WLAN & Security

Willkommen zum Workshop

Referent:
Reto Burger
Dipl. Inf Ing. HTL FH

Vorwort

- Hacking ist nach internationalem, deutschem und schweizerischen Recht strafbar.
- Deutschland: Siehe §202a, 303a und §303b StGB.Text
- Schweiz: Siehe Art. 143, 143bis, 179, 144, 147, 150, 150bis, Fernmeldegesetz: Art 49, 50, 51!

Was erwartet Sie?

- Grundlagen von WLANs
- Wer bricht in WLANs ein?
- Wie bricht man in WLANs ein?
- Knacken der WEP-Verschlüsselung
- WPA und WPA II
- Wie setzt man sichere WLANs auf?

WLANs sind praktisch

- Kabelarbeiten sind weitaus einfacher als bei einer strukturieren Ethernet-Verkabelung (geringere Investitionskosten).
- Netzteilnehmer werden örtlich ungebunden.
- Manche Netzwerke werden durch WLANs erst ermöglicht (Denkmalschutz, schwer zugängliche Bereiche).
- WLANs sind flexibel und daher einfach an neue Bedürfnisse anzupassen.

Was standardisiert 802.11?

<table>
<tr><td>OSI Layer 2</td><td colspan="3">802.2</td><td>Datalink Layer</td></tr>
<tr><td rowspan="2">OSI Layer 1</td><td colspan="3">802.11</td><td>MAC Layer</td></tr>
<tr><td>FHSS</td><td>DSSS</td><td>IR</td><td>Physical Layer</td></tr>
</table>

- **FHSS = Frequency Hopping Spread Spectrum**
- **DSSS = Direct Sequence Spread Spectrum**
- **IR = Infrarot**

WLAN-Standards (I)

- **IEEE 802.11 (1997)**
  - 2,4 GHz-Frequenzband, 1 und 2 MBit/sec
  - FHSS, DSSS, IR
  - Infrastructure (BSS) oder Ad-Hoc (iBSS)
  - WEP-Verschlüsselung
- **IEEE 802.11a (1999)**
  - 5 GHz-Frequenzband, 54 MBit/sec
  - in Europa nicht zugelassen

WLAN-Standards (II)

- **IEEE 802.11b (1999)**
  - 2,4 GHz-Frequenzband
  - 5,5 und 11 MBit/sec
  - nur noch DSSS
- **IEEE 802.11g (15.06.2003)**
  - 2,4 GHz-Frequenzband
  - 54 MBit/sec
- **IEEE 802.11i (25.06.2004)**
  - Sicherheitsstandard für Wireless LAN
  - auch WPA II genannt

WLAN-Standards (III)

- **IEEE 802.11n (Oktober 2009)**
  - 2,4 und 5 GHz-Frequenzband
  - 300 MBit/sec (bis 600Mbps möglich)
  - nur noch DSSS
- **IEEE 802.11ac (18.12.2013)**
  - 5 GHz-Frequenzband
  - 1299 MBit/sec (technisch möglich bis 6936 Mbps)
- **IEEE 802.11ad (25.06.2014)**
  - 60 GHz-Frequenzband
  - Nur wenige Meter (max. 10m)
  - Bis 6930 Mbps

Das zentrale Problem: offenes Medium

- Wireless LANs arbeiten auf Funkbasis und bieten im Gegensatz zu herkömmlichen Netzen keine physikalische Sicherheit mehr.
- Auf WLAN-Komponenten (Netzwerkkarte oder Accesspoint) kann mit entsprechendem Equipment häufig auch über mehrere hundert Meter Entfernung zugegriffen werden.
- Die Funkwellen sind sehr einfach zu empfangen und zu dekodieren (macht jede Wireless-Netzwerkkarte für Sie).
- Folge: Nicht vertrauenswürdige Personen können mit ihrem Netzwerk interagieren.

Wer greift WLANs warum an?

- **Unterteilung in vier Kategorien**
  - Spassfraktion
  - Pragmatiker
  - Kriminelle Typ 1
  - Kriminelle Typ 2

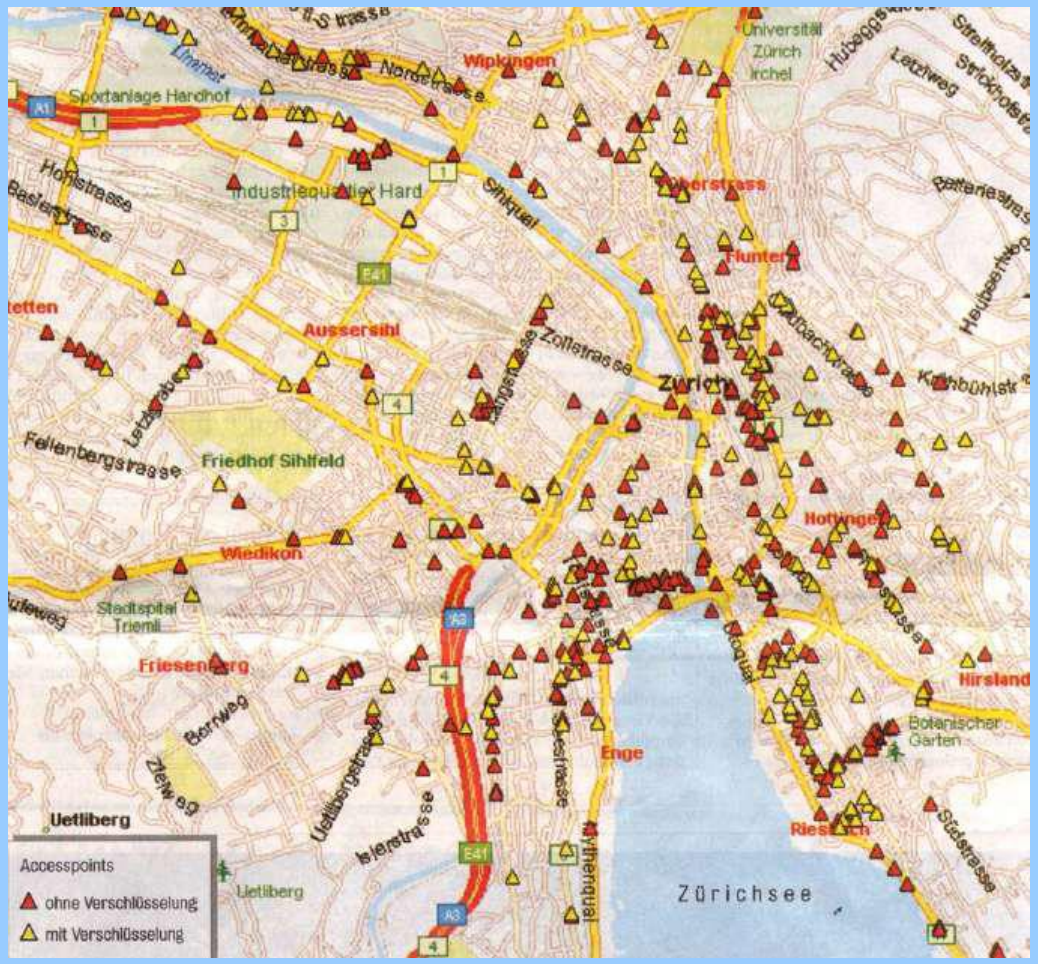
Spassfraktion: '3-Minuten-Instanthacking'

- WLANs sind sehr weit verbreitet
- Sehr viele WLANs arbeiten komplett ungeschützt.
- Das notwendige Equipment zum Aufspüren und Einbrechen ist preisgünstig und auch für Schüler oder Studenten erschwinglich.
- Das technische Know-How für das kreative Arbeiten mit WLANs kann sich einfach angeeignet werden.

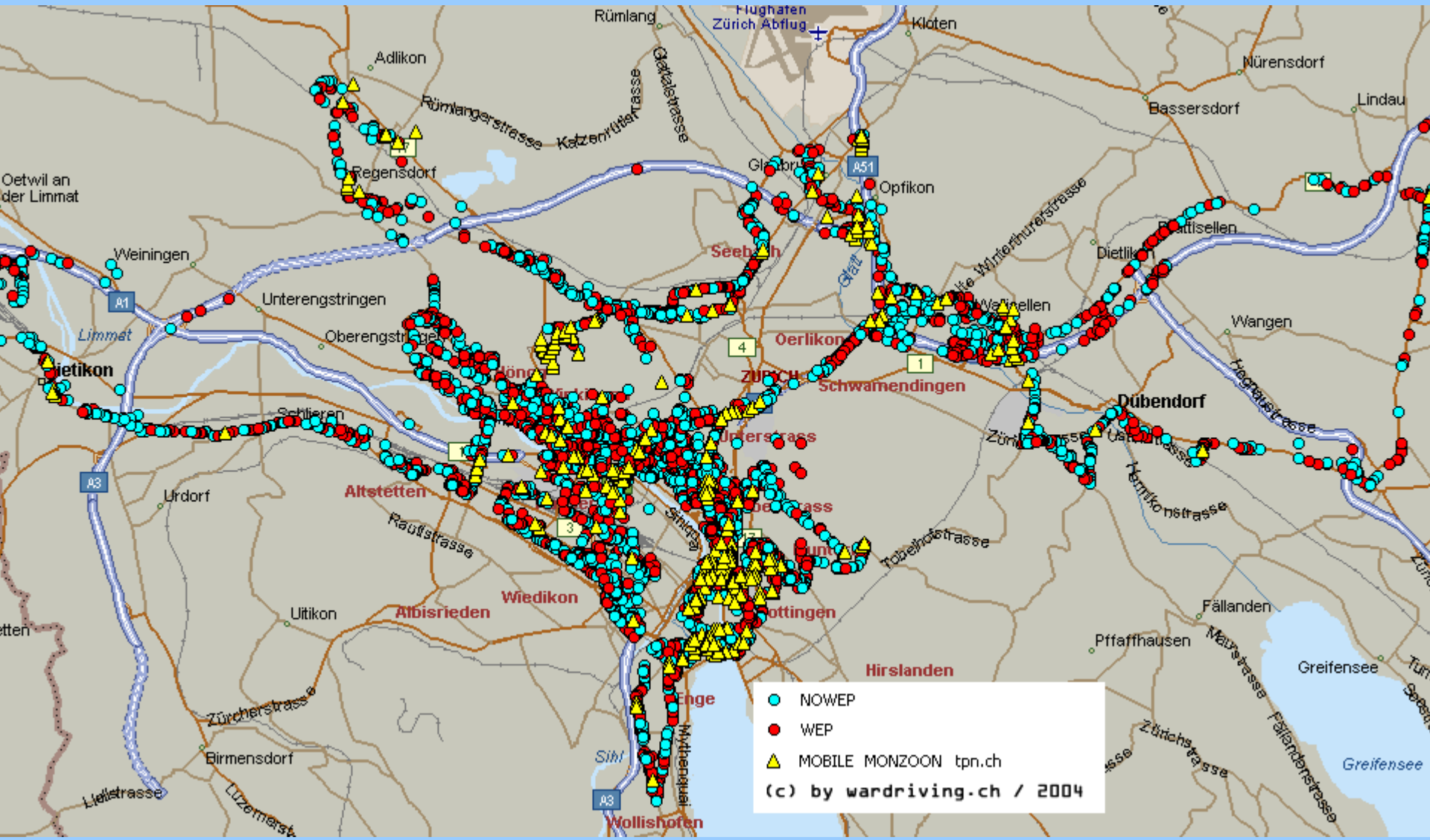
Spassfraktion: Volkssport Wardriving

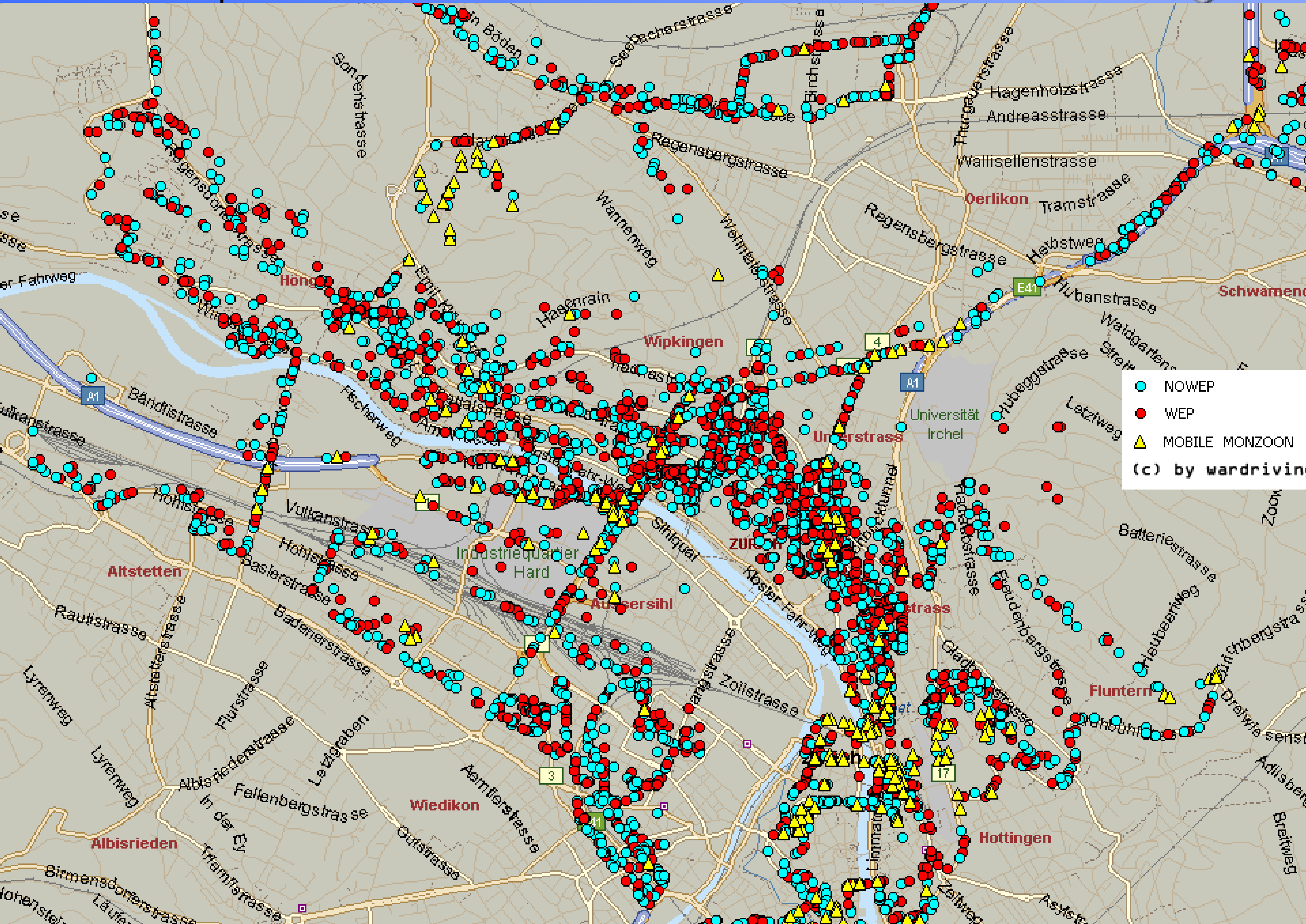
- Das systematische Auffinden und Katalogisieren von WLANs wird 'Wardriving' genannt
- Die deutsche und CH-Szene ist recht aktiv.
- Wardrivings haben z.T. echten Party-Charakter angenommen.

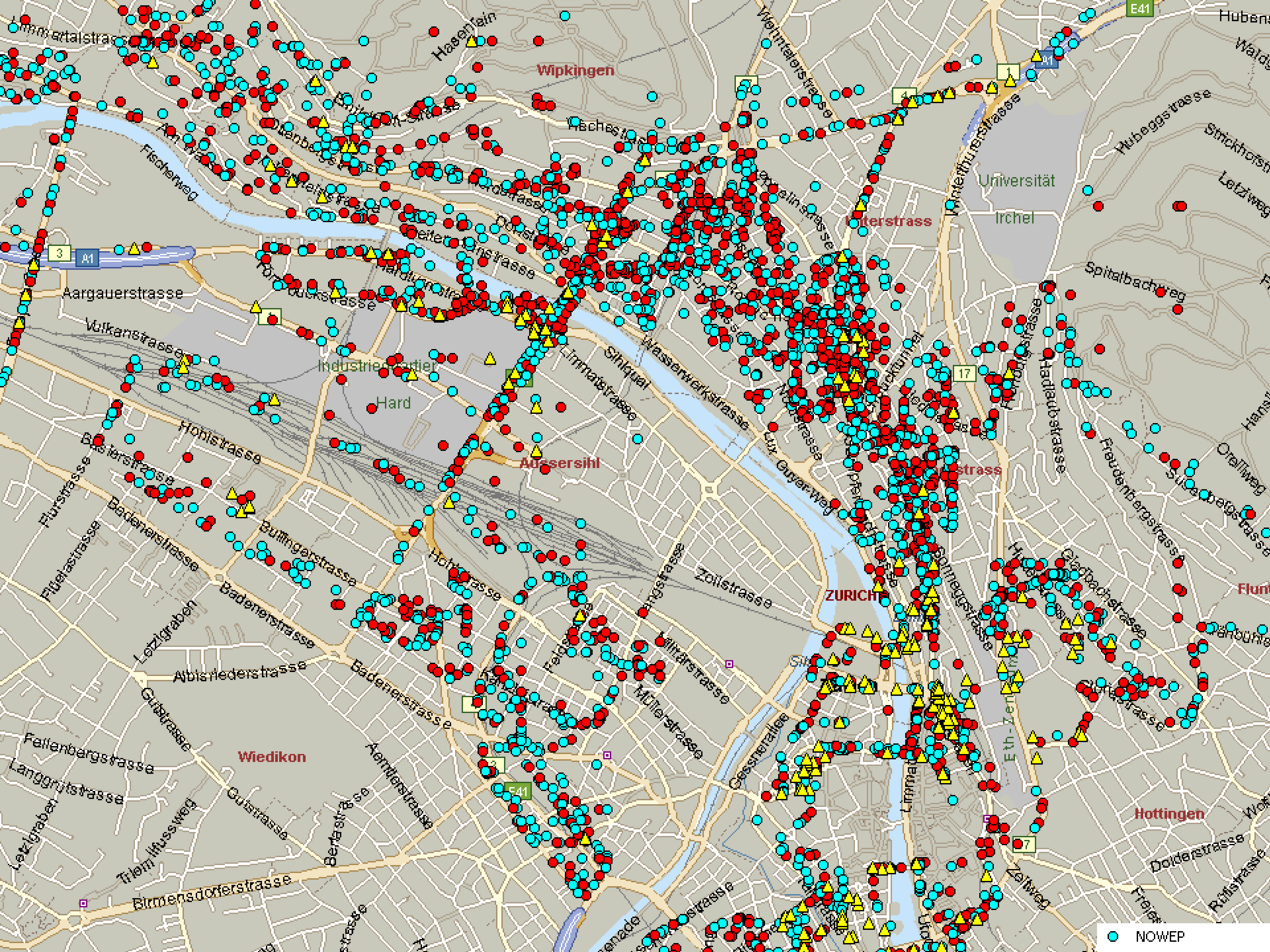
WLAN-Topologie: Beispiel Zürich 2002



WLAN-Topologie: Beispiel Zürich 2004



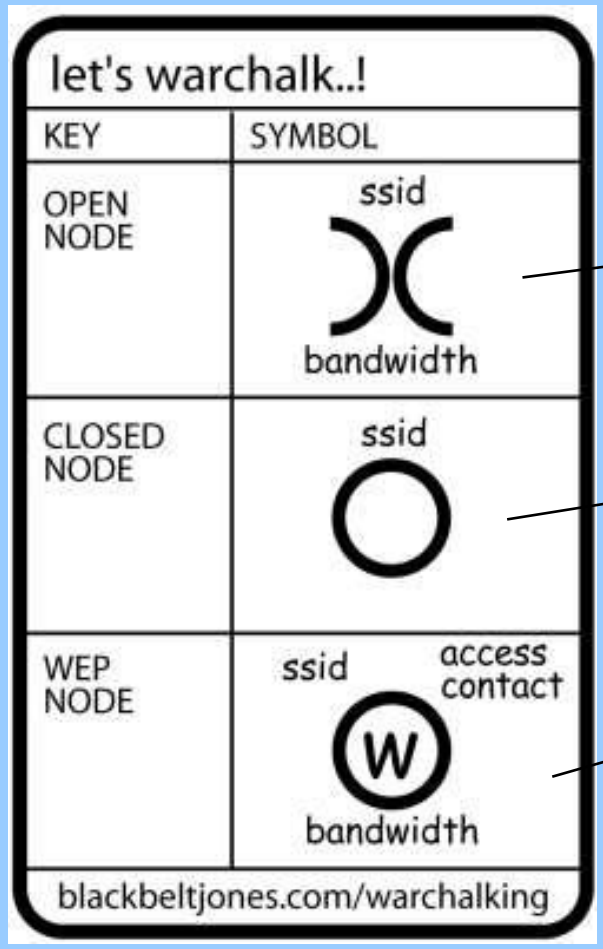

NOWEP
WEP
MOBILE MONZOON
(c) by wardrivin
Oerlikon
Wipkingen
Schwamend
Universität Irchel
Industriequartier Hard
Altstetten
Aussersihl
Fluntern
Wiedikon
Albisrieden
Hottingen
Regensbergstrasse
Hagenholzstrasse
Andreasstrasse
Wallisellenstrasse
Tramstrasse
Hubenstrasse
Batteriestrasse
Vulkanstrasse
Hohlstrasse
Badenerstrasse
Rautistrasse
Fellenbergstrasse
Zollstrasse



Wipkingen
Universität
Irchel
Aargauerstrasse
Vulkanstrasse
Industriequartier
Hard
Aussersihl
Hohlstrasse
Badenerstrasse
Bullingerstrasse
Zollstrasse
Limmatstrasse
Sihlquai
Wasserwerkstrasse
Wehntalerstrasse
Winterthurerstrasse
Hadlaubstrasse
Sonneggstrasse
Freudenbergstrasse
Spitalbachweg
Hubeggstrasse
ZURICH
Militärstrasse
Müllerstrasse
Albisriederstrasse
Letzigraben
Wiedikon
Fellenbergstrasse
Gutstrasse
Aemtlerstrasse
Bertastrasse
Birmensdorferstrasse
Hottingen
Dolderstrasse
Zeltweg
Eth-Zentrum
Fischerweg
Flurstrasse
A1
E41
NOWEP

Spassfraktion: Volkssport Warchalking (I)

- Markieren **von gefundenen Access-Points durch Graffiti**



- Offenes Netz.
  SSID=Netzbezeichnung
  BANDWITH=Bandbreite
- Geschlossenes Netz, Zugriff nicht (ohne Aufwand) möglich
- WEP vorhanden. Zugriff nach Rücksprache mit CONTACT möglich.

Spassfraktion: Volkssport Warchalking (II)

Spassfraktion: Volkssport Warchalking (III)

Opfer Infoscreen Hamburg

Am 05.10.2003


heise
online
www.heise.de
xploited
by
nfoscr3am
TELEPOLIS
wap.heise.de
INFOSCREEN

...war irgendwie...

...alles doch etwas anders...

...als sonst in der U1, U2 und U3

„Jagdrevier“ öffentliche Hotspots

Beispiel DB-Lounges

Der Pragmatiker

- Benötigt gerade einen Internet-Zugang
- Hat keine Lust, Geld für die Benutzung von öffentl. Hotspots zu zahlen oder befindet sich gerade ausserhalb deren Reichweite
- Benutzt deshalb einfach ein gerade vorhandenes WLAN
- Moderne Betriebssysteme unterstützen den Pragmatiker durch die automatische Konfiguration der Wireless-Karte.

Der Kriminelle

- Kriminelle suchen nach einem anonymen Internetzugang, um Straftaten anonym begehen zu können:
  - Versenden von SPAM
  - Freisetzen von Viren und Würmern
  - Down- oder Uploads von Kinderpornos
  - ...
- Besonders unangenehm:
  Die Betreiber der missbrauchten Netze unterliegen einem Anfangsverdacht, werden ggf. für die Machenschaften des ungebetenen Gastes bestraft.

Professionelle Marktteilnehmer

- Industriespionage ist ein Wachstummarkt
- WLANs werden benutzt, um an vertrauliche Daten zu gelangen.
  - WLANs werden i.d.R. zur Vernetzung von Computern des Produktivnetzes verwendet: Angreifer können via WLAN hinderliche Sicherheitseinrichtungen (Firewall, IDS, Anti-Viren-System...) umgehen und so unbemerkt in das interne Netz eindringen.
  - WLANs transportieren vertrauliche Informationen wie (Geschäfts-) Dokumente, Passwörter, Benutzernamen, E-Mails, Druckaufträge etc., an die man durch einfaches Abhören gelangen kann.

Unser Szenario

Mobiler Client

Access-Point **Server**

Eindringling

Wir brauchen gesicherte Verbindungen!

- **Vertraulichkeit**

  Die ausgetauschten Daten dürfen keinen Fremden in die Hände fallen (Auch nicht denen mit den Richtfunkantennen!).

- **Authentizität**

  Ich muss genau wissen, mit wem ich kommuniziere - es dürfen sich keine Fremden in das Wireless LAN einbuchen können.

- **Integrität**

  Wenn Pakete auf dem Weg zum Empfänger verändert werden, so muss ich das eindeutig feststellen können.

Wie sichert man WLANs ab?

- Basisschutzmassnahmen
- MAC-Filterlisten
- WEP-Verschlüsselung
- WPA (WiFi Protected Access)
- WPA II (IEEE 802.11i)
- VPNs

Basisschutz: Accesspoints

- Standardpasswort bei Inbetriebnahme ändern
- Administrationszugang nur bestimmten Maschinen erlauben *)
- Wartungszugänge (wie z.B. SNMP) möglichst abschalten *)
- Ggf. Portscan durchführen, um offene Ports zu finden (nützliche Programme: Superscan und nmap)

*) falls technisch möglich (Kaufkriterium!)

Basisschutz: Netzparameter

- Antennen so ausrichten, dass nur der gewünschte Bereich funktechnisch ausgeleuchtet ist *)
- Ggf. Sendeleistung der Accesspoints verringern *)

*) falls technisch möglich (Kaufkriterium!)

Basisschutz: ESSID

- Broadcasting der ESSID (Name des WLANs) abschalten *)
- Neutrale ESSID wählen

*) falls technisch möglich (Kaufkriterium!)

Basisschutz: Blackout

- Wireless LAN abschalten, wenn es nicht benutzt wird (z.B. wenn in der Nacht und an Feiertagen niemand im Büro ist).

MAC-Filterlisten

- **Funktionsweise:**

  Jede Netzwerkkarte verfügt über eine (theoretisch) einmalige Adresse (MAC-Adresse), die Pakete werden auf Basis der MAC-Adressen gefiltert.
- **Schwacher Schutz:**

  MAC-Adressen können sehr einfach mitgehört und gefälscht werden.
- **Problem:**

  Die Verwaltung der zugelassenen MAC-Adressen kann sehr aufwendig werden (Benutzer kommen und gehen, Karten werden gewechselt, Gäste wollen das Netz benutzen).

WPS

- **Funktionsweise:**
  - PIN-Eingabe
  - Push Button Configuration (PBC)
  - USB Flash Drive (UFD)
  - Near Field Communication (NFC)
- **Problem:**
  - PIN-Methode innert Sekunden geknackt
  - WPS nach Gebrauch deaktivieren!

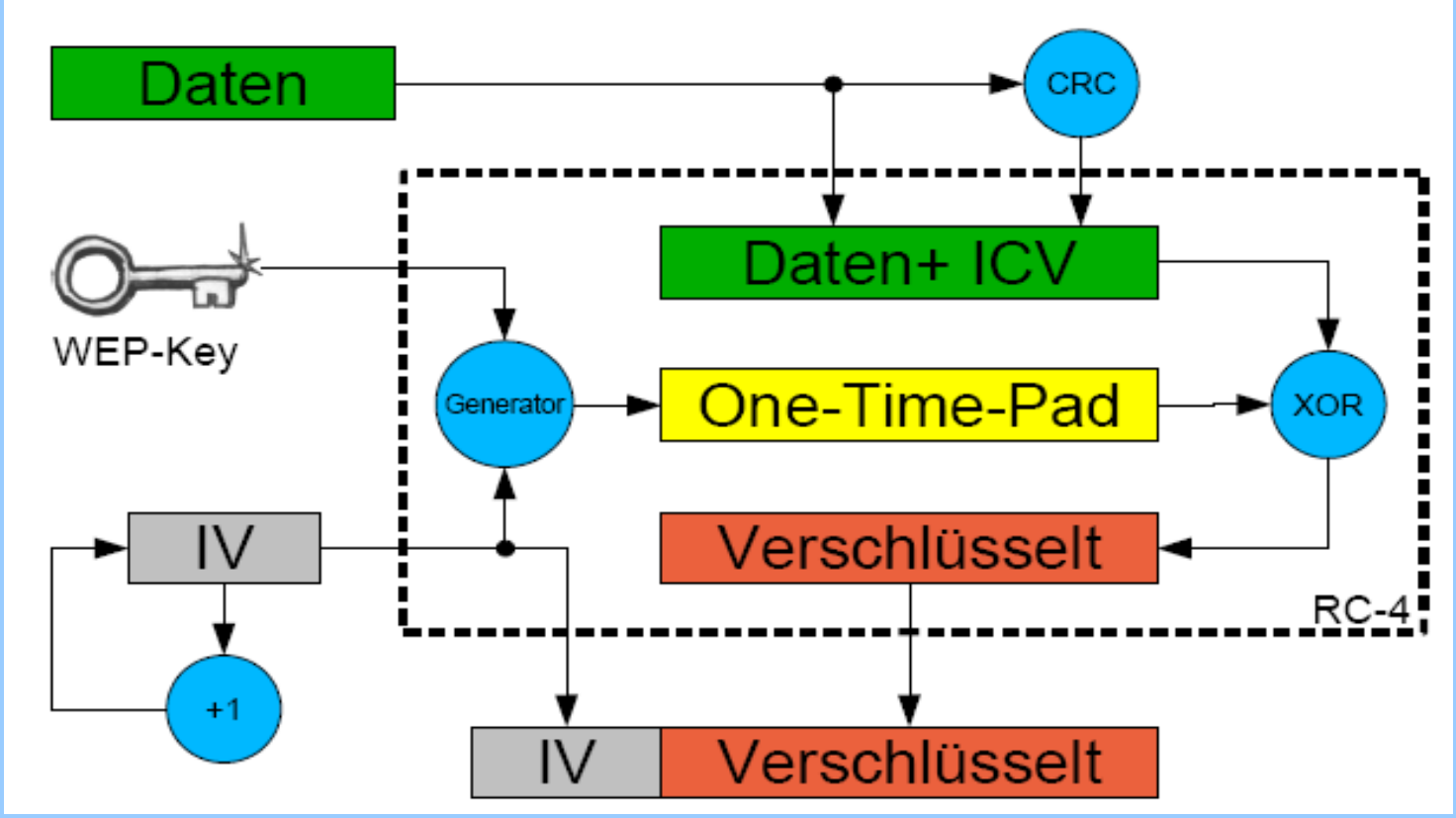
WEP (Wired Equivalent Privacy)

- Teil des Standards IEEE 802.11 aus dem Jahr 1997
- Wurde aufgrund der US-Exportbestimmungen geschwächt.
- Ist seit August 2001 komplett gebrochen und harrt seiner Ablösung.

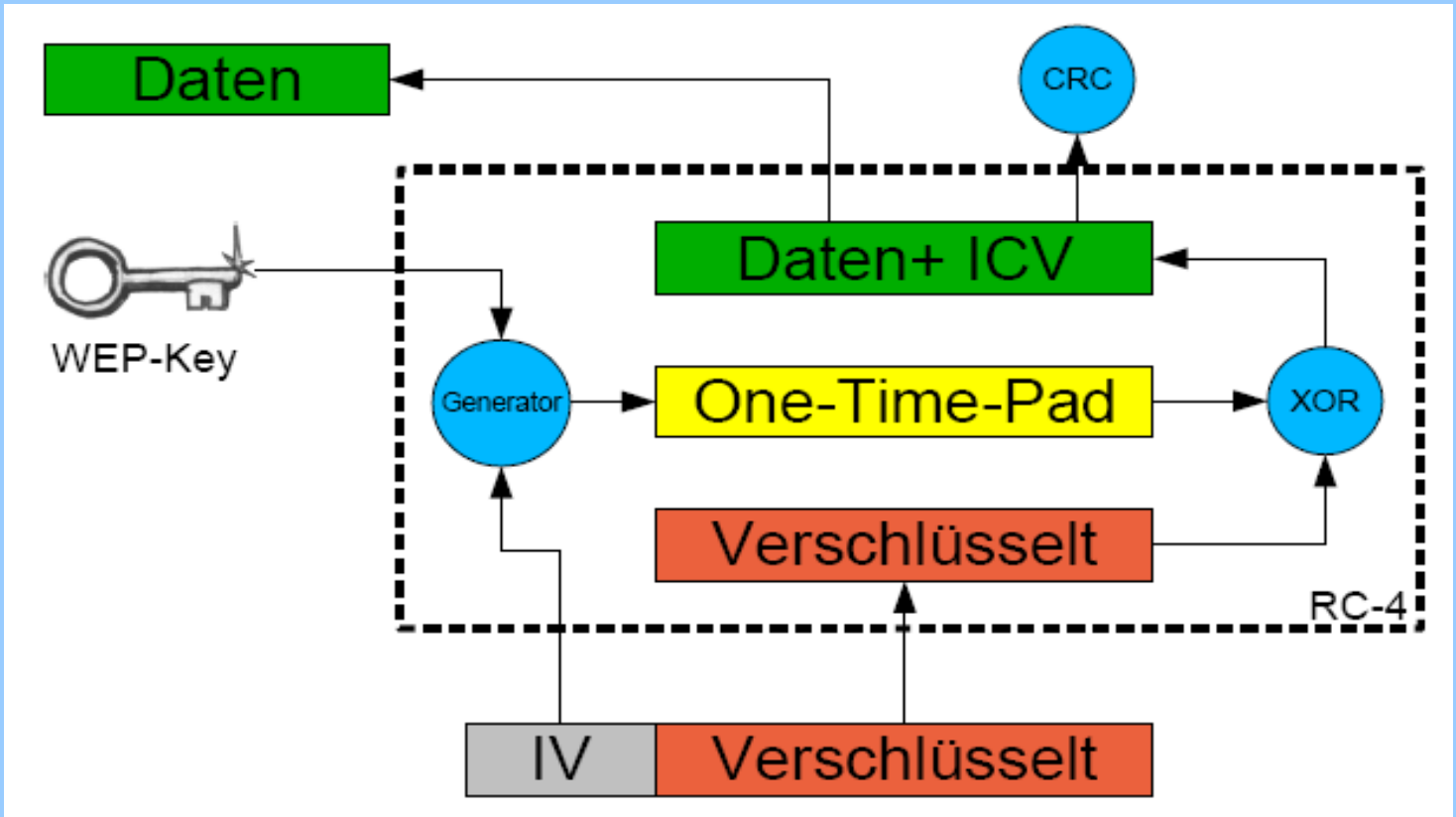
****

- ...ist ein absoluter Alptraum!
- Beim Design wurde alles – wirklich ALLES! – falsch gemacht, was falsch gemacht werden konnte.

Verschlüsselung eines Pakets via WEP



Verschlüsselung eines Pakets via WEP



Was fehlt WEP?

- Schlüsselmanagement...
- Adäquater dynamischer Anteil...
- Ein guter Verschlüsselungsalgorithmus...
- Eine ausreichend hohe Schlüssellänge...
- ...und vieles, vieles mehr.

WEP: praxisferne Authentifizierung

- Die Teilnehmer authentifizieren sich durch den WEP-Key: Sind die Pakete richtig verschlüsselt, so dürfen sie am WLAN teilnehmen.
- Jeder Teilnehmer verfügt über den gleichen Schlüssel.
- In der Praxis ist das Wechseln der Schlüssel so gut wie unmöglich.
- Die Schlüssel werden an unsicheren Orten aufbewahrt (Konfigurationsdateien bzw. Windows-Registry bzw. EPROM des Accesspoints).

Problem: Schlüssellänge

- 24 Bit des Schlüssels werden im Klartext übertragen
  - 64-Bit Key: Marketing Spam für 40-Bit Key
  - 128-Bit Key: Marketing-Spam für 104-Bit Key
- 40-Bit Key: via Brute-Force leicht zu knacken
  - Ein Kollege: “Easy going in wenigen Stunden!”
- 104-Bit Key: keine Chance für Brute-Force
- 104-Bit Key: kein WEP-Standard, Kompatibilitätsprobleme

Problem: statischer Schlüssel

- Das One-Time-Pad (der Schlüsselstrom) wird durch den Generator erzeugt, der mit dem statischen WEP-Schlüssel und dem dynamischen Initialisierungsvektor (IV) initialisiert wird.
- Jedes One-Time-Pad sollte (wie der Name schon sagt) nur ein einziges mal zur Verschlüsselung eingesetzt werden – die Wiederverwendung von One-Time-Pads eröffnet die Möglichkeit eines statistischen Angriffs.
- Da der IV nur 24 Bit gross ist, wird nach spätestens 224 Paketen wird der gleiche Schlüsselstrom wiederverwendet (also nach max. 24 GB Daten).

Das Waterloo für WEP: RC4

- RC4: Nimmt einen Schlüssel entgegen und erzeugt einen (beliebig langen) Schlüsselstrom.
- Vereinfacht ausgedrückt: Abhängig vom Schlüssel vertauscht RC4 jeweils zwei Einträge einer Tabelle und verwendet einen Eintrag der Tabelle als Schlüsselzeichen.
- Die “Unordnung” in der Tabelle nimmt mit jedem generierten Schlüsselzeichen zu.
- Das bedeutet aber: Die Anfänge des Schlüsselstroms werden von einer noch relativ geordneten Tabelle erzeugt.
- Bei einigen Schlüsseln (sogenannten Weak Keys) erlauben deshalb die ersten Bytes des Schlüsselstromes Rückschlüsse auf den Schlüssel.

Von der Theorie zur Praxis...

- **Ende Juli / Anfang August 2001:**

  Es wird eine Schäche im RC4-Algorithmus entdeckt und ein theoretischer Angriff gegen WEP beschrieben.

- **Anfang August 2001:**

  Unter Testbedingungen wird der Angriff erstmals erfolgreich durchgeführt.

- **Ende August 2001:**

  Die Software Airsnort wird von Hackern veröffentlicht. Der Angriff kann nun von jedem durchgeführt werden.

- **Stand heute:**

  Die Angriffe sind seit 2001 verfeinert und stark beschleunigt worden. Empfehlenswert: WepAttack und Aircrack.

~~WEP =~~
~~"Wired Equivalent Privacy"~~

WEP =
"Wireless Equivalent Placebo"

http://airsnort.shmoo.com

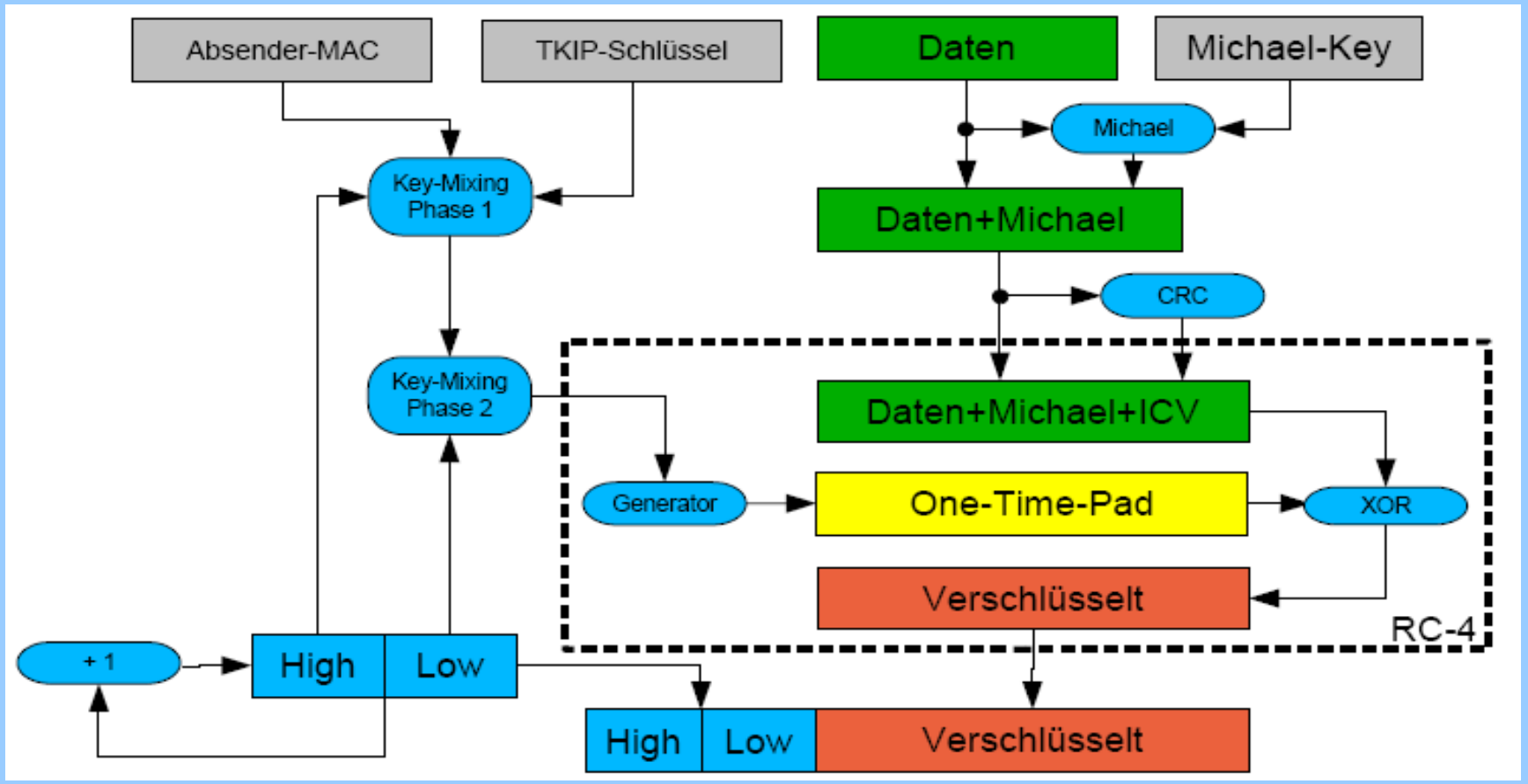
Das Leben nach WEP: WPA und WPA II

- Als Nachfolgerstandard von WEP ist 802.11i Mitte 2004 verabschiedet worden. Geräte, die diesen Standard einhalten, sind günstig zu bekommen.
- Bereits Mitte 2003 wurde eine Teilmenge des Standards 802.11i von der WiFi-Alliance als Interimslösung unter dem Namen WPA (WiFi Protected Access) verabschiedet.
- 802.11i wird deshalb auch als WPA2 bezeichnet.

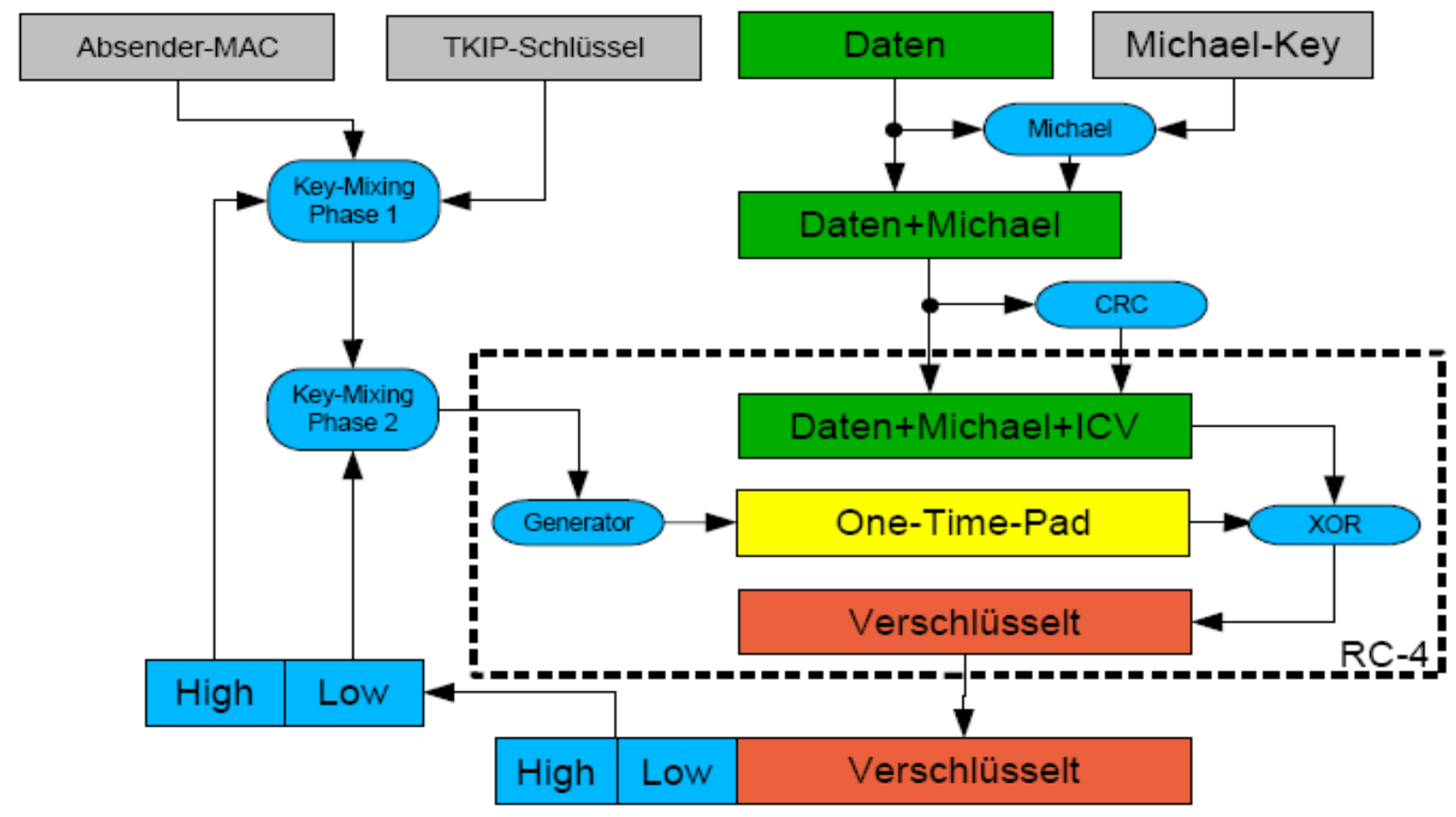
WPA in der (Kurz-)Übersicht

- WPA setzt noch immer den RC4-Algorithmus ein und ähnelt WEP.
- Die Schlüssel, mit denen der Schlüsselstrom erzeugt werden, werden jedoch immer wieder neu zwischen Acesspoint und Client ausgehandelt (TKIP-Algorithmus) und damit die Schwächen von WEP ausgeräumt.
- WPA gibt die Möglichkeit, Benutzer via 802.1x bei deren Anmeldung am Netz zu authentifizieren (Enterprise-Mode).
- Pakete werden bei WPA mit einer kryptographischen Checksumme (Michael-Algorithmus) versehen, um die Authentizität der Packete sicher zu stellen.
- WPA gilt – wenn gut konfiguriert – als sicher.

Verschlüsselung eines Pakets via WPA



Entschlüsselung eines Pakets via WPA



802.11i (WPA II) in der (Kurz-)Übersicht

- 802.11i (alias WPA II) beinhaltet den Standard WPA.
- 802.11i basiert jedoch auf dem Verschlüsselungsstandard AES (AES=Advanced Encryption Standard).
- 802.11i gilt – wenn gut konfiguriert – als sicher.

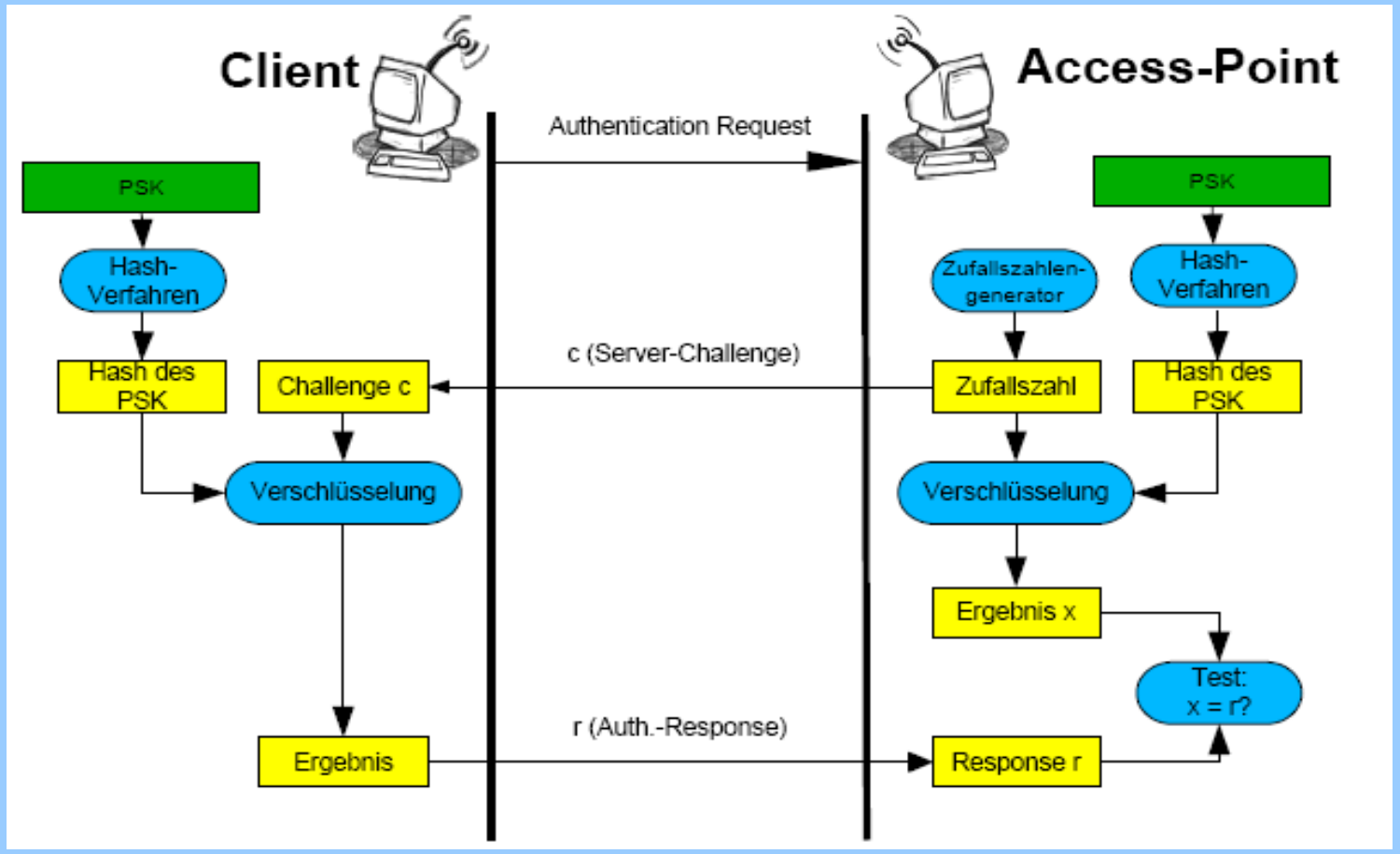
WPA I + II: die Authentifizierung (Teil I)

- WPA kann im sogenannten Consumer Mode (auch WPA-PSK genannt) betrieben werden.
- Hier authentifizieren sich – genau wie bei WEP - alle Stationen mit dem gleichen Passwort (auch Preshared Key oder kurz PSK genannt) am Netz.
- Die Authentifizierung der Stationen geschieht bei deren Einbuchen in das Netz.
- Hier kommt ein Challenge-Response-Verfahren zum Einsatz.

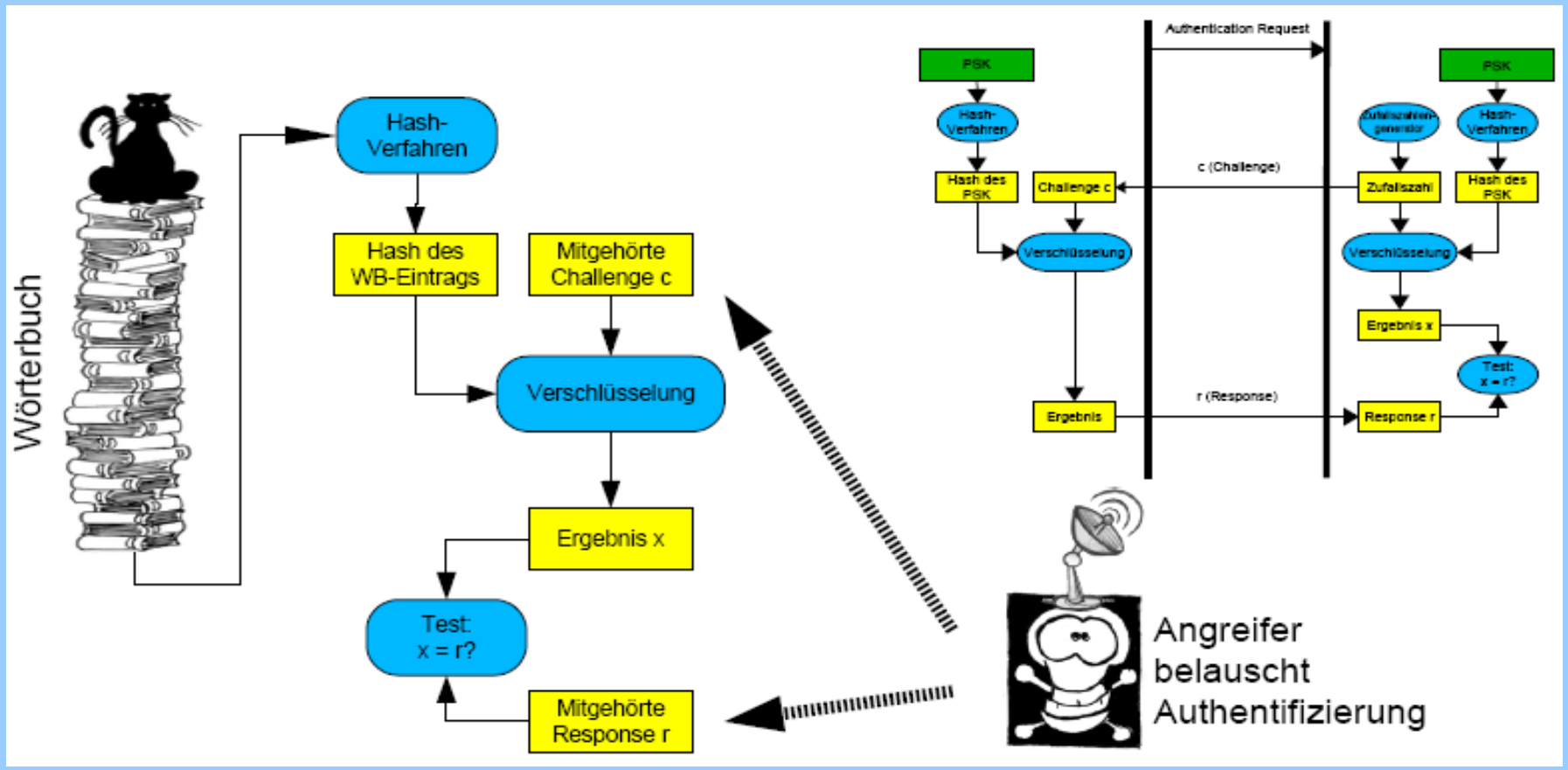
PSK Challenge-Response Authentifizierung (I)

- Für jede Authentifizierung generiert der Server eine eigene Zufallszahl (Challenge) und sendet diese an den Client.
- Der Client verschlüsselt die Challenge mit dem PSK und sendet das Ergebnis (Response) an den Server.
- Der Server verschlüsselt seinerseits die Challenge mit dem bei ihm gespeicherten PSK und vergleicht sein Ergebnis mit der Antwort des Clients.
- Sind die Ergebnisse von Client und Server identisch, so ist sicher gestellt, dass die PSKs auf beiden Seiten identisch sind, in diesem Fall ist der Client authentifiziert.

PSK Challenge-Response Authentifizierung (II)



Wörterbuch-Angriff auf CR-Authentifizierungen



WPA I + II: die Authentifizierung (Teil II)

- Im Enterprise-Mode von WPA I und II wird jeder Benutzer individuell authentifiziert.
- Auf den Wireless-Clients ist eine Software installiert, die über den Access-Point mit einem zentralen Server kommuniziert (z.B. einem RADIUS-Server) und dort den Benutzer authentifiziert.
- Problem: WPA sieht keine sichere Authentifizierungsart vor, sondern stellt nur ein Verfahren zur Verfügung, über das eine beliebige Authentifizierung durchgeführt werden kann.
- Heute bedeutet dies i.d.R. eine Authentifizierung via Username und Passwort der Windows-Domain des Benutzers...

WEP – WPA – IEEE 802.11i (WPA II)

Features	*WEP*	*WPA*	*IEEE 802.11i (WPA II)*
Verschlüsselungs-Algorithmus	RC4	RC4	AES
Schlüssellänge	**40** oder 104bit	128bit Verschlüsselung 64bit Authentisierung	128bit
Initialisierungsvektor			
- Länge	**24bit**	48bit	48bit
- Generierung	Inkrement o. Zufall	Key-Mixing-Verfahren	Nicht mehr notwendig
Integritätsüberprüfung			
- Daten	**CRC-32**	**Michael**	AES-CCM
- Packet-Header	**Nicht vorhanden**	**Michael**	AES-CCM
Schlüssel-Management	**Nicht vorhanden**	EAP	EAP
Packet-Authentisierung	**MAC-Adresse**	**Michael**	AES-CCM
Stations-Authentisierung	**PSK (WEP-Key)**	**Passwort mit mind. 8 Zeichen (Consumer-Mode)**	**Passwort mit mind. 8 Zeichen (Consumer Mode)**
Benutzer-Authentisierung	**keine**	Flexibel via EAP (Enterprise-Mode)	Flexibel via EAP (Enterprise-Mode)

Antennen

- Indoor / Outdoor

- Geräte interne Antennen
- Rundstrahlantennen / Stabantennen
- Deckenantennen
- Sektorantennen
- Richtfunkantennen
- Magnetfuss-Antennen

Zusammenfassung

- Wer ungesicherte Wireless LAN Netzwerke betreibt, handelt – auch im privaten Umfeld! – absolut leichtsinnig.
- WEP ist tot! Es sollte auch im privaten Umfeld nicht mehr eingesetzt werden. Accesspoints mit WPA sind heute verfügbar!
- Wenn kritische Daten über Wireless LAN transportiert werden, sollte WPA bzw. WPA II im Enterprise-Mode betrieben werden (Authentifizierung der Benutzer via 802.1x) oder auf den Einsatz von Wireless LAN grundsätzlich verzichtet werden.
- Das ungeschützte Arbeiten mit öffentlichen HotSpots ist absolut leichtsinnig! Hier gilt: Ohne VPN (SSL oder IPSec) läuft nichts!

Danke

- Sind noch Fragen ???