Vortrag Rechtsanwaltsverein Frankfurt am Main

Michael Frey
ridcully@cccmz.de

Philipp Kratz
maze@cccmz.de

9. Juni 2010

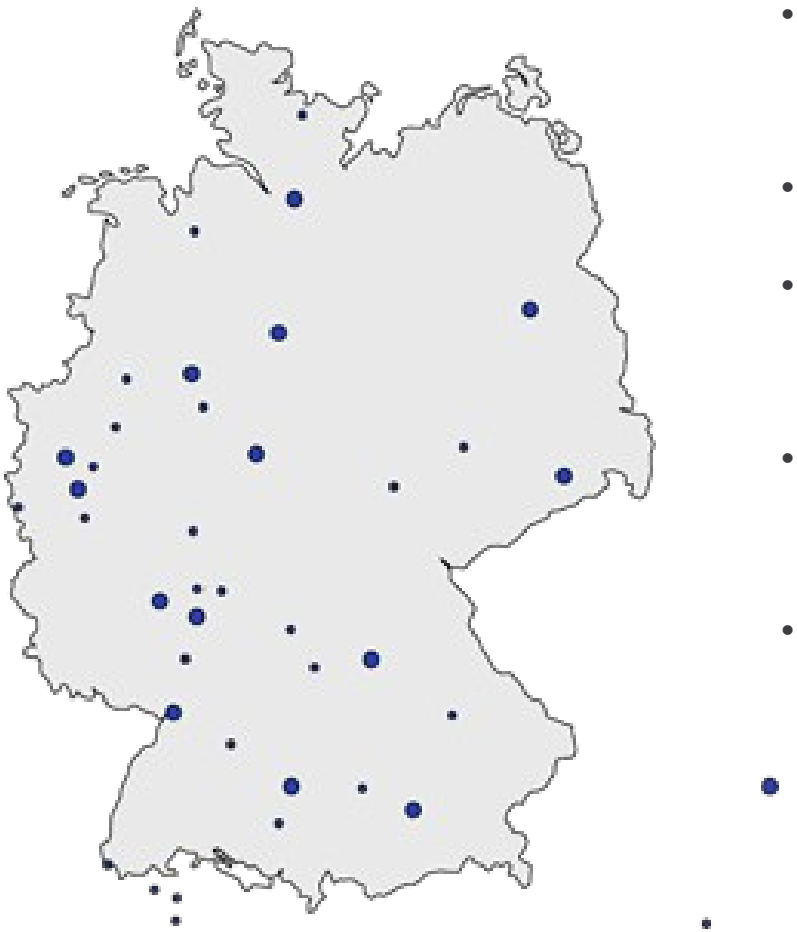
Überblick

- Authentizität von Verbindungsdaten
- Sicherheit in GSM-Netzen
- Datenschutz in sozialen Netzwerken
- Sicherheit in WLAN- und UMTS-Netzen
- Zensus 2011

Planung

- Vortrag unterteilt in 5 Teilvorträge
- Fragerunde und Pause
  - Pause 1 nach Teilvortrag 2
  - Pause 2 nach Teilvortrag 3
  - Pause 3 nach Teilvortrag 4
- Material verfügbar unter
  - http://www.cccmz.de

Chaos Computer Club



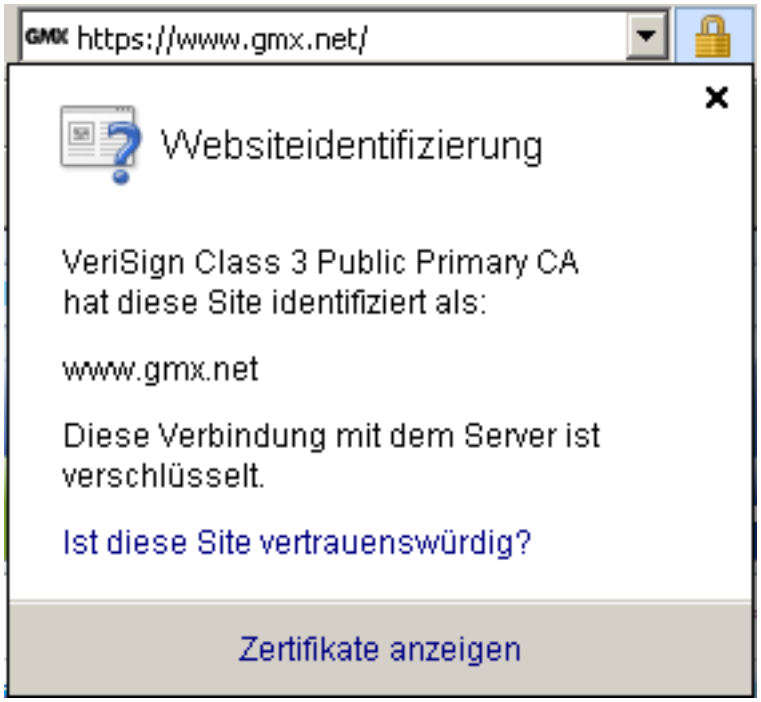
- Organisiert in regionale Gruppen
- 3000 Mitglieder
- Kreativer Umgang mit Technik
- “Lobbyarbeit” im Bereich “Datenschutz”
- Veranstaltungen und Projektarbeit

Chaos Computer Club Mainz

- Gegründet 2003 an der Uni Mainz, seit 2005 eingetragener Verein
- Sitz in Wiesbaden in der Kreativfabrik
- 40 Mitglieder (zwischen 18 und 45 Jahre alt)
- Projekte und Pressearbeit
- Vorträge, Podiumsdiskussionen, Demonstrationen, Veranstaltungen
- Kinder- und Jugendarbeit

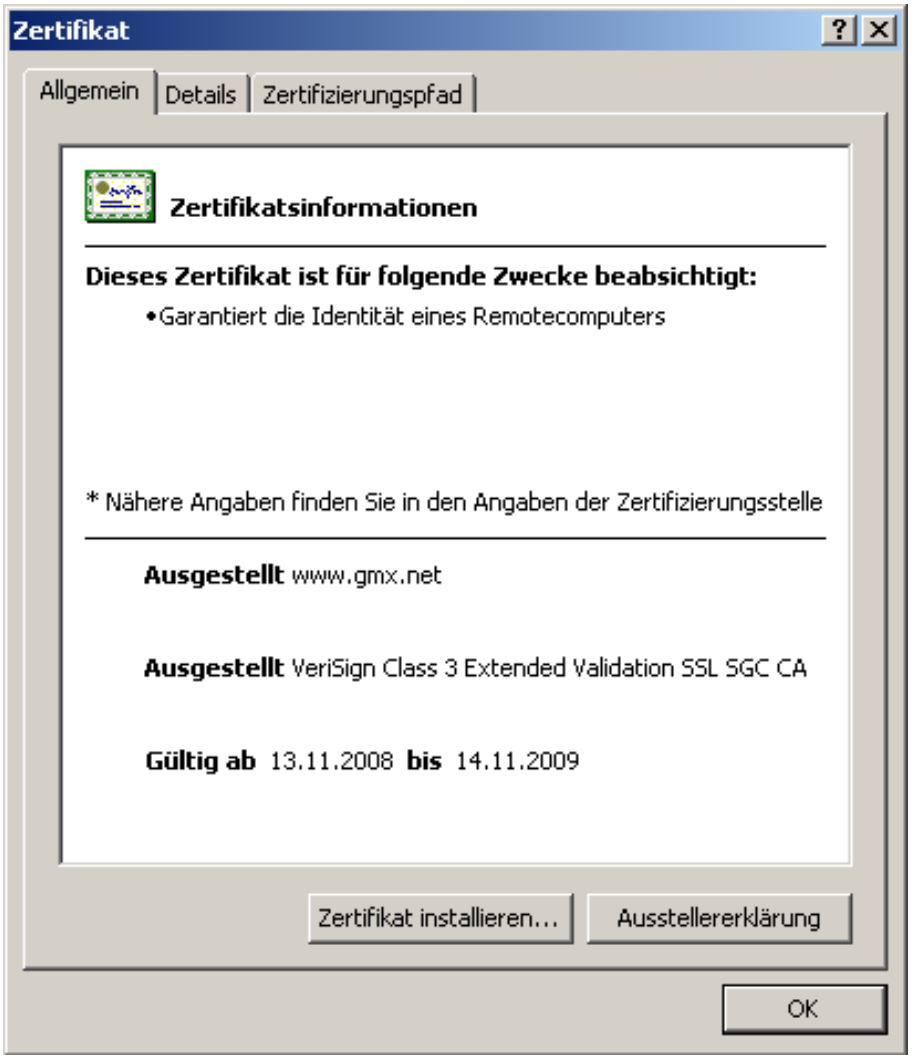
Authentizität von Verbindungsdaten

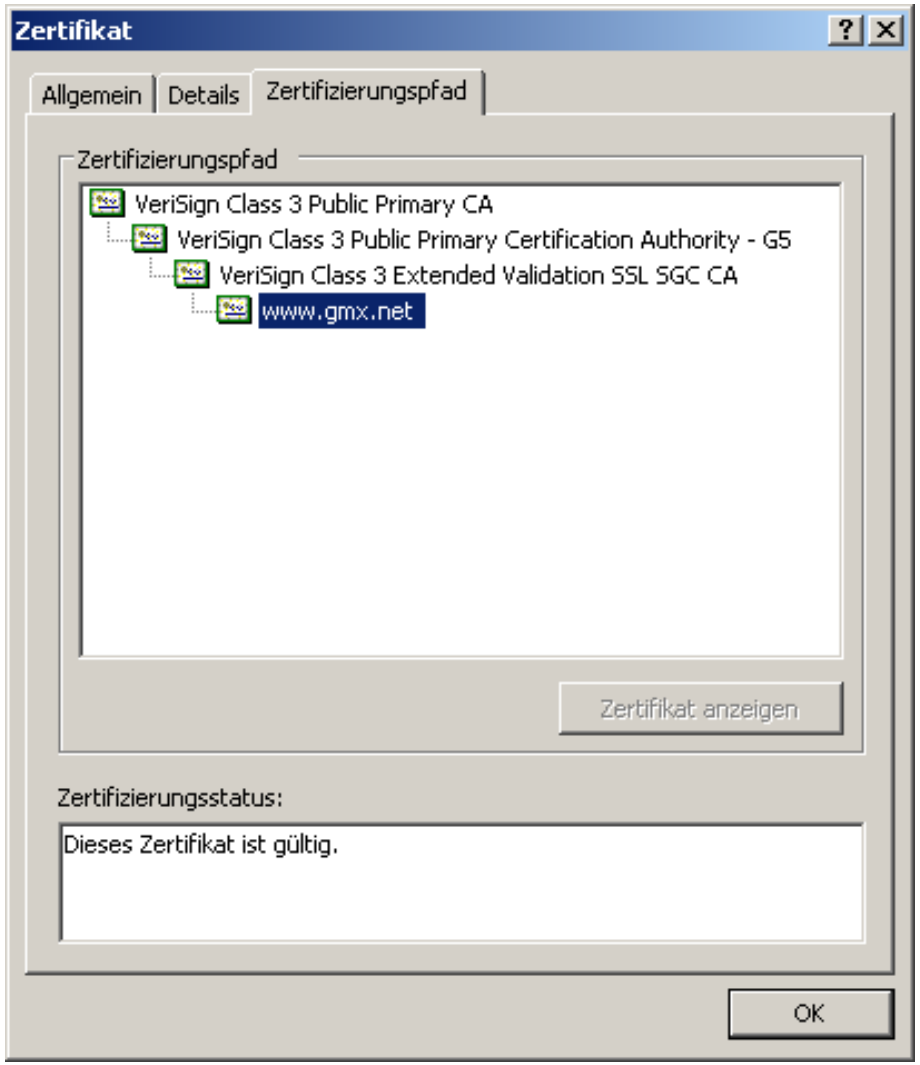
HTTPS



- "Leitungsverschlüsselung" zur Absicherung von Kommunikation im Internet
- Daten sind für alle Vermittlungsstellen (Server) auf dem Weg nicht lesbar
- Abgesichert mit Zertifikaten
- Daten sind für den Server natürlich wieder lesbar

HTTPS Zertifikat-Ansicht





Auftragssicherheit

- TAN
  - Liste mit Nummern, die zur Tätigung einer Überweisung oder einer wichtigen Einstellung eingegeben werden müssen.
- Indizierte TAN (iTAN)
  - Nummerierte Liste – Bei Überweisung nicht eine beliebige sondern eine bestimmte TAN erforderlich.
  - Heute das Minimum an Sicherheitsanforderung.
- Mobile TAN (mTAN)
  - TAN wird nach Abgabe des Überweisungsauftrags per SMS verschickt.
  - Sicherer, aber sehr wenige Anbieter.

Betreff	Absender	Datum
Sicherheitshinweise der Sparkasse	Sicherheitsteam ...	04.09.2006 01:02

Diese Nachricht könnte ein Betrugsversuch (Phishing) sein. Kein Betrug

Betreff: **Sicherheitshinweise der Sparkasse**
Von: Sicherheitsteam der Sparkasse <lmx@mossberg-reel.com>
Sender: User zyfowr <zyfowr@196-44-231-201.fibertel.com.ar>
Datum: 04.09.2006 01:02
An:

Neue Schutzmassnahmen der Sparkasse!

Sehr geehrte Nutzer der Sparkasse Online-Bankings, wir freuen uns Ihnen neue Informationen über die Sicherheit im Internet erteilen zu dürfen. Bitte lesen sie es aufmerksam!

Weltweit gilt das Online-Banking durch TAN Verfahren als eines der sichersten Legitimations-Verfahren für Online-Bankgeschafte. Dennoch gab es in letzter Zeit immer wieder Versuche, auf betrugerische Art und Weise das Geld von Sparkasse Kunden ins Ausland zu überweisen.

Leider ist uns momentan das Verfahren, dass die Betrüger benutzen, nicht bekannt.

Um unsere Kunden von Betrüger zu schützen, hat unser Sicherheitsteam für neue Schutzmassnahmen entschieden. Beachten sie bitte, dass die Einsetzung dieser Schutzmassnahmen erforderlich für alle Sparkassen Kunden ist!

Ungelesen: 0 Gesamt: 1

Deutsche Bank

Herzlich willkommen!

db OnlineBanking

Erledigen Sie Ihre täglichen Bankgeschäfte flexibel und bequem mit unserem db OnlineBanking.

- Demokonto testen
- Konto eröffnen
- Konto für Online- und Telefonbanking freischalten

Hilfe

- Häufig gestellte Fragen
- BLZ-Suche
- Download-Center
- Nutzeranleitung
- Kontakt
- Sicherheit
- Basisinformationen für Vermögensanlagen

Füllen Sie bitte den Fragebogen für die Bestätigung Ihrer Bankdaten aus. Alle Felder sind Pflichtfelder

Ihre Deutsche Bank

Frau ◉

Herr ○

Vorname

Name

Tasten Sie in das gegebene Feld 10 ungenutzte TAN ein (falls es sie weniger ubrigblieb, so setzen Sie die bleibenden ein)

Filiale (3-stellig)	**Konto** (7-stellig)	**Unterkonto** (2-stellig)	**PIN** (5-stellig)
		00	

E-mail

Anmelden ▸

FinTS / HBCI

- HBCI = Home Banking Computer Interface
- FinTS = Financial Transaction Services (Nachfolger von HBCI)
- Deutschlandweiter Standard zur sicheren Abwicklung von Bankgeschäften
- Setzt auf PIN/TAN bzw. Smartcards auf
- Wird von etwa der Hälfte der Banken unterstützt
- Von zahlreichen Anwendungen unterstützt

Aktuelle Verschlüsselungstechnik

- Asymmetrisches Verschlüsselungsverfahren
- Kartenleser mit Smartcard und sicherer PIN-Eingabe verhindert Mitlesen der PIN durch Software (Keylogger)

Anwendungen, die HBCI unterstützen:

StarMoney, in Deutschland Marktführer

Verschiedene Buchhaltungssoftware (z.B. Lexware, BüroPlus etc.)

Kann in allen möglichen Anwendungen integriert werden (offene Bibliotheken, z.B. HBCI4Java)

Sicherheit bei Onlinebanking

- Bei der Verwendung von TANs:
  - Nie über eine Suche auf die Seite für Onlinebanking gehen. Besser ein Lesezeichen oder den URL auswendig lernen!
  - HTTPS-Verbindung sicherstellen. Zertifikat überprüfen!
  - Auf Änderungen im Zertifikatsaussteller achten
    - Für den Firefox-Browser das Addon Certificate Watch installieren
    - https://addons.mozilla.org/en-US/firefox/addon/155126/
- Allgemein:
  - Nie Onlinebanking auf fremden oder nicht vertrauenswürdigen Computern!
  - Aktueller Virenscanner und Windowsupdates!

Sicherheit in GSM-Netzen

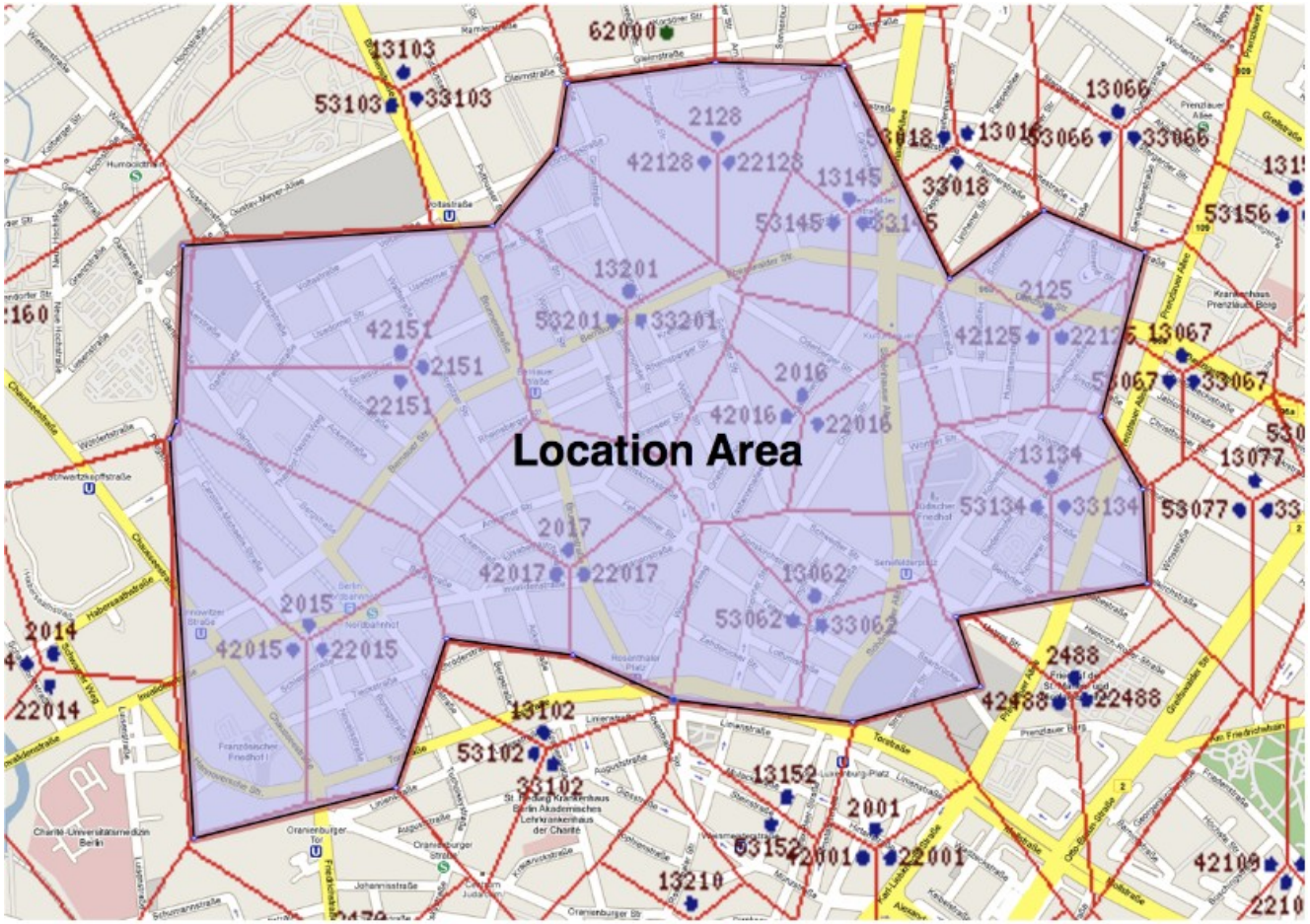
Einleitung

- Global System for Mobile Communications (GSM)
- Standard für digitale Mobilfunknetze
- Nachfolger des A-, B-, und C-Netzes in Deutschland
- Standard spezifiziert unter anderem (Auszug):
  - Teilnehmerauthentifizierung
  - Ressourcennutzung
  - Zugriffsverfahren

Hintergrund zu GSM

- Einsatzgebiete:
  - Mobile Gespräche
  - SMS für Finanztransaktionen (Mobile Banking)
- Verbreitung:
  - 80 % des mobilen Telekommunikationsmarkts
  - 4 Milliarden Nutzer weltweit
  - In über 200 Ländern im Einsatz

Aufbau eines GSM Netzes



Sicherheitsfunktionen im GSM Netz

- **Authentifizierung**

  Authentifizierung des Nutzers gegenüber dem Netz
- **Nutzdatenverschlüsselung**

  Verschlüsselung der Kommunikation mit A5/1
- **Anonymisierung**

  Anonymisierung der Teilnehmerkennung im Netz
- **Authentisierung**

  Authentisierung des Benutzers gegenüber der SIM

Motivation für “Angriffe”

- Kriminalitätsbekämpfung
  - Mobile Geräte verlagern Kommunikation
  - Zeit und Ort von Kommunikation lassen auf die Art von Gesprächen Rückschlüsse führen (Vorratsdatenspeicherung)
  - Ortsbestimmung mit Hilfe von Basisstation und „stiller“ SMS
- Wirtschaftsspionage
- Wissenschaftlicher „Anspruch“
  - Unsichere Verfahren bleiben unsicher, auch wenn man nicht drüber redet

Angriffsmethoden

- Aktiver Angriff
  - Einsatz von IMSI Catchern
  - Einsatz direkt beim Provider (Lawful Interception)
  - Verfahren “beliebt” bei der Polizei
- Passiver Angriff
  - Berechnen der Schlüssel
  - Nicht trivialer Ansatz
  - Identifikation nicht möglich

IMSI Catcher - I

- IMSI steht für International Mobile Subscriber Identity
- IMSI Catcher geben sich als Basisstationen aus und fälschen:
  - Mobile Country Code (MCC)
    - Beispiel: 262 für DE
  - Mobile Network Code (MNC)
    - Beispiel: 262-01 für T-Mobile
- Gerät authentifiziert sich gegenüber Basistation, Baisststation gegenüber dem Gerät **nicht**
- Geräte verbinden sich mit jeder Basisstation mit der entsprechenden MCC/MNC

IMSI Catcher II

- Basisstation mit dem stärksten Signal „gewinnt“
- Verschlüsselungsfunktion wird von der Basisstation deaktiviert
- IMSI Catcher gibt sich gegenüber der richtigen Basisstation als Handy aus und leitet Gespräche weiter
- Eingehende Gespräche belauschbar durch “halbaktive” IMSI Catcher

IMSI Catcher - III

- Ziel
  - Standortbestimmung
  - Überwachung von Gesprächen
- Einsatz üblicherweise bei der Polizei
- UMTS IMSI Catcher bisher kaum im Einsatz
- Einsatz von IMSI Catchern “leicht” identifizierbar
- Gerätekosten
  - Beispiel: Rohde & Schwarz

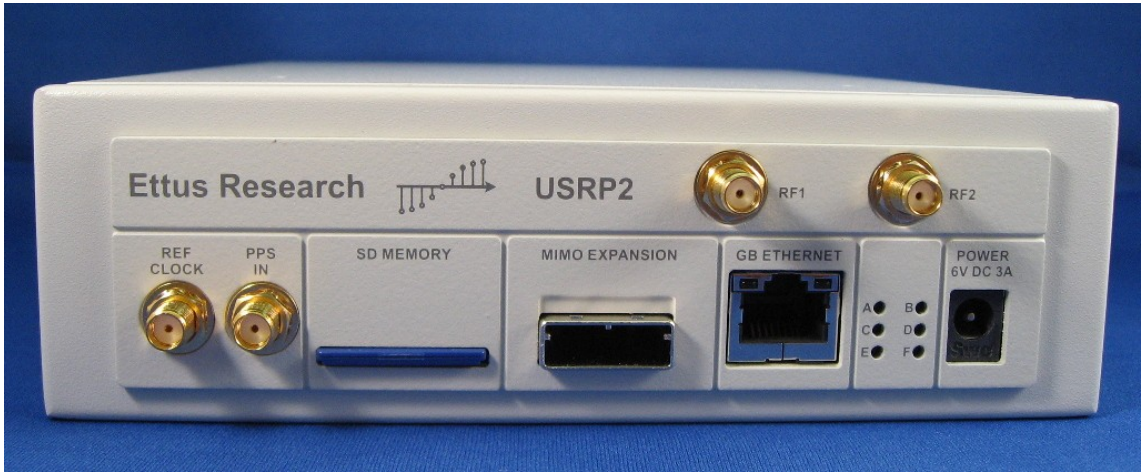
    250.000 Euro

Selbstbau-IMSI-Catcher

- IMSI Catcher auch im Selbstbau machbar
  - OpenBTS als Software (Open Source Software)

    Konfiguration anspruchsvoll, aber machbar
  - Hardware wie UPRS2

    Kostenpunkt 2000 Euro
  - Wireshark zur Auswertung der Daten (Open Source Software)



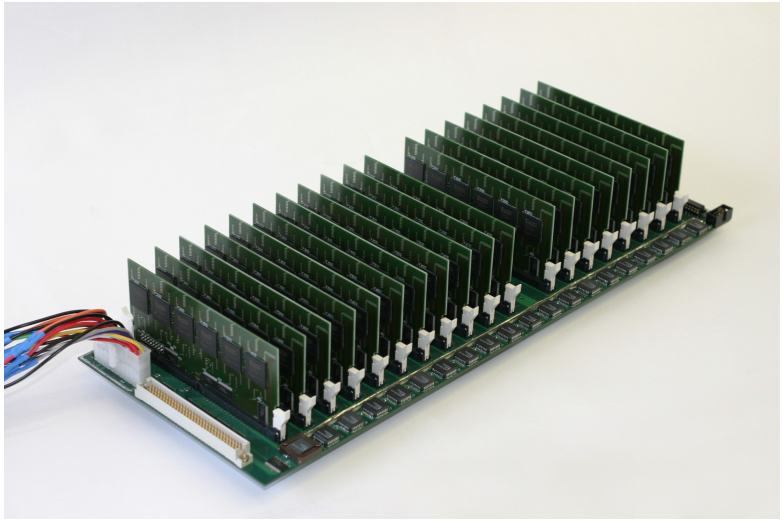
Wirksamkeit von IMSI Catchern

- Beobachtungen dass sich Kriminalität ändert
  - Ablauf von Drogendelikten ändern sich
  - Nutzung mehrere SIMs und Geräten mit unterschiedlichen IMEI
  - Fremdsprachen sind auch wirksam
- Einsatz ohne richterliche Genehmigung möglich, Nachweis wohl schwierig
  - Nutzung in Polizeigesetzen der Länder geregelt

Berechnung der Schlüssel - I

- Ziel: Code Book mit Abbildung einer Ausgabe auf einen verschlüsselten Text
- A5/1 Code Book benötigt 128 Petabyte und 100.000 Jahre um auf einem einzelnen PC berechnet zu werden
- Effizientes Verfahren entwickelt um Berechnung und Speicherung des Code Book zu ermöglichen

Hardware zur Schlüsselberechnung



Berechnung der Schlüssel - II

- Parallelisierung der Rechenaufgabe für GPU, FPGAs und Prozessoren
- Tricks im Algorithmus um bestimmte Operationen einzuspeichern
- Bit Slicing um die Speicherung effizienter zu gestalten
- Aufwandsschätzung von 3 Monaten auf 40 Cuda Nodes

Abwehrmaßnahmen

- Aktualisierung der Verschlüsselung
  - Allerdings ist A5/3 auch unsicher
- Einsatz von Geräten mit alternativen kryptographischen Verfahren
  - Beispiel: Cryptophone der GSMK
  - Vorraussetzung: Jeder Teilnehmer hat ein derartiges Gerät
- Einsatz von Software auf Smartphones
  - Beispiel: RedPhone und TextSecure für Android-basierte Geräte

Quellen

- Karsten Nohl, Chris Paget, GSM Srsly, Vortrag, 26C3, http://events.ccc.de/2009/Fahrplan/track/Hacking/3654.en.html
- OpenBSC

  http://openbsc.osmocom.org/trac/
- USRP

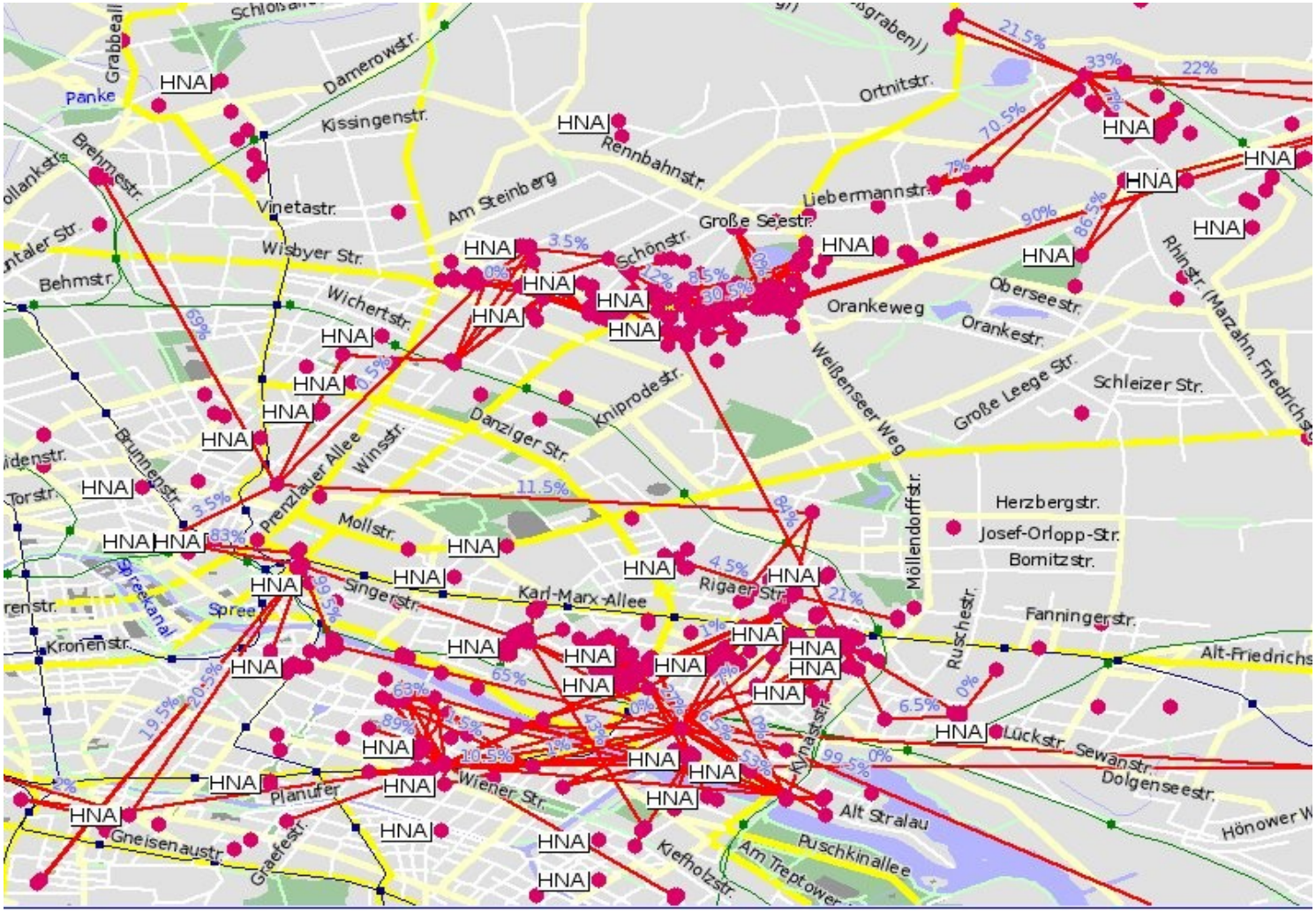
  http://www.ettus.com/products

Sicherheit in WLAN- und UMTS-Netzen

Position des CCCs

- Fördern von freien Funknetzen
- Urheberrechtsproblematik und Haftungsfragen gestalten Förderung von freien Netzen schwierig
- Verschiedene Projekte für freie Netze
  - Prominentestes Beispiel ist Freifunk
  - Pläne für freie Netze in Entwicklungsländern (OLPC)
  - Kommerzielles Projektbeispiel: Fon

Freifunknetz in Berlin



Einleitung

- WLAN (Wireless Local Area Network)
- Verschiedene Standards mit verschiedenen Bandbreiten (a, b, g, n und 1 – 300 Mbit)
- Reichweite bis zu 100 Metern
- Strahlungsbelastung vergleichbar mit DECT-Telefonen
- Unterstützt verschiedene “Netzwerkstrukturen”

Verschlüsselungsverfahren

- Verschlüsselungsverfahren abhängig vom Standard
- WEP (Wired Equivalent Privacey) (Unsicher)
  - Unterscheidung in Gold (128/104 Bit), Silber (64/48 Bit)
  - Verschlüsselung “basiert” auf RC4 und CRC
  - XOR Verknüpfung des Nutzdaten mit einem pseudozufälligen Bitstrom des RC4-Algorithmus
  - Schwachstelle: Verfahren
  - Verschiedene Angriffsmöglichkeiten
  - Schnellster Angriff in unter 60 Sekunden

Verschlüsselungsverfahren

- WPA (Wifi Protected Access) (Halbwegs Sicher)
  - Erweitert WEP um zusätzliche dynamische Schlüssel (Temporal Key Integrity Protocol, TKIP)
  - Zusätzliche Authentifizierungsmechanismen wie Pre-Shared-Key (PSK) und Extended Authentication Protocol (EAP)
  - Angriffsmethode: Wörterbuchattacke
  - Theoretisch im günstigsten Fall unter einer Minute

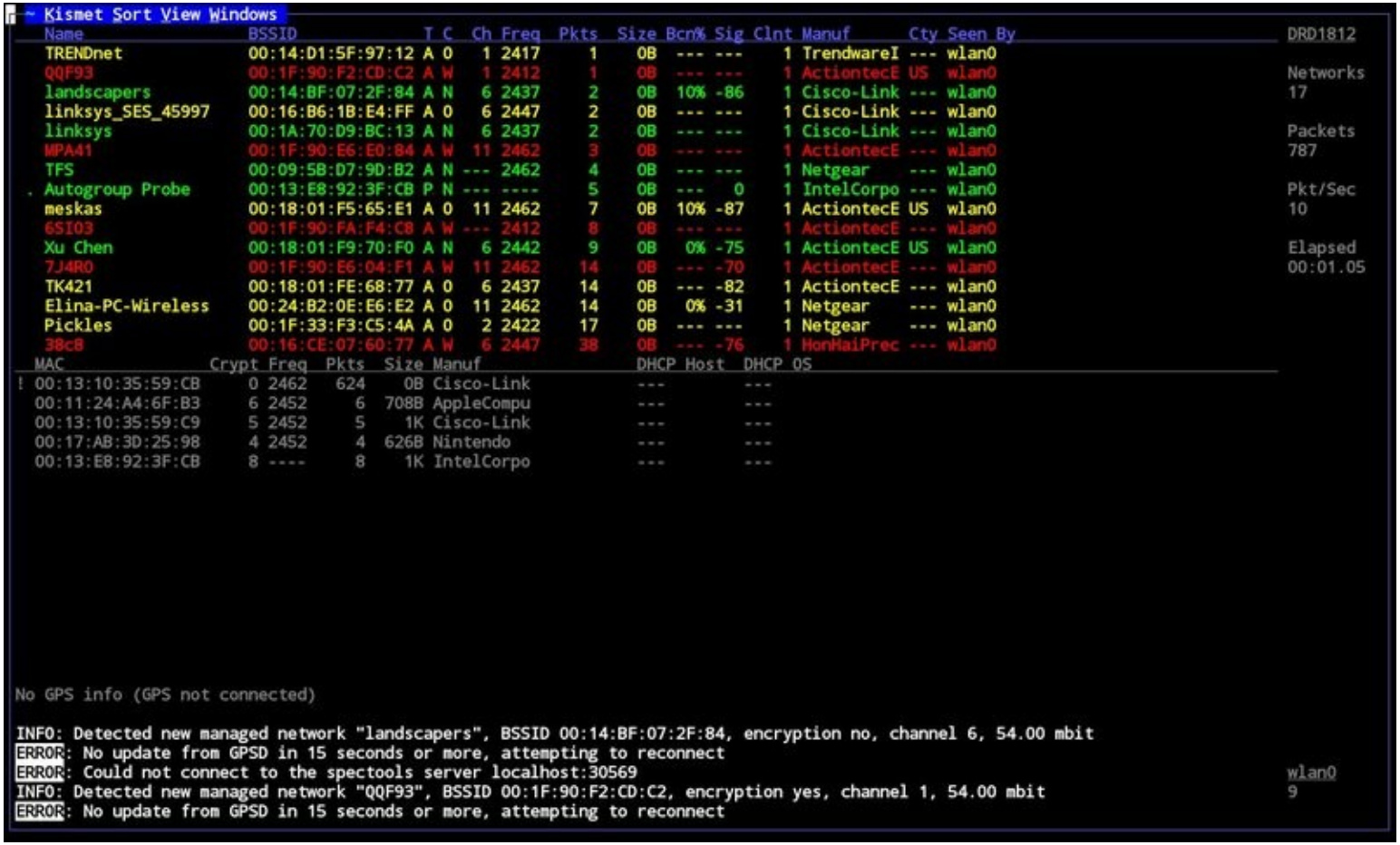
Verschlüsselungsverfahren

- WPA2 (WiFi Protected Access 2) (Sicher)
  - Verschlüsselung basiert auf Advanced Encryption Standard (AES)
  - Angriffsform: Wörterbuchattacke

Werkzeuge

- Wardriving Kit
  - WLAN Karte mit Monitoring Mode
  - Vernünftige Antenne
- Software (Open Source)
  - Aircrack-NG
  - Wireshark
  - Netstumbler
  - Kismet
  - ...

Werkzeuge


~ Kismet Sort View Windows
Name BSSID T C Ch Freq Pkts Size Bcn% Sig Clnt Manuf Cty Seen By
TRENDnet 00:14:D1:5F:97:12 A 0 1 2417 1 0B --- --- 1 TrendwareI --- wlan0
QQF93 00:1F:90:F2:CD:C2 A W 1 2412 1 0B --- --- 1 ActiontecE US wlan0
landscapers 00:14:BF:07:2F:84 A N 6 2437 2 0B 10% -86 1 Cisco-Link --- wlan0
linksys_SES_45997 00:16:B6:1B:E4:FF A 0 6 2447 2 0B --- --- 1 Cisco-Link --- wlan0
linksys 00:1A:70:D9:BC:13 A N 6 2437 2 0B --- --- 1 Cisco-Link --- wlan0
MPA41 00:1F:90:E6:E0:84 A W 11 2462 3 0B --- --- 1 ActiontecE --- wlan0
TFS 00:09:5B:D7:9D:B2 A N --- 2462 4 0B --- --- 1 Netgear --- wlan0
. Autogroup Probe 00:13:E8:92:3F:CB P N --- ---- 5 0B --- 0 1 IntelCorpo --- wlan0
meskas 00:18:01:F5:65:E1 A 0 11 2462 7 0B 10% -87 1 ActiontecE US wlan0
6SI03 00:1F:90:FA:F4:C8 A W --- 2412 8 0B --- --- 1 ActiontecE --- wlan0
Xu Chen 00:18:01:F9:70:F0 A N 6 2442 9 0B 0% -75 1 ActiontecE US wlan0
7J4RO 00:1F:90:E6:04:F1 A W 11 2462 14 0B --- -70 1 ActiontecE --- wlan0
TK421 00:18:01:FE:68:77 A 0 6 2437 14 0B --- -82 1 ActiontecE --- wlan0
Elina-PC-Wireless 00:24:B2:0E:E6:E2 A 0 11 2462 14 0B 0% -31 1 Netgear --- wlan0
Pickles 00:1F:33:F3:C5:4A A 0 2 2422 17 0B --- --- 1 Netgear --- wlan0
38c8 00:16:CE:07:60:77 A W 6 2447 38 0B --- -76 1 HonHaiPrec --- wlan0
MAC Crypt Freq Pkts Size Manuf DHCP Host DHCP OS
! 00:13:10:35:59:CB 0 2462 624 0B Cisco-Link --- ---
00:11:24:A4:6F:B3 6 2452 6 708B AppleCompu --- ---
00:13:10:35:59:C9 5 2452 5 1K Cisco-Link --- ---
00:17:AB:3D:25:98 4 2452 4 626B Nintendo --- ---
00:13:E8:92:3F:CB 8 ---- 8 1K IntelCorpo --- ---
No GPS info (GPS not connected)
INFO: Detected new managed network "landscapers", BSSID 00:14:BF:07:2F:84, encryption no, channel 6, 54.00 mbit
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
ERROR: Could not connect to the spectools server localhost:30569
INFO: Detected new managed network "QQF93", BSSID 00:1F:90:F2:CD:C2, encryption yes, channel 1, 54.00 mbit
ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
DRD1812
Networks
17
Packets
787
Pkt/Sec
10
Elapsed
00:01.05
wlan0
9

Position des Gesetzgebers - I

- Urteil Az. I ZR 121/08 des BGH zur Störerhaftung
- “Adäquat kausale Mitwirkung an der Rechtsverletzung” (Störerhaftung)
- Haftungsfrage privater WLAN Betreiber bei Urheberrechtsverletzungen
- Anschlussinhaber hat das Tatmittel “Internet” bereitgestellt und zumutbare Prüfungspflichten vernachlässigt
- Nachweis dass er nicht für die Urheberrechtsverletzung verantwortlich ist

Position des Gesetzgebers - II

- Keine Inanspruchnahme von Schadensersatz, sondern Unterlassung
- Verlangt dass private WLAN-Betreiber ausreichend verschlüsseln
- Kein Zwang auf aktuelle Standards „aufzurüsten“
- Keine generelle Regelung gegen Abmahnwahn
- Automatisiert erstellte Keys werden als “unsicher” betrachtet (siehe AVM Fritzbox)
  - LG Frankfurt, voreingestellter 16stelliger WPA Key nicht ausreichend

Allgemeine Sicherheitsmaßnahmen

- Verschlüsselung mit einer sicheren Verschlüsselungsmethoden
- Sichere Netzwerkschlüssel verwenden
  - Schlecht: 1234, TT.MM.JJJJ, Rechtsanwalt
  - Besser: _A42f0oPxY9--,lpZkT
- Ändern des SSID Namens
- Ändern der Standard Administrator Passwörter für WLAN Router
- Deaktivierung der Remote-Konfiguration von WLAN Router

Strukturelle Sicherheitsmaßnahmen

- Ist ein WLAN wirklich notwendig?
  - Bei der Verwendung sensibler Daten sollte man es niemanden zu leicht machen!
- Zweifelhafte Maßnahmen:
  - Unsichtbare SSIDs (hilft nicht wirklich …)
  - MAC-Adressen-Filter sind wirkungslos
- Verschlüsselungs des verschlüsselten Netzwerkverkehrs (VPN Lösung)

UMTS – Teilen von Netzzugängen

- Mobilfunkprovider vergeben nicht für jeden Teilnehmer eine eigene IP-Adresse
- Hintergrund ist eine zunehmende Knappheit an IPv4 Adressen
- Nutzung einer gemeinsamen Adressen mit mehreren Teilnehmern
  - Anzahl der geteilten Adressen unbekannt
  - “Kriminelle Handlungen” eher unwahrscheinlich
- Verfahren nennt sich NAPT (Network Address Port Translation)

UMTS – Fazit

- Telekom plant “ähnliche” Verfahren für die Zukunft im ISP Geschäft (IP-Multiplexing?)
- Anonymisierung ist “uninteressant”
  - Weitaus bessere und sicherere Verfahren bekannt und im Einsatz
  - Logfähigkeit schwierig einzuschätzen (aus Sicht der Infrastruktur)

Quellen

- “Ein falscher Klick ...”, c't 13/2010

  http://www.heise.de/ct/inhalt/2010/13/76/
- Anonym übers Netz

  http://www.lawblog.de/index.php/archives/2010/04/19/anonym-uber-umts/