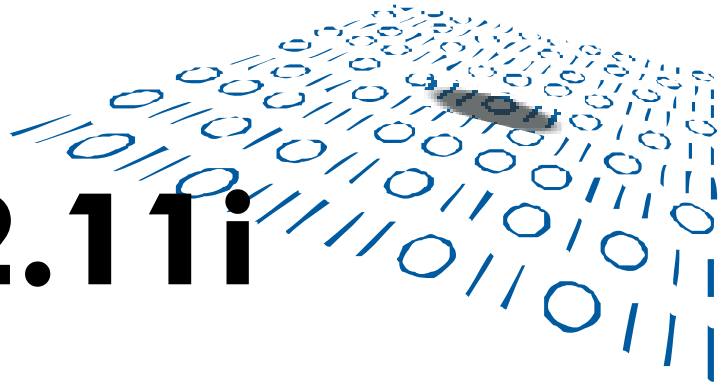
on focus



BSP. CONSULT

IEEE 802.11i
-
endlich sichere WLANs?

Dipl. Wirt.-Inf. Michael Raith
IT-Security Consultant
Tel. (0941) 29 77 4 - 0
mr@bsp-consult.com
PGP Key-ID: 0x 83F0 5C6A

Überblick

- Bestandsaufnahme WLAN-Sicherheit
- WEP, der erste Versuch
- WPA, die Nachbesserung
- 802.11i, die Lösung?

BSP. CONSULT

Dipl. Wirt.-Inf. Michael Raith

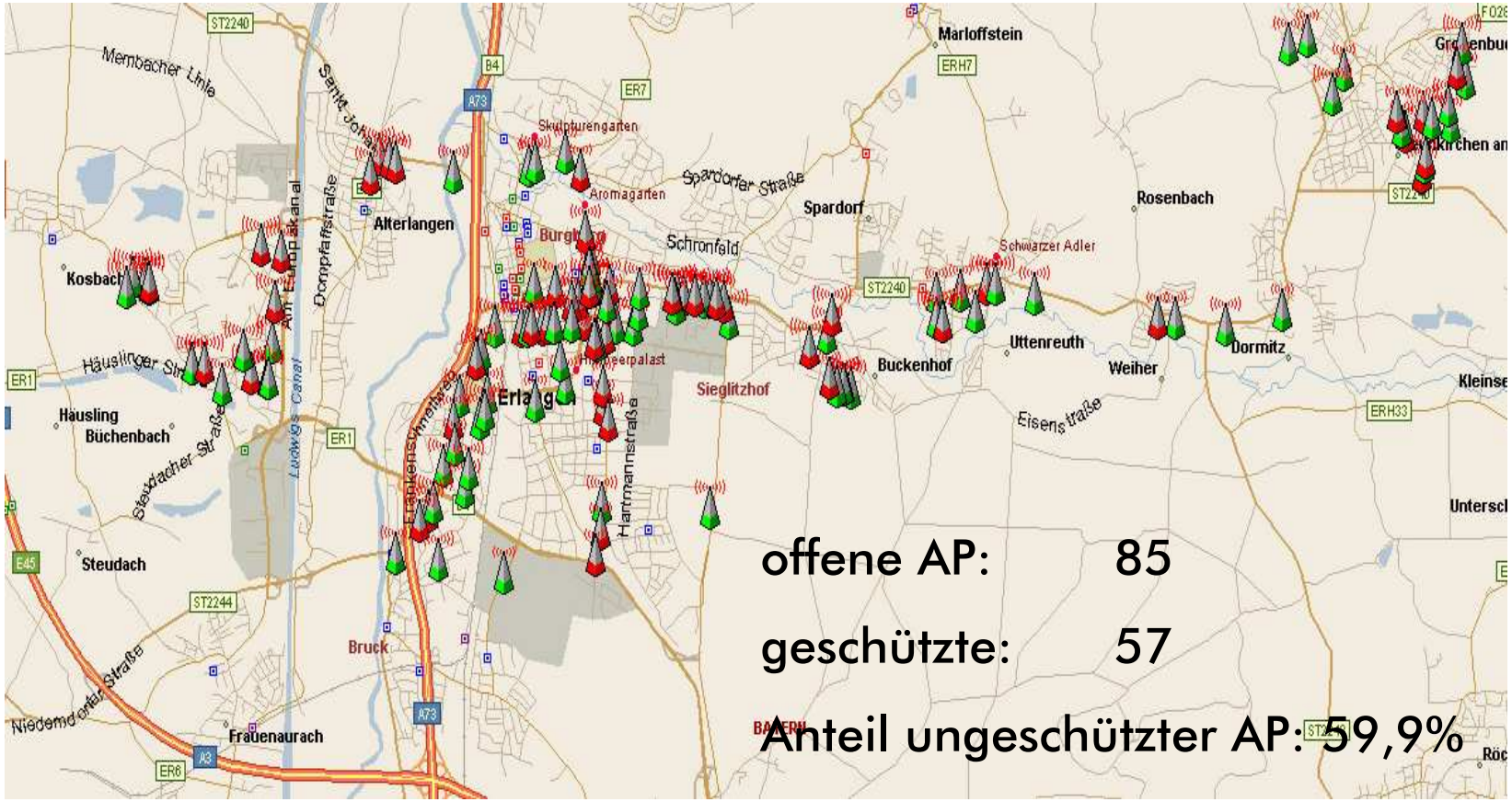
Bestandsaufnahme

- WLAN sehr beliebt, Verbreitungsgrad stark steigend
- derzeit knapp über 97000 Netze in Deutschland von Wardrivern erfasst

- ca. 60% der erfassten Netze komplett ungeschützt

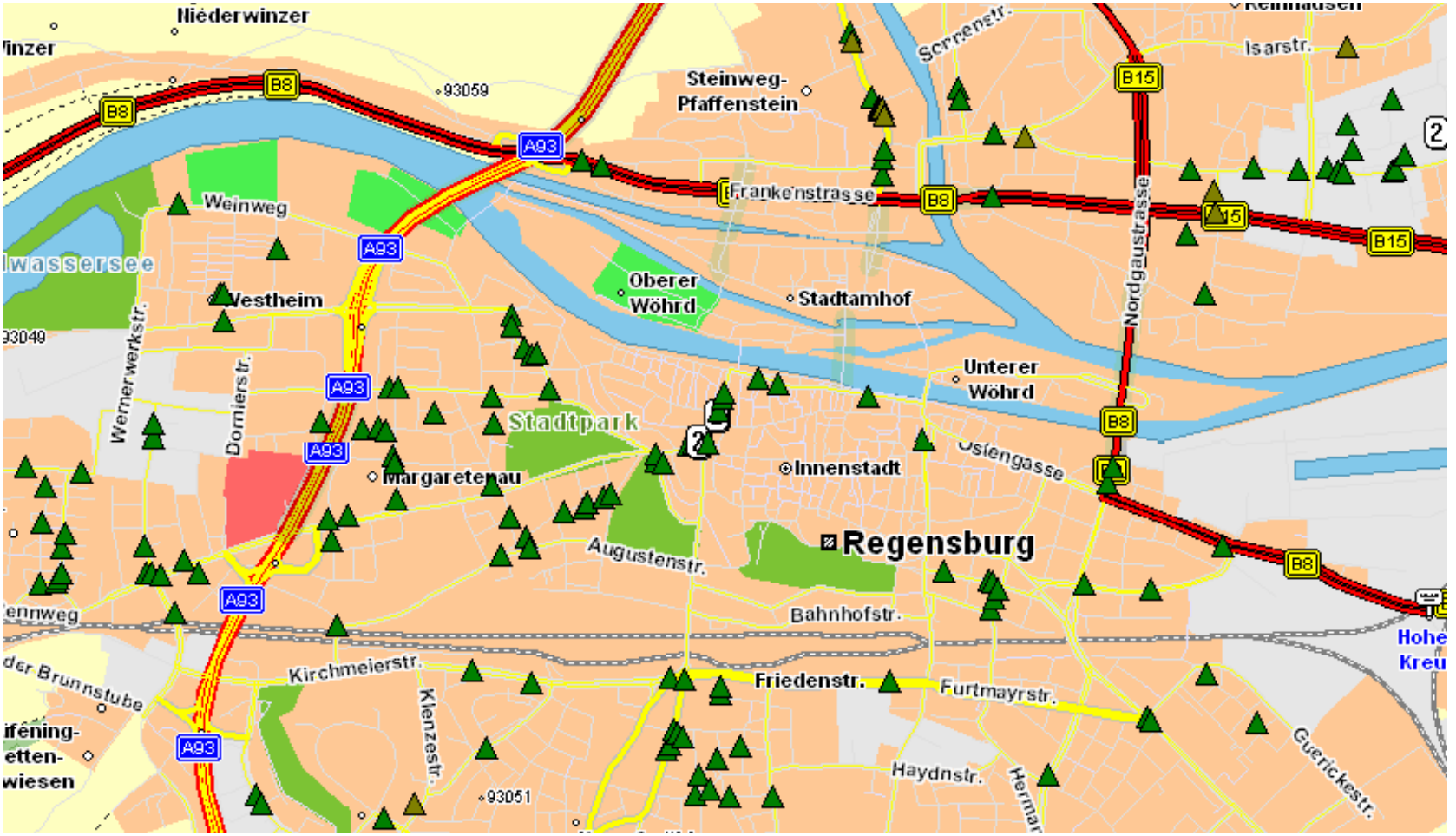
BSP. CONSULT
Dipl. Wirt.-Inf. Michael Raith

Wardriving Erlangen



BSP. CONSULT
Dipl. Wirt.-Inf. Michael Raith

Wardriving Regensburg



BSP. CONSULT

Dipl. Wirt.-Inf. Michael Raith

WLAN Bestandsaufnahme

- Sicherheitsbewusstsein nicht existent
- Unsicherheit zuzugeben verkauft sich nicht (z.B. DSL/WLAN-Router)
- unwissende Mitarbeiter?
- Defaultkonfiguration: Zugang frei und unverschlüsselt

=> nicht existente Sicherheit bei den meisten Installationen

BSP. CONSULT
Dipl. Wirt.-Inf. Michael Raith

WEP

- bei Verabschiedung des WLAN-Standards vorgesehenes Protokoll zur Absicherung von Funknetzen

- Wired Equivalency Protocol
- kein „Peer Review“ vor Veröffentlichung des Standards
- offensichtlich keine Kryptoexperten bei der Entwicklung beteiligt

BSP. CONSULT
Dipl. Wirt.-Inf. Michael Raith

WEP

- Preshared Key (PSK)
- Keylänge 40 Bit (später 104)

- Verschlüsselung mit RC4-Stromchiffre per XOR-Verknüpfung
- Integritätsprüfung per CRC-Verfahren
- 24 Bit IV (Initialisierungsvektor) per Zufallsgenerator erzeugt dient zusammen mit PSK als symmetrischer Schlüssel

WEP

- Implementierung des IV Zufallsgenerators teilweise fehlerhaft oder nicht vorhanden (Paketzähler als IV missbraucht)
- selbst bei gutem Zufallsgenerator liegt die Wahrscheinlichkeit von zwei identischen IVs schon nach nur 4823 Paketen bei 50%. (Geburtstagsüberraschung)
- Prüfsummenverfahren (CRC) zur Integritätsprüfung völlig ungeeignet, da Angreifer diesen ebenfalls korrekt berechnen können.

BSP. CONSULT
Dipl. Wirt.-Inf. Michael Raith

WEP

- zusätzliche kryptografische Schwächen in RC4 (FMS Fluhrer-Mantin-Shamir) haben schwache IV zur Folge
- Schlüsselmanagement
  - alle Beteiligten haben identische PSK
  - alle PSK müssen manuell eingegeben und geändert werden
  - Änderungen werden dementsprechend selten durchgeführt

Dipl. Wirt.-Inf. Michael Raith

WPA

- Wifi-Protected Access
- Nachbesserung von bestehender WiFi-kompatibler Hardware unter Zugriff auf Verfahren, die in 802.11i kommen werden
- Besseres Schlüsselmanagement
- Verschlüsselung mit TKIP (Temporal Key Integrity Protocol) – benutzt jedoch weiterhin RC4
- Integrität wird durch MIC mit Hilfe des sog. Michael-Algorithmus sichergestellt
- Authentifizierung: 802.1x, EAP, Radius oder PSK

802.11i

- Robust Security Network (RSN)

- soll alle Sicherheitsprobleme seiner Vorgänger lösen
- Entwurf im Sommer 2004 verabschiedet
- Erste WLAN Produkte mit implementiertem 802.11i sind im Herbst zu erwarten

Dipl. Wirt.-Inf. Michael Raith

802.11i

Schlüsselmanagement:
(wahlweise per Radius oder PSK)

- Pairwise Master Key (PMK) 256 Bit
  erzeugt bei Bedarf
- Pairwise Transient Keys (PTK) 384 Bit

  vom PTK werden
- EAPOL-Keys zum Schlüsseltausch (128Bit)

  sowie
- Session Keys (128Bit) abgeleitet

Dipl. Wirt.-Inf. Michael Raith

802.11i

- da Benutzer keine 256Bit Master Keys definieren werden, wurde ein Verfahren definiert, das aus Klartext-Passwörtern möglichst sichere 256Bit Keys generiert

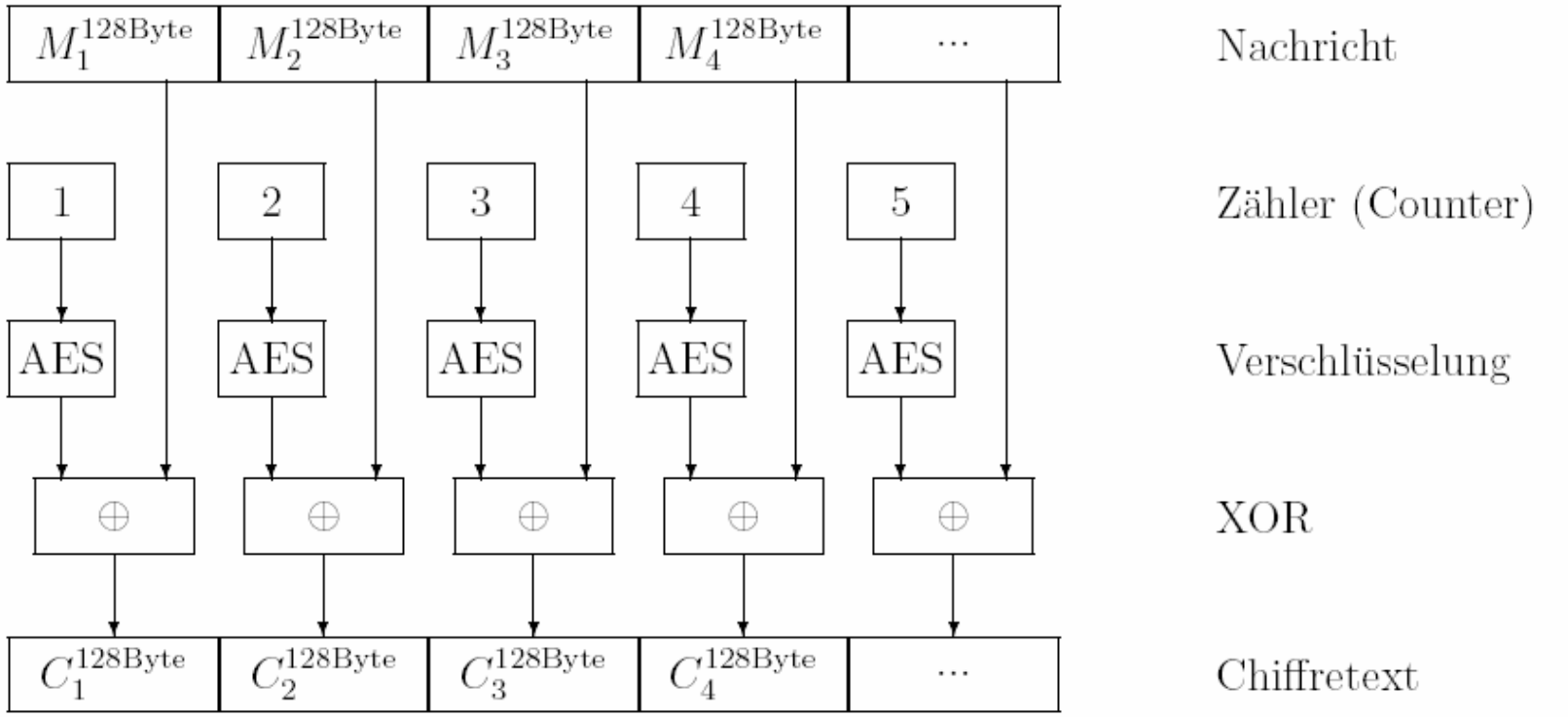
- solange sichere Master Passwörter benutzt werden, sind auch resultierende Master Keys sicher
- zu kurze oder einfach zu erratende (Wörterbuch) Master Passwörter erlauben Angreifern eine einfachen Zugriff auf das Netz

Dipl. Wirt.-Inf. Michael Raith

802.11i

- Verschlüsselung wahlweise TKIP oder AES-CCMP
- AES (Advanced Encryption Standard) genießt als offizieller Nachfolger des DES hohes Ansehen
- frühere 24Bit IV durch 48Bit PN (Packet Number) abgelöst
- AES wird in 802.11i im Counter-Mode betrieben, positiver Nebeneffekt: Reply Attacken können verhindert werden

AES Counter Mode



BSP. CONSULT
Dipl. Wirt.-Inf. Michael Raith

AES CCM

- CCM ist eine spezielle Entwicklung die zusätzlich zur Verschlüsselung auch noch die Integritätssicherung der Nachrichten übernimmt

- AES wird hierzu verwendet, um eine kryptografische Prüfsumme über eine Nachricht zu ermitteln und deren Integrität bestätigen zu können

-> tatsächlich sinnvolle Replay und Fälschungserkennung

BSP. CONSULT
Dipl. Wirt.-Inf. Michael Raith

Authentifizierung

- 802.11i nutzt die auch schon in WPA vorweggenommenen Methoden von 802.1x, um nicht nur Clients besser gegenüber dem AP authentifizieren zu können, sondern auch um den AP gegenüber dem Client zu authentifizieren

- EAP (EAPOL, EAP over LAN)
- TLS Transport Layer Security (z.B. in EAP/TLS)
- PEAP (Protected EAP)
- RADIUS

BSP. CONSULT
Dipl. Wirt.-Inf. Michael Raith

Fazit

- Verbesserungen in 802.11i sind ein Quantensprung in der Sicherheit gegenüber WEP
- Im Vergleich zu WPA, das die wichtigsten Änderungen schon vorwegnahm, fällt hauptsächlich die Verwendung von AES statt RC4 auf.
- Wichtig bei PSK Einsatz: gute Passwörter wählen
- auch WEP ist immer noch besser als gar kein Schutz

Dipl. Wirt.-Inf. Michael Raith