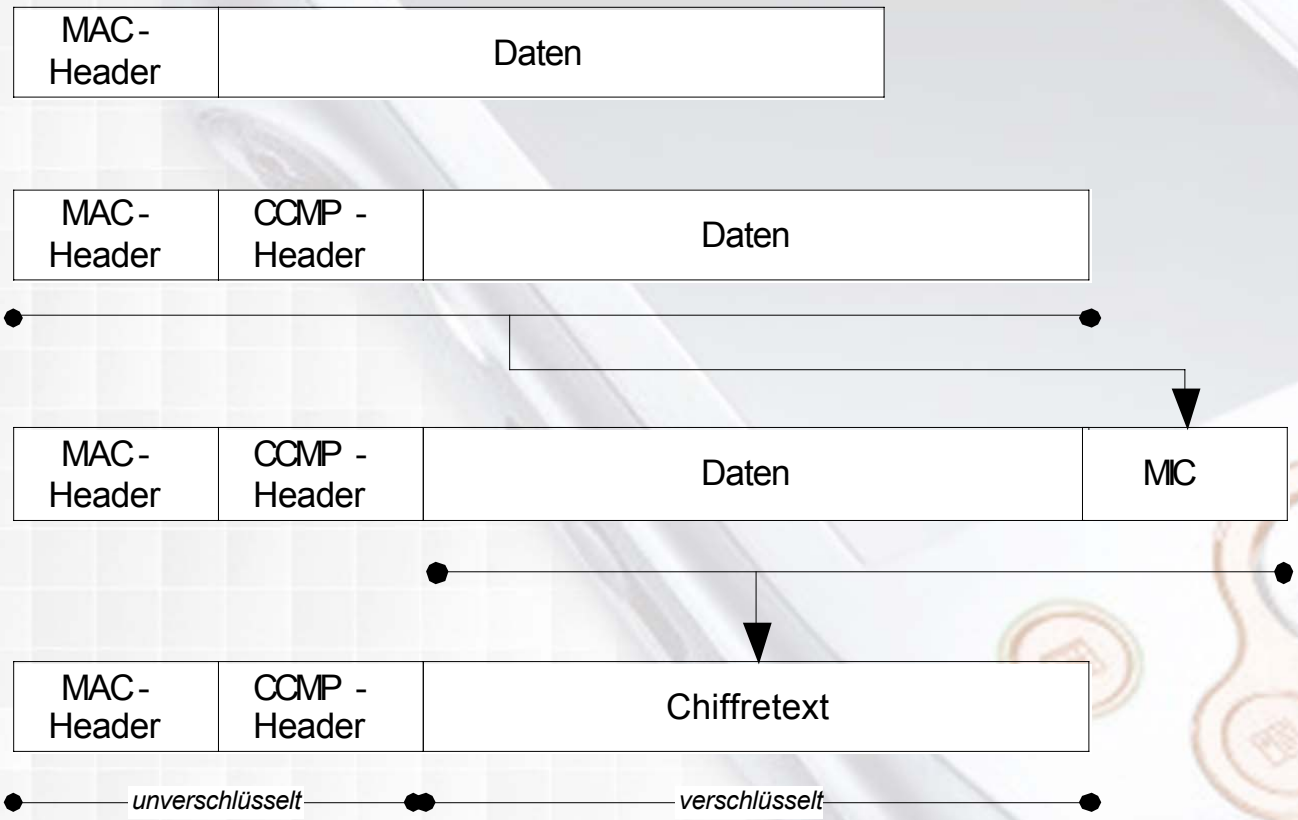
Robust Security Networks _ WLAN-Sicherheit mit IEEE 802.11i

802.11i / WPA2 _ Wirkungsweise des Counter Mode



- Der Modus benutzt nicht die AES-Blockchiffre direkt, um Daten zu verschlüsseln, sondern verschlüsselt den sog. Counter (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 des TKIP ist).

802.11i / WPA2 _ Verschlüsselung



- Die Verschlüsselung arbeitet auf Basis eines Schicht-2-Datenpakets namens „MAC Protocol Data Unit (MPDU)“.
- Von diesem Paket entnimmt man zuerst den MAC-Header.
- Im nächsten Schritt wird ein CCMP-Header erzeugt, der Informationen über das verschlüsselte Paket enthält.
- Danach wird der "Message Integrity Code (MIC)" berechnet, und anschließend die Nachricht und der MIC zusammen verschlüsselt (AES).
- Im letzten Schritt wird das Paket zusammengesetzt.

Robust Security Networks _ WLAN-Sicherheit mit IEEE 802.11i

802.11i / WPA2 _ Die Vorteile

- **Zentrale Authentisierung und Autorisierung:** Zentralisierter AAA-Mechanismus zur einzelnen Identifikation/Authentisierung von Clients → Policy-basierter Netzwerkzugang. Da AAA-Infrastrukturen nicht nur für WLAN, sondern auch für LAN und VPN einsetzbar sind, ist eine hohe Flexibilität in der Zugangstechnik gegeben.
- **Gegenseitige Authentisierung** (802.1X und EAP):
  - Einheitliche Authentisierungsmethodik mittels EAP-Verfahren.
  - Änderung der Authentisierungsmethode hat kaum Auswirkungen auf Client und Netzwerkinfrastruktur.
- **Session-basierte Verschlüsselung:** Kombination von 802.1X, EAP (z.B. EAP-TLS) und RADIUS erlaubt pro Verbindung und Sitzung verschlüsselten Datenverkehr mit dynamischen Schlüsseln.
- **Dynamische Sitzungsschlüssel und Schlüsselmaterial:** EAP-Methoden, die Schlüsselmaterial zur Verfügung stellen → z.B. EAP-TLS.
- **Schnelles Re-Keying:** Re-Keying fordert Clients auf, Schlüssel zu aktualisieren (z.B. periodisch). Essentiell für Multicast/Broadcast-Verkehr.
- **Nachrichtenintegrität:** Message Integrity Check (MIC mittels CBC-MAC).

802.11i / WPA2 _ Die Vorteile

- **Leistungsfähige Verschlüsselung und Integritätsüberprüfung:** Das CCMP-Verfahren ist wesentlich leistungsfähiger als TKIP, da ein und derselbe Schlüssel zur Frame-Verschlüsselung und Integritätsprüfung zum Tragen kommt.
- **Sicher:** Im Vergleich zu WPA deutlich sicherer. WPA2 hat diverse Untersuchungen und Prüfungen von Kryptoanalytikern bestanden und entspricht dem Stand der Technik.
- **Punkt-zu-Punkt-Verbindungen:** 802.11i bietet geschützten Ad-hoc-Modus.

802.11i / WPA2 _ Einsatz und Handlungsempfehlungen

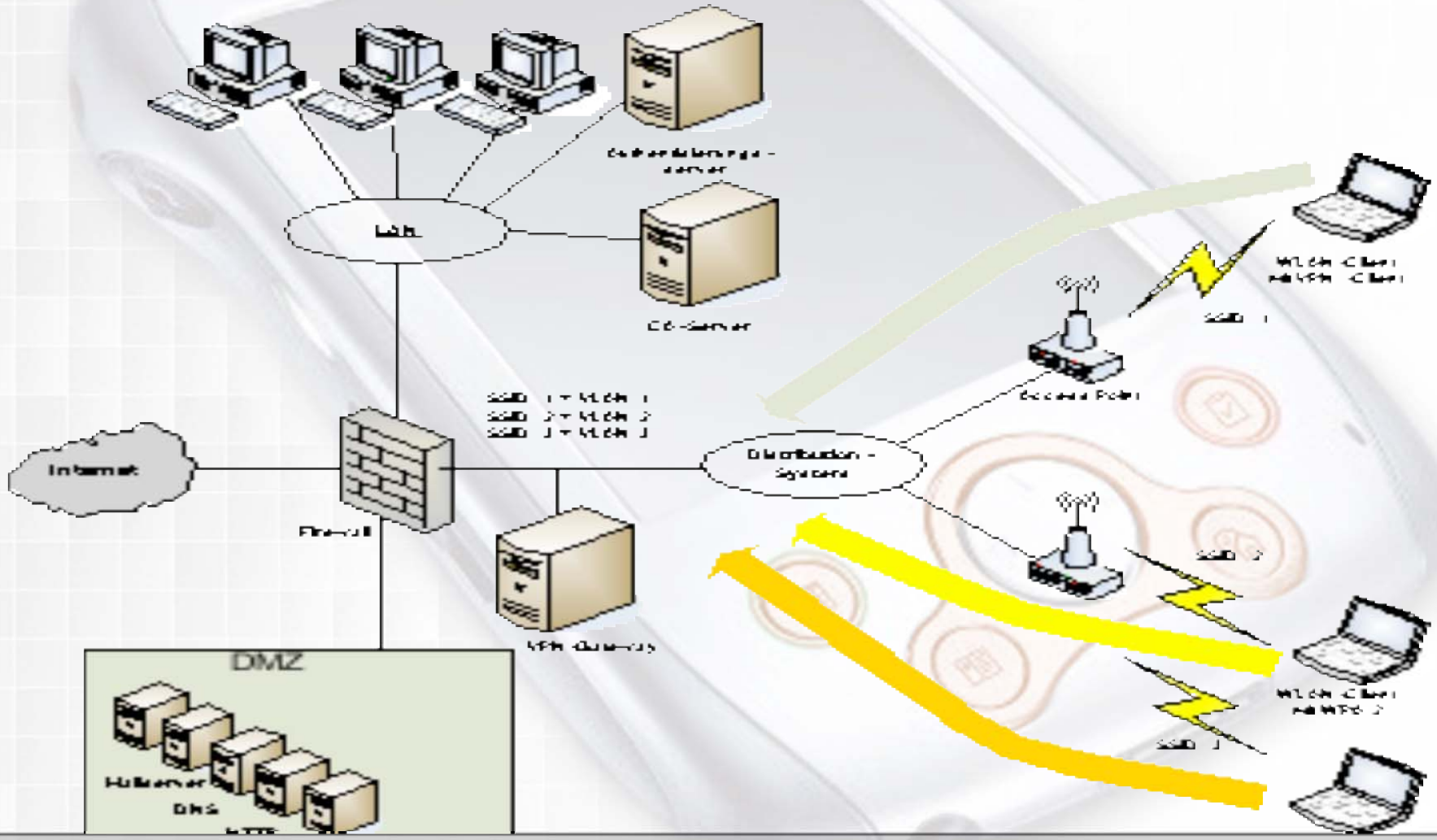
- **EAP-Verfahren:**
  - 802.11i stützt sich auf EAP, jedoch sind nur EAP-TLS, EAP-TTLS und PEAP zu empfehlen.

- **Mischbetrieb von WPA und 802.11i:**
  - Sicherheitstechnisch problematisch, da innerhalb eines WLANs die Verschlüsselung entweder per TKIP (WPA) oder AES-CCMP (WPA2) erfolgen kann (Exklusivität). Abhilfe: TSN-konforme Access Points erlauben Mischbetrieb von 802.11i und schwachen Verfahren wie WEP.

  - **SSID/VLAN-Mapping:** SSID/VLAN-Mapping empfehlenswert, da mit verschiedenen SSIDs Funkzellen logisch voneinander getrennt werden können (pro SSID unterschiedliche Sicherheitslevel abbildbar). Der Access Point leitet Benutzer entsprechend der SSID in verschiedene VLANs). (vgl. Abbildung S. 12).

Robust Security Networks _ WLAN-Sicherheit mit IEEE 802.11i

802.11i / WPA2 _ Einsatz und Handlungsempfehlungen (WLAN-Mischbetrieb)



Handlungsempfehlungen _ EAP-Verfahren

- **Welches EAP-Verfahren einsetzen?**
  - 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 Access Point Zertifikat sicher zum Client übertragen wird oder durch eine CA überprüft wird.
    - ***Wenn keine PKI vorhanden:*** EAP-TTLS/PEAP, besonders geeignet in heterogenen Netzwerken (Microsoft und Linux). Nur Server-Zertifikat notwendig; ist jedoch abhängig von nachgelagerter Authentisierung.

Handlungsempfehlungen _ EAP-Verfahren

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

  - *Alternative zur "gegenseitigen Authentisierung":* EAP-Methoden, die mit zwei Tunneln (äußerer und innerer Tunnel) arbeiten und im inneren Tunnel schwächere Authentisierungsverfahren schützen (z.B. PEAP).

Vielen Dank für Ihre Aufmerksamkeit.

Haben Sie Fragen?