Retour sur le 25C3: l'Allemagne quel beau pays

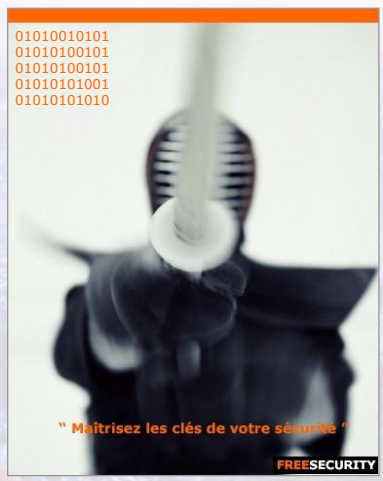
« Historique, compte rendu des conférences clefs »

Présentation OSSIR 2009

FREESECURITY™

Sommaire

- Histoire,
- Evolution de la population,
- Le 25C3,
- Jour 1,
- Jour 2,
- Jour 3,
- Jour 4,
- Conclusion,



FREESECURITY™ « Des experts au service de votre sécurité »

Histoire

- Le Chaos Computer Club Allemand a entretenu dans les années 80 des relations assez particulières avec les services Est-Allemand. Un très bon film "23" présente et rappelle un peu cette époque, où les attaques en "brute force" et les chevaux de Troie venaient de naître.
- Aujourd'hui, c'est un club allemand avec une certaine influence politique.
- Une revue du 19C3 est disponible à l'adresse : http://www.pagesecurite.com/19C3/

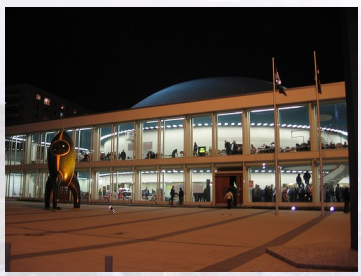
FREESECURITY™ « Des experts au service de votre sécurité »

Evolution de la population

- L'ambiance a beaucoup changé, assez familiale à ses débuts (pour moi le 15c3 en 1998), ces congres sont devenus assez impersonnels et vulgarisent maintenant les concepts ou les outils auprès du plus grand nombre.
- Cette approche est peut-être trop marquée aujourd'hui, mais permet une vraie prise de conscience des risques de la société de l'information par des utilisateurs de tout âge.

FREESECURITY™ « Des experts au service de votre sécurité »

Le 25C3



Le 25C3 s'est déroulé comme chaque année entre noël et le jour de l'an et plus précisément du 27 au 30 décembre 2008.

FREESECURITY™ « Des experts au service de votre sécurité »

25C3

- Objectifs :

  Contrairement aux premiers « congress », les conférences du CCC depuis les années 2000 ont une vocation pédagogique, ils utilisent ainsi leurs couvertures médiatiques pour :

  - lancer des alertes,
  - protéger la vie privée,
  - communiquer avec les autorités,

- Ainsi de nombreux conférenciers qui peuvent apporter des sujets intéressants sont invités par le chaos computer club.

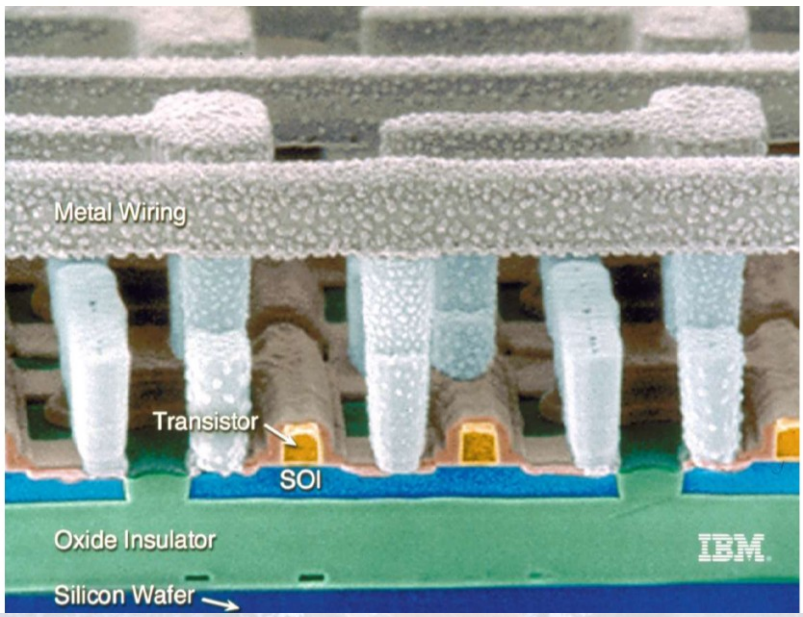
FREESECURITY™ « Des experts au service de votre sécurité »

Au menu du jour :

- Quelques conférences du 25C3, je vous conseille de prendre le temps de découvrir les vidéo des conférences qui sont normalement disponibles sur le site du CCC (http://events.ccc.de/congress/2008/wiki/Streaming)
- Mirroir (http://dewy.fem.tu-ilmenau.de/CCC/25C3/video_h264_720x576/)

Jour 1 : Chip Reverse Engineering

- Conférencier(s): Karsten Nohl, starbug
- Objectifs de la conférence:
  - présentation des moyens d'analyse des « chipsets »,
  - utilisation de la reconnaissance de forme,
  - analyse des composants par ponçages successifs,
  - création d'un logiciel spécifique d'analyse.
- *Commentaires et présentation des « slides » clefs de la conférence.*



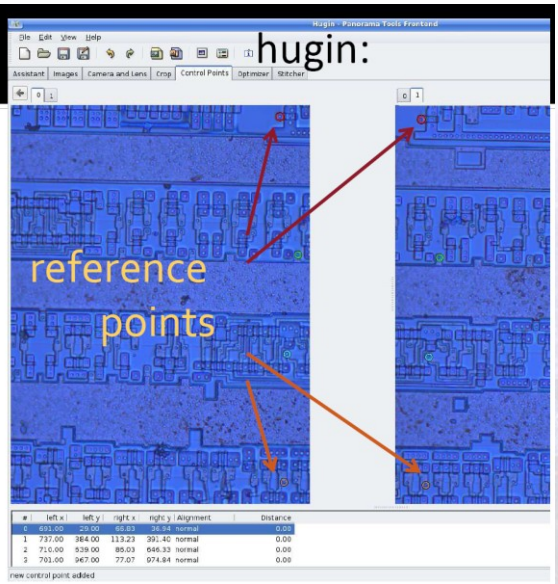
Imaging Chips

- Simple optical microscope
  - 500x magnification
  - Camera 1 Mpixel
  - Costs < $1000, found in most labs
  — or—
- Confocal microscope
  - Colors images by layer
  - Makes structures easy to spot
  - Expensive: > $10k

Starbug & Karsten Nohl – Hardware Reverse Engineering 21

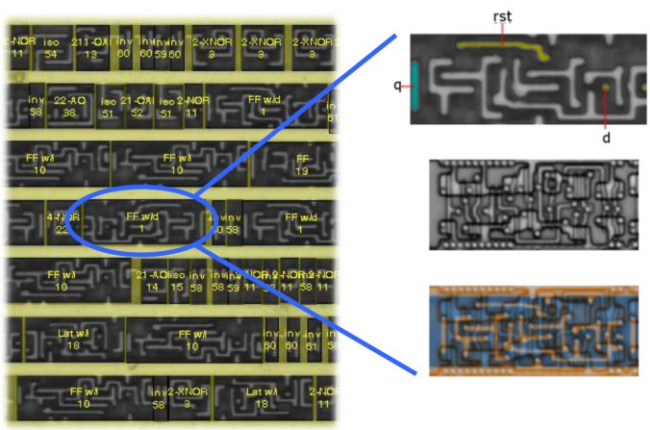
Stitching Images

- Need to stitch 100x100µm images
- Tool of choice: **hugin**
- Borrowed from panorama photography

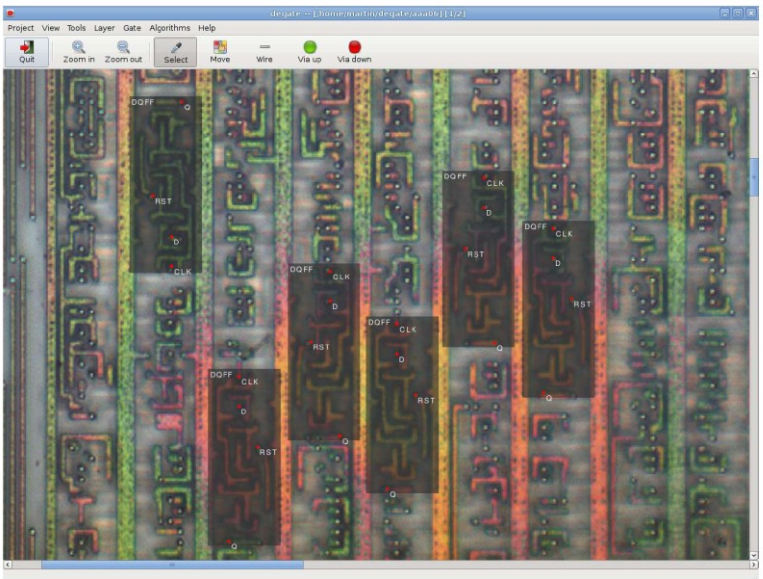


Starbug & Karsten Nohl – Hardware Reverse Engineering 23

Automated Cell Detection



Starbug & Karsten Nohl – Hardware Reverse Engineering 29



Starbug & Karsten Nohl – Hardware Reverse Engineering 33

FREESECURITY™ « Des experts au service de votre sécurité »

Jour 1 : Locating Mobile Phones using SS7

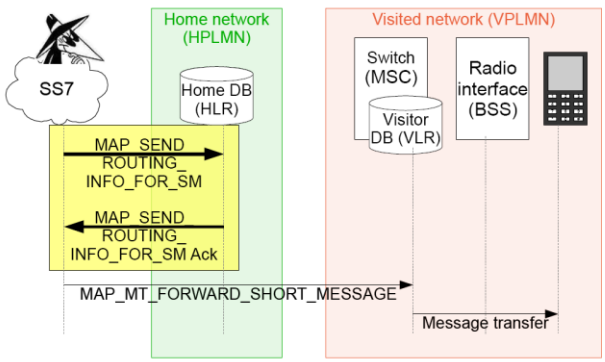
- Conférencier(s): Tobias Engel
- Objectifs de la conférence:
  - présentation des moyens de localisation par ss7,
  - identification par zone géographique,
  - présentation des contre-mesures,

- *Commentaires et présentation des « slides » clefs de la conférence.*

FREESECURITY™ « Des experts au service de votre sécurité »

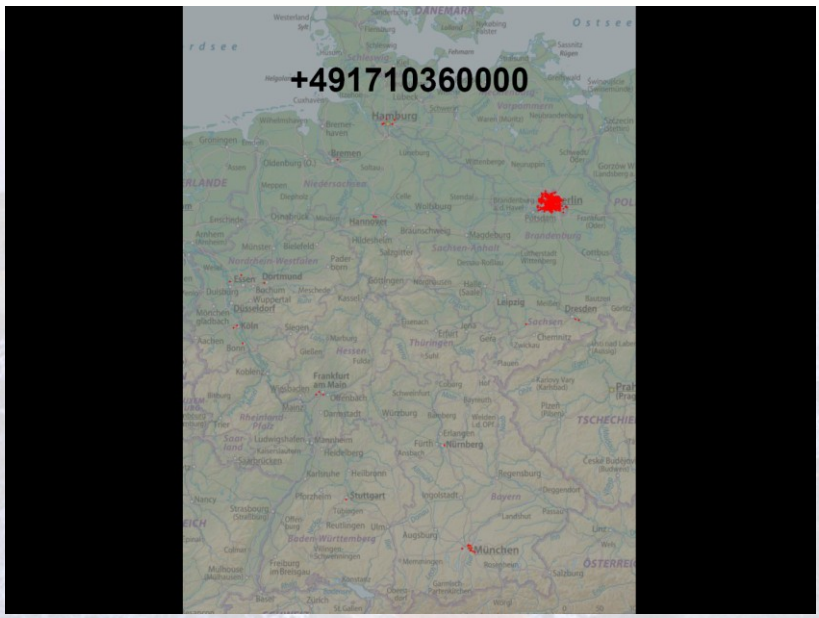
Copyright©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.com

Sending a short message



Automated approach to narrow down the area an MSC is serving (1/2)

- Rop had a great idea: if we have a lot of mobile phone numbers and already know their location, we could query the network for the current MSC of these numbers, thus creating a MSC ↔ geolocation mapping
- thanks to erdgeist, we have a decoded copy of the "Das Telefonbuch" CD
- sent tens of thousands of MAP_SEND_ROUTING_INFO_FOR_SM requests for numbers from the phonebook
  - requests where done at night, when most people are at home
  - removed the obvious errors



FREESECURITY™ « Des experts au service de votre sécurité »

Jour 2 : Exploiting Symbian

- Conférencier(s): Collin Mulliner
- Objectifs de la conférence:
  - présentation des attaques contre l'OS Symbian,
  - création d'outils spécifiques,
  - proof of concept.

- *Commentaires et présentation des « slides » clefs de la conférence.*

FREESECURITY™ « Des experts au service de votre sécurité »

SymbianOS Overview

- Currently the major smart phone operating system
  - About 50% market share (smart phones only!)
- Mainly used by Nokia and SonyEricsson (other: Samsung, Siemens, Sharp, ...)
  - Nokia bought Symbian Ltd. in mid 2008 plans to make it open source
- SymbianOS is based on EPOC (formerly Psion)
  - Renamed from EPOC to Symbian v6 in 2001
  - Current major version is 9
- Symbian separates OS from UI
  - OS from Symbian Ltd. UI from hardware vendor
    - Series60 (S60) from Nokia
    - UIQ from Sony Ericsson
    - MOAP from Sharp/NTT DoCoMo

SymbianOS 9.x Platform Security

- Capabilites
  - API based rather than resource based
  - Assigned at build-time, cannot change at runtime
  - DLL code is executed with application process' capabilities
  - Capabilites stored in executable
- Mandatory Code Signing
  - Controls who is allowed to produce software for SymbianOS
  - Needed in order to protect capabilities
- Data Caging
  - Executables and libraries are separated from data
  - Executables in \sys\bin (can only execute binaries in this directory)
  - Process data in \private\<APP UID>

State of The Art Symbian Security Issues and Attacks

- MMS and Bluetooth worms (pre SymbianOS 9.x)
  - Commwarrior, Carbir, Mabir, and others...
- Trojans and viruses (pre SymbianOS 9.x)
- Some Bluetooth bugs (DoS, file access, ...)
- Workarounds for the capability system of SymbianOS 9.x
  - Developers and users hate the capability system since they can't easily distribute and get their software anymore
  - → Reflash smart phone with modified firmware image that switches off some capability checks
  - → Use on-device DebugStub (AppTrk) to change capabilites of running app. in kernel memory

Mandatory Code Signing

- Applications need to be signed in order to get installed on a Symbian 9.x device
  - Control who gets to produce software (and what kind of software)
  - Suppress malware: worms, trojans
- Needed to protect capabilities stored in SIS files
- Ways to get application signed
  - Buy certificate
    - Different levels of capabilites
    - Payment options (per app., per device)
  - Open Signed Online
    - Free, but can only sign for individual device (per IMEI)

Our First Symbian Shellcode

- Just calls printf() and sleep() from libc
  - Loadnlookup is omitted for clarity (discussed later)

```
main:
  ldr     r0, sleep     @ r0 = ordinal of sleep
  add     r1,pc,#4*11   @ r1 = addr of libc_name
  bl      loadnlookup   @ call loadnlookup
  str     r0, sleep     @ store addr of sleep
  ldr     r0, printf    @ r0 = ordinal of printf
  add     r1,pc,#4*7    @ r1 = addr of libc_name
  bl      loadnlookup   @ call loadnlookup
  str     r0, printf    @ store addr of printf

  add     r0,pc,#4*7    @ r0 = addr of printtext
  mov     lr,pc         @ store pc in lr
  ldr     pc,printf     @ call printf
  mov     r0,#30        @ r0 = 30, sleep(30)
  mov     lr,pc         @ store pc in lr
  ldr     pc,sleep      @ call sleep

libc_name:
  .word   4
  .ascii  "l\0i\0b\0c\0"

printtext:
  .ascii  "This is your first Symbian shellcode!!\n\0"

printf:
  .word   259
sleep:
  .word   336
load_fptr:
  .word   0xF82056C0
lookup_fptr:
  .word   0xF81E35B0
```


Fraunhofer Institut Sichere Informations-Technologie

Jour 2 : Anatomy of smartphone hardware

- Conférencier(s): Harald Welte
- Objectifs de la conférence:
  - présentation d'un reverse engineering pour le Motorola X800,
  - point sur les thèmes suivants : jtag, Haret, IDA,
- *Commentaires et présentation des « slides » clefs de la conférence.*

Project gnufiish

gnufiish Status

- Kernel (2.6.24/2.6.27) booted on _first attempt_
- Working
  - I2C host controller
  - I2C communication to CPLD and FM Radio
  - USB Device mode (Ethernet gadget)
  - Touchscreen input
  - LCM Framebuffer
  - LCM Backlight control
  - GPS and Bluetooth power control
  - GPIO buttons
- In the works
  - Audio Codec driver (50% done)
  - GSM Modem (SPI) driver (80% done)
  - M800 Keyboard + Capsense driver (25% done)
  - SPI glue to libertas WiFi driver (70% done)

HOWTO

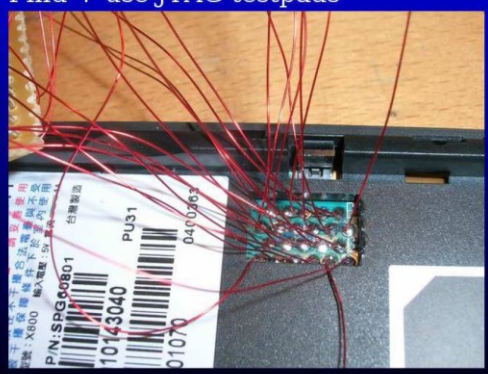
How was this done?

- Various reverse engineering techniques
  - Take actual board apart, note major components
  - Use HaRET (hardwar reverse engineering tool)
  - Find + use JTAG testpads
  - Find + use serial console
  - Disassemble WinMobile drivers

Anatomy of Contemporary Smartphone Hardware

JTAG pins

Find + use JTAG testpads



Anatomy of Contemporary Smartphone Hardware

JTAG pins

Find + use JTAG testpads

FREESECURITY™
« Des experts au service de votre sécurité »

Copyright ©2003-2005 FREESECURITY - Tous droits réservés - 27/29 Rue Raffet - 75016 Paris - Tél. +33 (0)1 46 94 66 53 - http://www.freesec.com

What's HaRET

What is HaRET

- a Windows executable program for any WinCE based OS
- offers a control interface on a TCP port
- connect to it using haretconsole (python script) on Linux PC
- supports a number of popular ARM based SoC (PXA, S3C, MSM)
- features include
  - GPIO state and tracing
  - MMIO read/write
  - virtual/physical memory mapping
  - IRQ tracing (by redirecting IRQ vectors)
  - load Linux into ram and boot it from within WinCE

Using HaRET

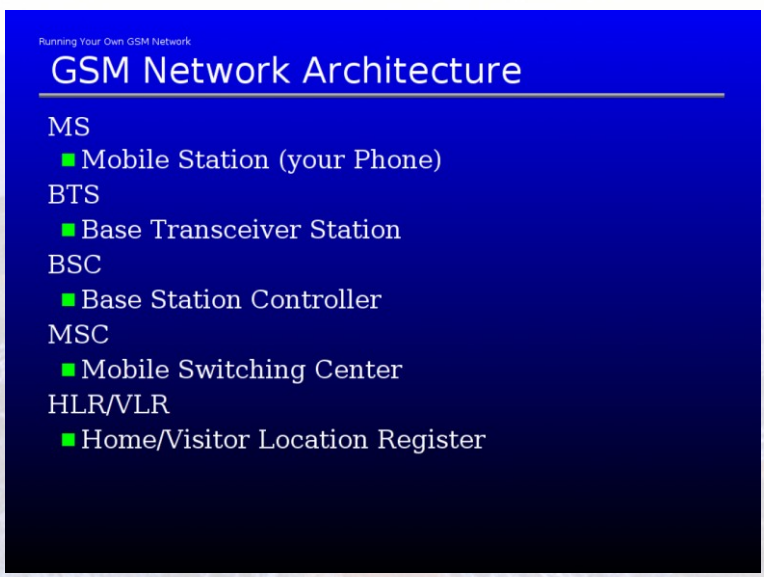
Using HARET

- watch for IRQ changes/events
  - e.g. you see DMA3 interrupts while talking to the GSM
  - read MMIO config of DMA controller to determine user: SPI
  - read SPI controller configuration + DMA controller configuration
  - find RAM address of data buffers read/written by DMA
- haretconsole writes logfiles
  - you can start to annotate the logfiles
- of course, all of this could be done using JTAG, too.
  - but with HaRET, you mostly don't need it!!!

Jour 3 : Running your own GSM network

- Conférencier(s): Harald Welte, Dieter Spaar
- Objectifs de la conférence:
  - présentation de l'analyse du protocole GSM/BTS,
  - démonstration en live,
  - projet openBSC.

- *Commentaires et présentation des « slides » clefs de la conférence,*
- *Extraits vidéo.*



The Siemens BS-11 microBTS

Siemens BS-11 microBTS
- plain old 2G (GSM voice calls, CSD)
- one or two TRX, 30mW to 2W each, GSM900
- two E1 interfaces (for daisy-chaining)
- documentation under NDA, but
  - 99.9% of the A-bis protocol available from GSM specs
    - See TS 04.08 (RLL), 12.21 (OML), 08.58 (RSL)
- RS232 serial port for Local Maintenance Terminal
  - LMT software proprietary under NDA
    - not needed for operation of the BTS

The Siemens BS-11 microBTS

First steps with the Siemens BS-11
- Harald bought a BS-11 on e-Bay in 2006
  - Started to read some specs (08.5x) about A-bis
  - Started to build cables for E1 and power
  - Bought HFC-E1 PCI card
  - Bought Elmi EGM35 Abis analyzer (e-Bay once again)
  - Contacted with other people who also bought BS-11
  - Found somebody who could provide Abis traces
  - Never really had time due to Openmoko and other projects

The Siemens BS-11 microBTS

Work at 25C3

The Egypt simulation

- apparently GPS is illegal in mobile phones in Egypt
  - "Egypt detection" implemented by checking if any surrounding cells are with Egypt country code
  - phones don't even have to register to our BTS!
  - so if we claim to be e.g. MobiNil, phones will shut off their GPS

- Vidéo -

FREESECURITY™ « Des experts au service de votre sécurité »

Jour 3 : Analyzing RFID Security

- Conférencier(s): Henryk Plötz, Karsten Nohl
- Objectifs de la conférence:
  - point sur la sécurité RFID,
  - projet openpicc & openpcd,
  - présentation des outils d'attaque,
- *Commentaires et présentation des « slides » clefs de la conférence,*

FREESECURITY™ « Des experts au service de votre sécurité »

Mifare Classic Break

- Mifare cards uses proprietary Crypto-1 algorithm
  - Never publicly reviewed for 20+ years
- We reverse-engineered algorithm and announce insecurities at 24C3
- Feb/Mar: Reports find Crypto-1 to be strong enough for a "few more years"
  - We releases more details about attacks
    - Final report recommends migration
- April: Dutch researchers publicly demonstrate attacks against Oyster
  - Law suit erupts, free speech prevails
  - Details published in October

30

Emulation

- Spoof "unique" data of tags such as UID
- Done with RFID emulator (OpenPICC) or higher-powered tag (SmartMX)
- Foundation for other attack vectors

Karsten Nohl, Henryk Plötz - RFID Security 10

Replay

1. Overhear legitimate authentication
2. Force same challenge, answer with same response
   - Requires predictable "random" numbers

Karsten Nohl, Henryk Plötz - RFID Security 12

RFID Tools – TI EVM

- Multi-protocol, software-extensible RFID kit
- Evaluation module w/ support for Tag-It, ISO 15693, 14443 A/B incl. software-based *Mifare Classic* encryption
- Excellent base for :
  - (upgrade) reader design
  - RFID fuzz tester

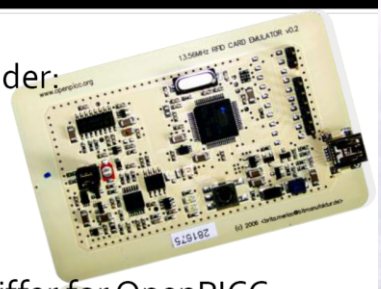
Download utility and firmware patch at www.cs.virginia.edu/~kn5f

Karsten Nohl, Henryk Plötz - RFID Security 22

RFID Tools – OpenPICC Sniffer

Open source RFID tools:

- multi-protocol RFID reader: OpenPCD
- RFID emulator: OpenPICC



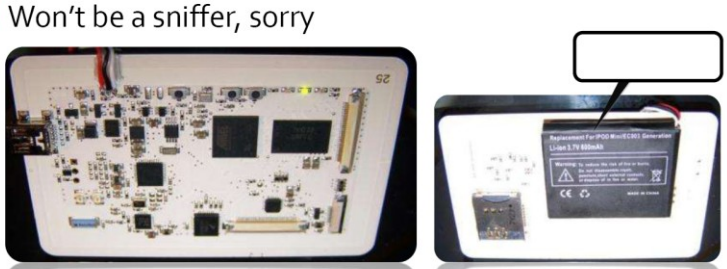
- Implemented Mifare sniffer for OpenPICC
  - capture both directions simultaneously
  - sniffing distance: millimeters from card, centimeters from reader

Firmware at svn.openpcd.org/branches/sniffonly/

Karsten Nohl, Henryk Plötz - RFID Security 23

RFID Tool – OpenPICC2

- Next Generation RFID emulator OpenPICC2:
  - Implements tag and reader side, and OpenBeacon!
  - Sufficient resources for on-board crypto (cracking?):
    - 16 MB Ram, 48 MHz ARM7, SD-card slot
  - Won't be a sniffer, sorry



Karsten Nohl, Henryk Plötz - RFID Security 24

Jour 4 : MD5 considered harmful today

- Conférencier(s): David Molnar, Marc Stevens, Arjen Lenstra, Benne de Weger, Alexander Sotirov, Jacob Appelbaum, Dag Arne Osvik
- Objectifs de la conférence:
  - présentation des failles MD5,
  - soumission d'un faux certificat,
- *Commentaires et présentation des « slides » clefs de la conférence,*

Vulnerable CAs in 2008

- We collected 30,000 website certificates
  - 9,000 of them were signed with MD5
  - 97% of those were issued by RapidSSL
- CAs still using MD5 in 2008:
  - RapidSSL
  - FreeSSL
  - TrustCenter
  - RSA Data Security
  - Thawte
  - verisign.co.jp

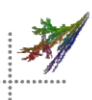
Collision generation

Based on the 2007 chosen-prefix collisions paper with new improvements

1-2 days on a cluster of 200 PlayStation 3's

Equivalent to 8000 desktop CPU cores or $20,000 on Amazon EC2

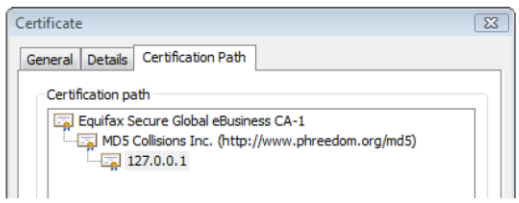
Real life execution of the attack



- 3 failed attempts
  - problems with timing
  - other CA requests stealing our serial number
- Finally success on the 4th attempt!
- Total cost of certificates: USD $657

Man-In-The-Middle

- We can sign fully trusted certificates
- Perfect man-in-the-middle attacks



- A malicious attacker can pick a more realistic CA name and fool even experts

Repeating the attack

With optimizations the attack might be done for $2000 on Amazon EC2 in 1 day

We want to prevent malicious entities from repeating the attack:

- We are not releasing our collision finding implementation or improved methods until we feel it's safe
- We've talked to the affected CAs: they will switch to SHA-1 very, very soon

Remerciements

- Un grand merci aux conférenciers et au CCC qui chaque année réalisent un événement de qualité,
- Si cela vous tente de découvrir l'Allemagne entre noël et le jour de l'an : laurent.dupuy@freesec.com.

FREESECURITY™
« Des experts au service de votre sécurité »