NSA PLAYSET: GSM

pierce , loki DEFCON 22

Who are we?

whois: Pierce

- 4th DEFCON talk
- Attending DEFCON since 10
- Infosec Professional (product security rocks)
- Much Wireless

Who are we?

whois: Loki

- 12 years as a software developer and architect
- Currently specializing in data analytics
- Has always worn a security hat
- Interested in GSM for the past 4 years

Intro to GSM

- Most widely used cellular system in the world
- First to seriously consider security threats
- Originally developed during the late 1980s
- First deployed in the early 1990s
- Still in wide use today

Intro to GSM

- Almost all implementations use the A5/1 stream cipher to communicate between handset and base station
- Occasionally, the less secure A5/2
- Potentially, but not seen in the wild, the more secure A5/3 aka KASUMI

History Lesson: 1990s

- 1994: First attack on A5 Proposed
- 1997: First formal Cryptanalysis of A5

History Lesson: 2000

- Plaintext-required time-memory tradeoff attack

History Lesson: 2003

- Ciphertext-only time-memory tradeoff attack

History Lesson: 2007

- COPACOBANA

History Lesson: 2008

- First tables generated, but never released

History Lesson: 2009

- A5/1 Cracking Project
- Kraken
- First Rainbow Tables Released

History Lesson: 2010

- Airprobe: GSM capture via USRP
- OsmocomBB: GSM capture via Calypso

History Lesson: 2012

- RTL-SDR: inexpensive SDR

History Lesson: 2013

- HackRF & BladeRF
  - improved inexpensive SDR
- Toorcon
- NSA ANT Catalog Leak

History Lesson: 2014

- NSA Playset is born!
  - Shmoo
  - HITB Amsterdam
  - Toorcamp
  - DEFCON

NSA Playset

- ease of use
- cost reduction

“If a 10 year old can’t do it, it doesn’t count”

What We Did So Far

- Airprobe working with multiple SDR platforms
- Airprobe signal tracking improved
- Kraken A5/1 tables and indexes on portable disks
- Bootable environment for capture

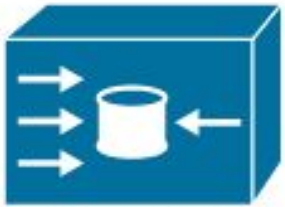
TWILIGHTVEGETABLE

- A system for automatic collection and decryption of GSM data on multiple channels
- Source support for any SDR; as well as Osmocom and Samsung Galaxy devices
- No, it’s not ready yet

TWILIGHTVEGETABLE

Overview:

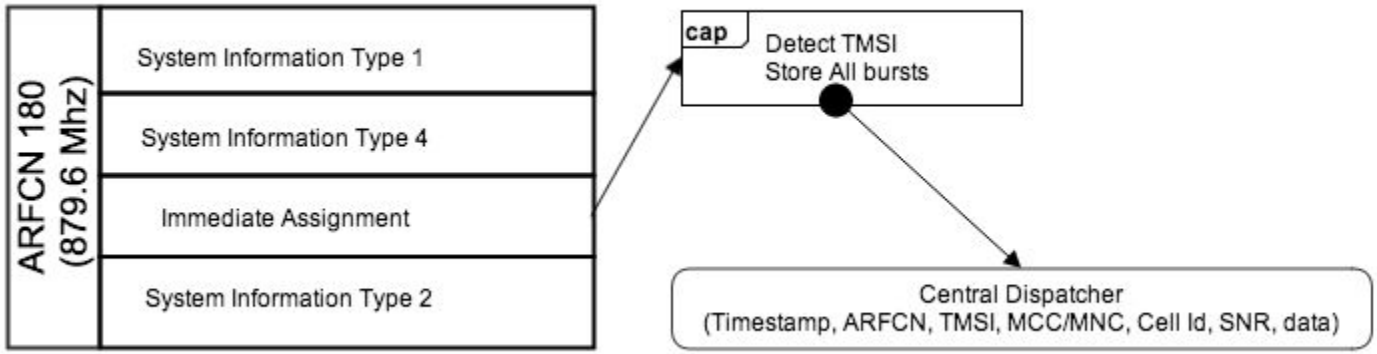
Um Interface Client Capture Devices


Central Dispatcher


Kraken Server

TWILIGHTVEGETABLE

Um Interface client capture device:



TWILIGHTVEGETABLE

Central Dispatcher

- it accepts and stores submitted capture files
- runs plain text statistics and submits to kraken
- it associates cracked keys with TMSIs
- decodes SMS and voice traffic

TWILIGHTVEGETABLE

Kraken:

- When run in server mode, allows queuing of crack requests
- Can also run multiple instances in parallel and load balance.

TWILIGHTVEGETABLE

Our Kit:

- 16GB Customized Bootable Kali Linux Image
-

TWILIGHTVEGETABLE

SDR Supplier: NooElec

- provided free swag for you
- $5 off $40 discount code: DEFCON1
- Accepts Bitcoin!

SECRET//COMINT//REL TO USA, FVEY

GENESIS

Covert SIGINT Transceiver

(S//SI//REL) Commercial GSM handset that has been modified to include a Software Defined Radio (SDR) and additional system memory. The internal SDR allows a witting user to covertly perform network surveys, record RF spectrum, or perform handset location in hostile environments.

01/27/09

(S//SI//REL) GENESIS Handset

(S//SI//REL) The GENESIS systems are designed to support covert operations in hostile environments. A witting user would be able to survey the local environment with the spectrum analyzer tool, select spectrum of interest to record, and download the spectrum information via the integrated Ethernet to a laptop controller. The GENESIS system could also be used, in conjunction with an active interrogator, as the finishing tool when performing Find/Fix/Finish operations in unconventional environments.

➢ **(S//SI//REL) Features:**

- Concealed SDR with Handset Menu Interface
- Spectrum Analyzer Capability
- Find/Fix/Finish Capability
- Integrated Ethernet
- External Antenna Port
- Internal 16 GB of storage
- Multiple Integrated Antennas

➢ **(S//SI//REL) Future Enhancements:**

- 3G Handset Host Platform
- Additional Host Platforms
- Increased Memory Capacity
- Additional Find/Fix/Finish Capabilities
- Active Interrogation Capabilities

Status: Current GENESIS platform available. Future platforms available when developments are completed.

Unit Cost: $15K

POC: [redacted], S32242, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

SECRET//COMINT//REL TO USA, FVEY

LEVITICUS

LEVITICUS

- Regular C139 phone
- C123 is for suckers (and Europeans)
- OsmocomBB is great
- Cable is simple FTDI to micro audio
- Custom firmwares exist only in memory

LEVITICUS (rssi)

- ./rssi.sh

LEVITICUS (layer1)

- ./layer1.sh
- ./ccch_scan.sh
- wireshark

LEVITICUS

- Make sure the scripts are pointing to the correct serial device!
- Generally advised to not leave the phones charging unattended.

LEVITICUS

- GSM Map is a cool project (gsmmap.org)

LEVITICUS (DIY)

- Search ebay for C139
- Avoid Tracphones
- Cingular phones work out of the box

- uber.waves on ebay
  - uberwaves@gmail.com

DRIZZLECHAIR

- Kraken!
- A5/1 Rainbow Tables
- 2T WD Elements
- USB 3.0

DRIZZLECHAIR

- First 5G partition has all the tools
- The tables are ***in*** the partition
- Known-Plaintext attack

DEMO TIME!

QUESTIONS?

(prizes)

Your turn!

- Visit NSAPlayset.org
- Join the mailing list! Right now!
- We have stuff to sell you!