# GSM Security Problems

Harald Welte

osmocom.org
hmw-consulting.de
sysmocom.de

July 2013, TSC TIB, Taipei/TAIWAN

# About Harald Welte

hwelte@hmw-consulting.de

- Linux Kernel, bootloader, driver, firmware developmer since 1999
- IT security specialist, focus on network protocol security
- Board-level Electrical Engineering
- Interested in various protocols (RFID, DECT, GSM)
- netfilter/iptables, OpenPCD, OpenMoko, librfid, OpenEZX
- Main developer of OpenBSC project
- Founder and key developer of OsmocomBB project
- Co-founder of sysmocom - systems for mobile communications GmbH

# About Osmocom.org

## Open Source MObile COMmunications

- community-driven project to implement communcation systems on protocol and/or radio level
- many sub-projects, including
  - OsmocomBB (telephone-side GSM stack)
  - OpenBSC (OsmoNITB, OsmoBSC, network-side GSM stack)
  - OsmoSGSN and OpenGGSN (network-side GPRS+EDGE)
  - OsmocomTETRA (TETRA PMR receiver/decoder)
  - OsmocomGMR (GMR satellite telephony decoder)
  - OsmocomDECT (DECT cordless telephony)
  - OsmocomSIMTRACE (SIM protocol tracer hardware)
  - OsmocomSDR (SDR receiver hardware)

# Legal Disclaimer

- GSM operates in licensed spectrum
- Operating any transmitter in the GSM frequency bands requires a license from the respective regulatory authority
- Interference with commercial cellular operators is often a fellony and punishable as a crime
- It is the users responsibility to configure OpenBSC and BTS equipment in a way that complies with the law

# Legal Disclaimer

- We are demonstrating normal GSM operations and security flaws using a private network and informed participants
- By leaving your GSM handset turned on during this workshop, you consent to participate in these demonstrations
- Nothing we do will damage your handset, but may cause temporary disruptions in service, unsolicited text messages or other annoyances
- Not all of the software used to demonstrate security weaknesses is part of the normal OpenBTS or OpenBSC distributions

# Information Sources

- All information presented here is available form public sources
- Most of the information presented here is readily derived from public specifications, *if you actually take the time to read them*
- Nothing presented here is subject to trade secret restrictions
- Nothing presented here was received under a government security clearance agreement

# Threat Models

- GSM is a massively distributed network with many interfaces
- Some interfaces are exposed completley public, others not
- Attack vectors and threat models depend on who you are

# If you are an operator

- The subscriber is a potential attacker
  - may want to commit fraud
  - may want to DoS or otherwise impact your network
  - may be violating your terms of services (VoIP, SIMboxes)
  - SIM card cloning
- A third party is a potential attacker
  - only as much as a subscriber (see above)
  - SS7 based fraud (SMS spam, etc.)
  - eavesdropping on Um, Abis/microwave, SS7 etc. is mostly to invide subscriber privacy. Not primarliy an operator concern!

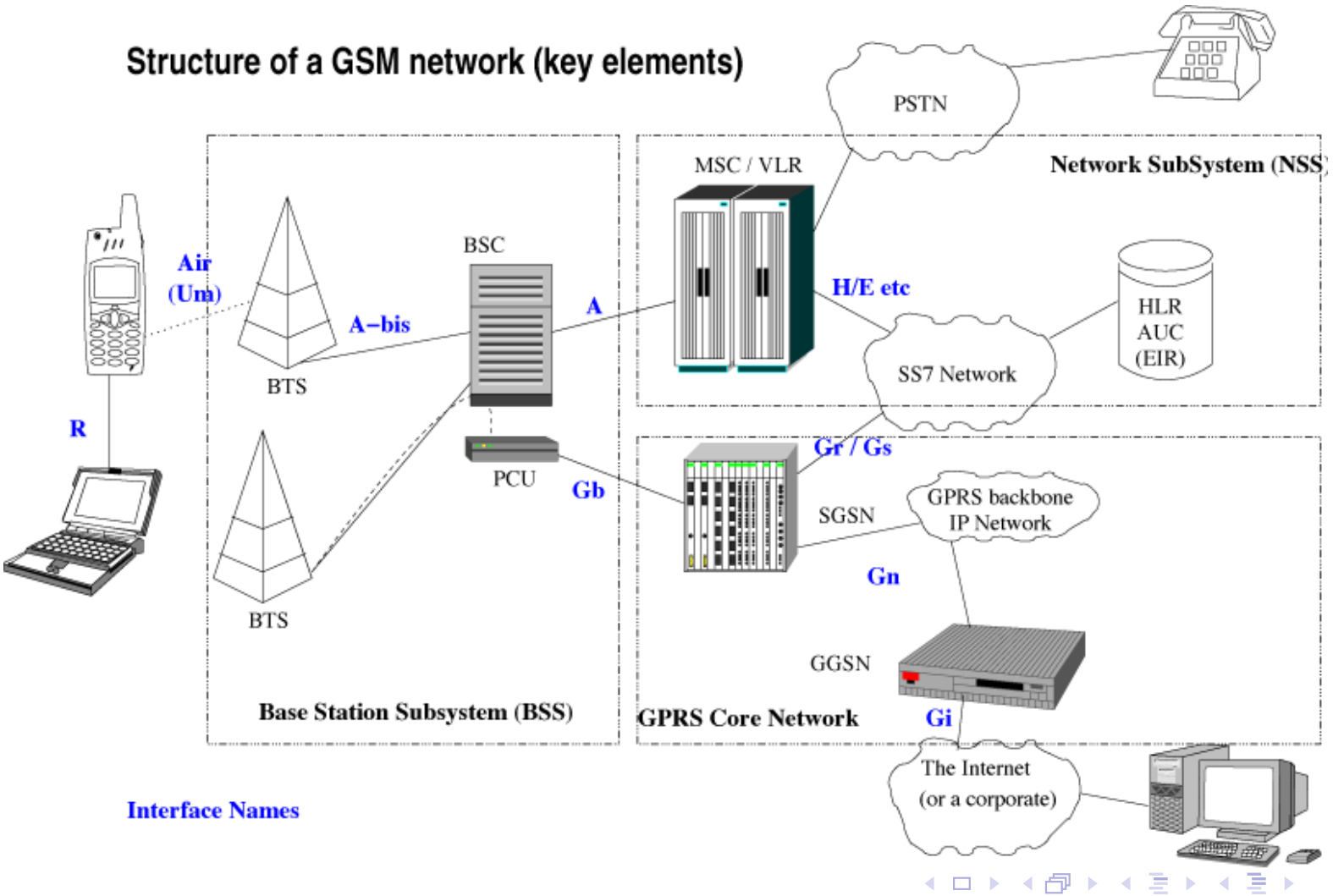
# If you are a subscriber

- The operator is a potential threat
  - detailed location profiles about subscriber
  - access to all plain-text communication
  - untrusted operator SIM card tied into your phone
- A third party is a potential threat
  - eavesdropping on the radio interface
  - eavesdropping on microwave back-haul
  - intelligence based on SS7 queries on the worldwide SS7 network
  - mobile malware on your phone, on your SIM
- Governments are a potential threat
  - access to all data (location, CDR) at the operator
  - actively performing air interface attacks (IMSI catcher, etc)
  - lawful intercept at the core network

# If you are a government

- The operator is a potential threat
  - mostly because operator has all CDRs, location profiles and access to content of communication. An informant at the operator could coopeate with foreign governments or criminal groups
  - security of the private operator affects your security
  - operator wants to maximize profits, not subscriber :security
- Other governments are a potential threat
  - eavesdropping on the air interface or microwave back-haul
  - active attacks on the air interface
  - mobile malware on phone or SIM cards
  - SS7 based intelligence (location, etc.) from worldwide SS7 network
- Criminal organizations are a potential threat
  - the same as *Other governments* above

# The GSM network



# GSM network components

- The BSS (Base Station Subsystem)
  - MS (Mobile Station): Your phone
  - BTS (Base Transceiver Station): The *cell tower*
  - BSC (Base Station Controller): Controlling up to hundreds of BTS
- The NSS (Network Sub System)
  - MSC (Mobile Switching Center): The central switch
  - HLR (Home Location Register): Database of subscribers
  - AUC (Authentication Center): Database of authentication keys
  - VLR (Visitor Location Register): For roaming users
  - EIR (Equipment Identity Register): To block stolen phones

# Known GSM security problems

## Scientific papers, etc

- No mutual authentication between phone and network
  - leads to rogue network attacks
  - leads to man-in-the-middle attacks
  - is what enables IMSI-catchers
- Weak encryption algorithms
- Encryption is optional, user never knows when it's active or not
- DoS of the RACH by means of channel request flooding
- RRLP (Radio Resource Location Protocol)
  - the network can obtain GPS fix or even raw GPS data from the phone
  - combine that with the network not needing to authenticate itself

# Known GSM security problems

## The Baseband side

- GSM protocol stack always runs in a so-called baseband processor (BP)
- What is the baseband processor
  - Typically ARM7 (2G/2.5G phones) or ARM9 (3G/3.5G phones)
    - Runs some RTOS (often Nucleus, sometimes L4)
    - No memory protection between tasks
  - Some kind of DSP, model depends on vendor
    - Runs the digital signal processing for the RF Layer 1
    - Has hardware peripherals for A5 encryption
- The software stack on the baseband processor
  - is written in C and assembly
  - lacks any modern security features (stack protection, non-executable pages, address space randomization, ..)

# Interesting observations

## Learned from implementing the stack

While developing OpenBSC, we observed a number of interesting

- Many phones use their TMSI from the old network when they roam to a new network
- Various phones crash when confronted with incorrect messages. We didn't even start to intentionally send incorrect messages (!)
- There are tons of obscure options on the GSM spec which no real network uses. Potential attack vector by using rarely tested code paths.

OpenBTS developers observed the same.

# GSM Security: A5 – Ciphering

- A5 is a family of symmetric ciphers inside the GSM Um Layer 1
  - A5/0 means no encryption
  - A5/1 is the *secure* cipher variant
  - A5/2 is the *weak* cipher variant
  - A5/3 is the 64bit variant of UMTS cipher for GSM
  - A5/4 is the 128bit variant of the UMTS cipher for GSM
  - A5/5..8 mentioned in protocol spec but never defined
- MS indicates A5 capabilities in classmark procedure
  - Compromised MS software could indicate no A5/1 capability to the network
  - Network can decide to use A5/0 even if the phone supports A5/1,2,3

# GSM Security: A5 – Ciphering

- Encryption Key $K_C$ is produced as result to A3/A8 authentication
- Re-keying can be initiated by the network at any given time by means of the authentication procedure
- $K_C$ as a result of authentication is stored on SIM
- $K_C$ can be read and written by the phone itself
  - OS on Baseband Processor typically has some kind of API to access SIM
  - However, quite often direct access to $K_C$ is not permitted
  - Still, baseband processor software exploits do exist!

# GSM uses symmetric session keys

Operator and phone share a master key to derive session keys

Random nonce

Master key

Hash function

Session key

**Operator Home Location Register**

Random nonce and **session key**

**Base station**

Random nonce

Communication A5/1-encrypted with **session key**

**Cell phone**

**This talk discusses a technique for extracting session keys**

# GSM Security – Bad Assumption

## Bad Assumption

No rogue actors in L3

- Any entity that can implement L1 and L2 correctly is assumed to be legitimate until a challenge fails
- This was a common telco security assumption in the 1980's, back when equipment was big and expensive and all of the networks were run by governments and quasi-governmental monopolies
- It is an assumption inherited from wireline telcos, and is even weaker in the wireless world

# GSM Security – Oversights

## Oversight

No authentication of the network

- GSM allows the network to authenticate a handset, but provides no means for the handset to authenticate the network
- Authentication is based on challenge-response, but the only comparison happens in the network end
- Any entity that can present a network-side Um interface is assumed to the legitimate, making it easy to create the GSM equivalent of a rogue access point.

# GSM Security – Oversights

## Oversight

Handset cannot release in L3 RR

- The channel release operation must always be initiated by the network
- As long as the handset sees a valid idle pattern in L2, it can be made to hold an active channel indefinitely

# GSM Security – Oversights

## Oversight

The network controls privacy

- GSM privacy controls are in the network, not in the handset
- Ciphering indications controlled by carrier.
- Any entity that assumes the role of the network takes control of the privacy features as well.
- Once camped, the MS is essentially a slave of the BTS.

# GSM Security – Oversights

## Oversight

Ciphering was an afterthought

- Ciphering was added to the system low in L1, below FEC
- L2 idle frames generate a lot of known plaintext
- FEC lowers the entropy of the plaintext stream
- The A5 ciphering algorithms were not subject to adequate review by cryptographic experts prior to standardization
- Encryption at L1 cannot be end-to-end since L1 terminates in the BTS, *so microwave backhaul can still be fully exposed*

# GPRS Security – Oversights

## Oversight

GPRS uses same $K_C$ key generation (A3/A8) as GSM

- Even if GPRS has stronger crypto algorithm, $K_C$ is generated the same way as in GSM
- $K_C$ key recovery attack using A5/2 can be performed using same random challenge
- GPRS traffic can thus be recorded and later reviewed if MS with same SIM enters IMSI-Catcher and is presented with challenge from the recording

# GSM Security – Oversights

## Oversight

UMTS handsets also support GSM

- Many GSM security problems are fixed in UMTS, but all UMTS handsets fall back to 2.5G GSM operation when UMTS is not available.
- UMTS handsets can be ordered to fall back to GSM by a rogue 3G Node B before mutual authentication even happens.
- UMTS handsets can be forced into the GSM mode by jamming the UMTS service.

# GSM Security – Anachronism

## Anachronism

Predates public key encryption

- Network cannot authenticate the initial access attempt
- Any transaction must begin with the revelation of some subscriber ID over an unencrypted channel
- All security depends on the protection of $K_i$
- Once $K_i$ is broken, the SIM is permanently compromised

# GSM Security – Intentional Weaknesses

## Intentional Weakness

A5/1 & A5/2

- Western governments were reluctant to export “strong” encryption to other parts of the world, so they defined two ciphering algorithms, A5/1 for the US and Europe and A5/2 for everywhere else
- The specification requires that any handset support both of these algorithms, so the cryptosystem is exported anyway and determined party can reverse-engineer either A5 from a standard handset.

# GSM Security – Intentional Weaknesses

## Intentional Weakness

Carriers do not use the full range of $K_i$, $K_C$.

- The spec allows 128 bits for $K_i$, but some carriers allegedly use only 64.
- The spec allow 64 bits for $K_C$, but some carriers evidently use only 54.

# GSM Security – Intentional Weaknesses

## Intentional Weakness

Security features are optional

- Authentication is optional
- A5/0 means no ciphering at all and all handsets support it
- TMSIs are optional
- A3/A8 is selected by the operator, used to be COMP128

# GSM Security – Handset Bugs

- TMSI exposure bugs compromise anonymization
- Many handsets crash or hang when presented with erroneous message formats or sequences
- Many features of the protocol are not widely used and therefore probably not well tested
- Many handsets vendor specific OTA and SIM support features not subject to outside review

# GSM/3G protocol level security

- Observation
  - Both GSM/3G and TCP/IP protocol specs are publicly available
  - The Internet protocol stack (Ethernet/Wifi/TCP/IP) receives lots of scrutiny
  - GSM networks are as widely deployed as the Internet
  - Yet, GSM/3G protocols receive no such scrutiny!
- There are reasons for that:
  - GSM industry is extremely closed (and closed-minded)
  - Only about 4 closed-source protocol stack implementations
  - GSM chip set makers never release any hardware documentation

# The closed GSM industry
## Handset manufacturing side

- Only very few companies build GSM/3.5G baseband chips today
  - Those companies buy the operating system kernel and the protocol stack from third parties
- Only very few handset makers are large enough to become a customer
  - Even they only get limited access to hardware documentation
  - Even they never really get access to the firmware source

# The closed GSM industry

## Network manufacturing side

- Only very few companies build GSM network equipment
  - Basically only Ericsson, Nokia-Siemens, Alcatel-Lucent and Huawei
  - Exception: Small equipment manufacturers for picocell / nanocell / femtocells / measurement devices and law enforcement equipment
- Only operators buy equipment from them
- Since the quantities are low, the prices are extremely high
  - e.g. for a BTS, easily 10-40k EUR
  - minimal network using standard components definitely in the 100,000s of EUR range

# The closed GSM industry
## Operator side

From my experience with Operators (prove me wrong!)

- Operators are mainly finance + marketing today
- Many operators outsources
  - Network servicing / deployment, even planning
  - Other aspects of business like Billing
- Operator just knows the closed equipment as shipped by manufacturer
- Very few people at an operator have knowledge of the protocol beyond what's needed for operations and maintenance

# The closed GSM industry
## Security implications

The security implications of the closed GSM industry are:

- Almost no people who have detailed technical knowledge outside the protocol stack or GSM network equipment manufacturers
- No independent research on protocol-level security
  - If there's security research at all, then only theoretical (like the A5/2 and A5/1 cryptanalysis)
  - Or on application level (e.g. mobile malware)
- No open source protocol implementations
  - which are key for making more people learn about the protocols
  - which enable quick prototyping/testing by modifying existing code

# Security analysis of GSM
## How would you get started?

If you were to start with GSM protocol level security analysis, where and how would you start?

- On the handset side?
  - Difficult since GSM firmware and protocol stacks are closed and proprietary
  - Even if you want to write your own protocol stack, the layer 1 hardware and signal processing is closed and undocumented, too
  - Known attempts
    - The TSM30 project as part of the THC GSM project
    - MADos, an alternative OS for Nokia DTC3 phones
  - none of those projects successful so far

# Security analysis of GSM
## How would you get started?

If you were to start with GSM protocol level security analysis, where and how would you start?

- On the network side?
  - Difficult since equipment is not easily available and normally extremely expensive
  - However, network is very modular and has many standardized/documented interfaces
  - Thus, if equipment is available, much easier/faster progress
  - Also, using SDR (software defined radio) approach, special-purpose / closed hardware can be avoided

# Security analysis of GSM
## The bootstrapping process

- Read GSM specs day and night (> 1000 PDF documents)
- Gradually grow knowledge about the protocols
  - OpenBSC: Obtain actual GSM network equipment (BTS)
  - OpenBTS: Develop SDR based GSM Um Layer 1
- Try to get actual protocol traces as examples
- Start a complete protocol stack implementation from scratch
- Finally, go and play with GSM protocol security

# False BTS Basis #1

**Problem**

The handset does not authenticate the network.

- Any device that can generate the network-side Um interface can be used to spoof a cellular carrier.
- All you need to do is terminate L3 locally and run a partial simulation of the carrier's core network.
- Once you overcome the technical hurdle of generating Um, the rest is depressingly easy.

# False BTS Basis #2

**Problem**

Ciphering is optional.

- If ciphering were mandatory, it would allow the handset a means of authenticating the network Oh well...

# False BTS IP History

- Patents are public records:
  - Early Nokia work
  - R&S EP 1051053 – the first real IMSI-catcher patent
- Litigation produces public records:
  - MMI v CellXion – lots of discussion of IMSI-catcher history, identified several IMSI-catcher developers
  - Martone v Burgess – public identification of IMSI-catcher developers working for the US gov't

# R&S “Virtual Basestation”

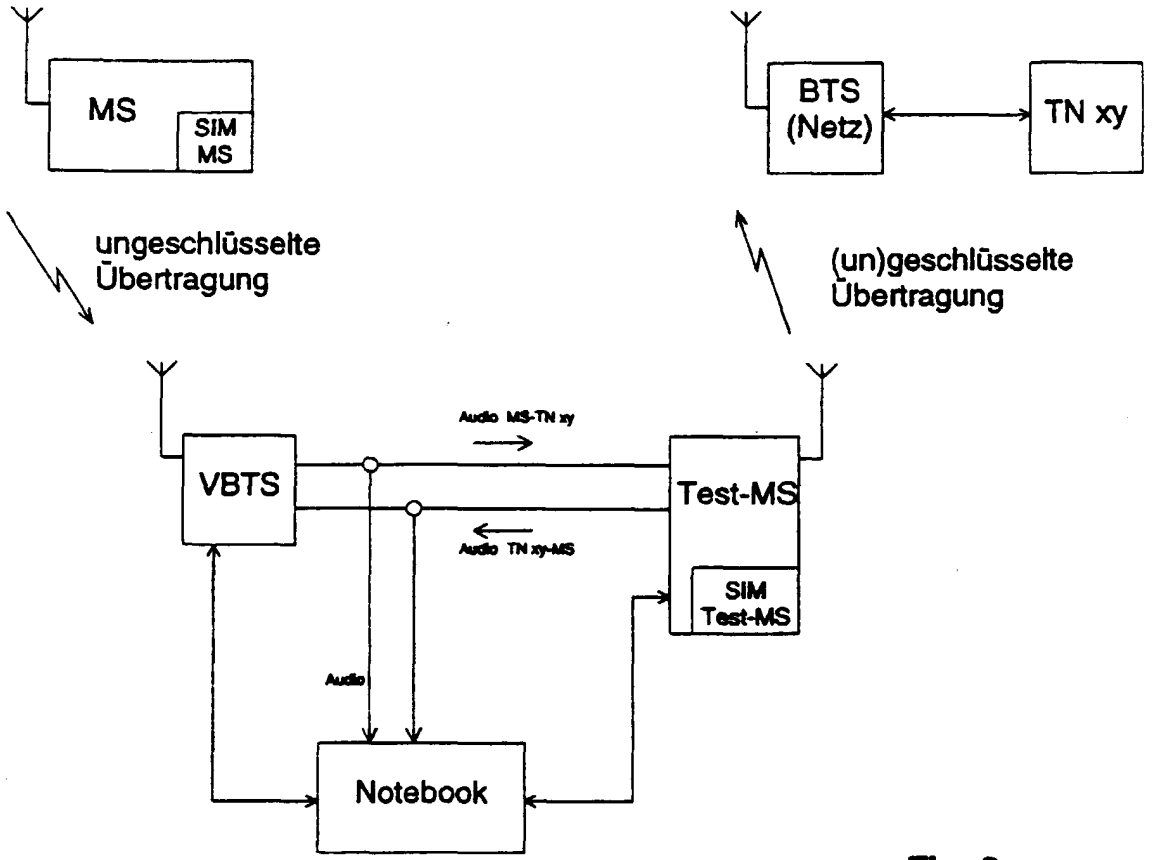



Figure : From EP 1051053

# False BTS Design Approaches

- Early R&S designs (GA 090) based on BTS emulators.
- Standard approach: mini-BTS and laptop with T1/E1 card. Hardware similar to OpenBSC w/BS11.
- Abis-over-IP quickly replacing T1/E1 systems (CellXion/Datong DX series). Hardware same as OpenBSC w/NanoBTS.
- All-software BTS units with tighter L3 integration starting to appear (MRT-BTS). Software approach more similar to OpenBTS.

# False BTS Example – Datong

The Datong series of DX products are primarily designed to provide Law Enforcement and the Military with a comprehensive toolkit of functionality in the increasing battle against mobile communications technology.
The DX series is primarily intended for

- Hard identification of mobiles in a given area
- A mechanism to enable a tracking signal from a “target” mobile
- Providing an interface for monitoring target mobile originated calls and SMS’s
- The protection of personnel and real estate from injury, harm or damage where mobile communications equipment have been known to be used to remotely trigger incendiary devices.


Figure : From Datong brochure

# False BTS Example – MRT

Figure : From MRT, Inc. public web pages

# False BTS Example – Tecore

### WHAT IS IT AND HOW DOES IT WORK?

IntelliJAM is comprised of a control unit and a mini base station. It is deployed within the area of interest and emits a signal to compel handsets within its range to lock on to it. This stronger signal forces users within the controlled coverage area to register onto the IntelliJAM network while appearing to still be on the commercial network. Based on the IntelliJAM settings, wireless phone users in the controlled coverage area will either be approved and redirected to the commercial network for normal service, or they will be denied and will be unable to place or receive calls or text messages.


**Facility coverage within the mobile network**

Figure : From Tecore public web pages

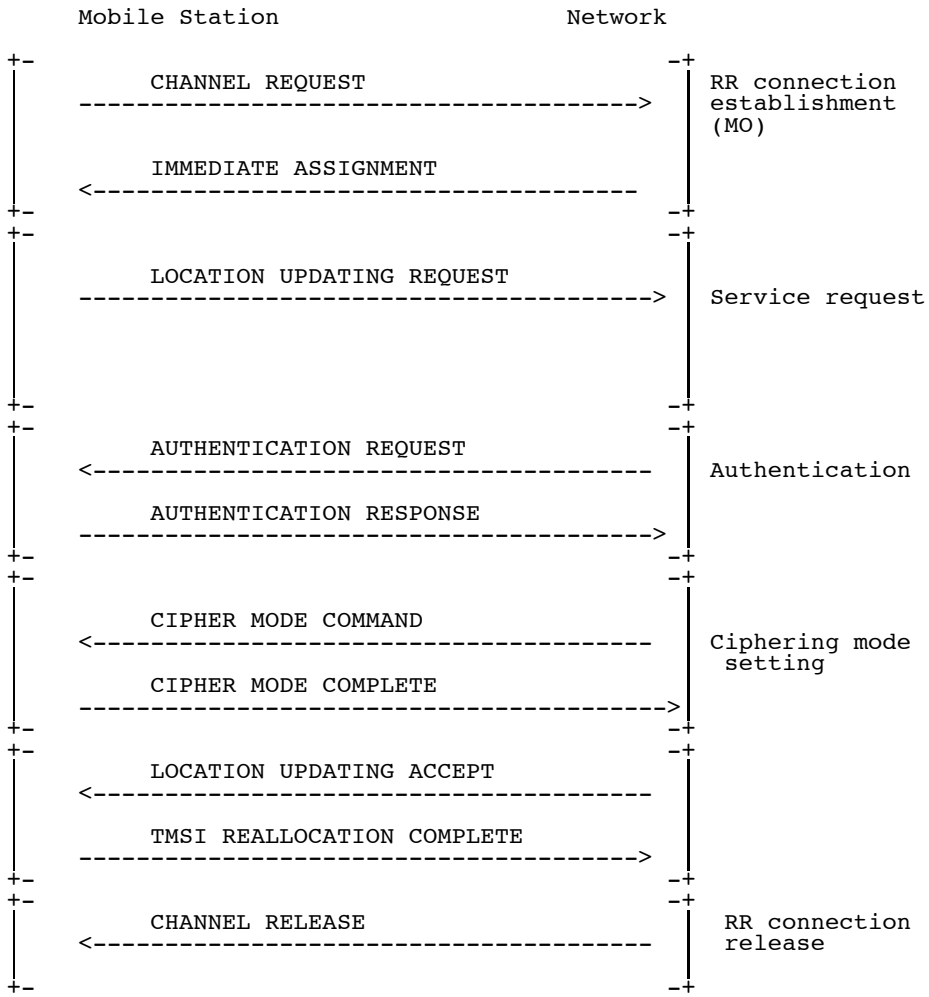
# Cell Selection Behavior

- “Capture” technique based on handset’s BTS selection rules, GSM 03.22 4 and GSM 04.08 4.2.
- Use the same MCC/MNC/NCC as the local GSM carrier.
- Choose an ARFCN from the serving cell’s neighbor list.
- Ramp up power gradually to avoid congestion.
- Can also use CRO to increase effective power advantage.

# Mobility Behavior

- Based on rules of GSM 04.08 4.
- When the handset enters a new “location area” it will attempt to register.
- So the IMSI-catcher advertises LAC different from any of the other cells in the area.
- Set timer T3212 for registrations on 6-minute intervals or change LAC to induce registration, like a broadcast ping to all camped handsets.

# Key Transaction – Location Update



# Location Update Options

- Location update request includes IMSI or TMSI of MS, plus MCC/MNC/LAC of previous serving cell.
- Authentication and ciphering are optional, so don't use them.
- Can request IMSI, TMSI or IMEI during update operation.
- Can assign a new TMSI.
- Can accept or refuse location update attempt *based on inspection of ID*.

# Accept/Reject Tricks

- If IMSI-catcher accepts registration, the handset remains camped to IMSI-catcher and ignores real network. DOS.
- Reject cause codes matter:

| | |
|---|---|
| illegal MS | locks handset until SIM is removed. |
| no roaming in LA | denies service *in any cell with the same LAC* until next time phone power-cycles. |
| IMSI not in VLR | kicks the phone back to the carrier with little or no disruption. |

# More Accept/Reject Tricks

- Send an “MM Information” message.
  - Set network name on the display.
  - Set the handset clock. (May allow smartphones to accept expired security certs, BTW.)
- Query the handset GPS receiver. (More on that later.)

# Boy-In-the-Middle

- Accept target handset registrations.
- Allow MO call attempts, using A5/0.
- Connect call with wireline phone or another GSM handset, as in EP1051053 figure.
- Suppress CLID in the PSTN.
- Collect both sides of the conversation.

# Man-In-the-Middle

- Accept target handset registrations
- Allow MO call attempts, using A5/0
- Connect call with wireline phone, VoIP carrier, ISDN or another GSM handset
- *Spoof* CLID in the PSTN
- Collect both sides of the conversation

# Covert Call – Technique

- Starts like a normal MT call setup, but user is never alerted.
- Connection in RR and MM, but no CC/Q.931 steps.
- Phone goes to an active TCH and transmits an idle pattern.
- Phone is assigned a known training sequence, unique on its ARFCN, to make tracking easier.
- BTS controls power and channel release, tracks timing advance for distance estimate.

# Covert Call – Applications

- Battery drain, by pushing tx power to maximum.
- Handset tracking via geoobservables.
  - Timing advance and measurement reports.
  - Midamble and idle pattern as markers for TOA & AOA estimation.

# IMSI-Catcher with Integrated Geolocation

## BTSGeo, an integrated BTS with Geolocation

BTSGeo enables **unique** capabilities and supersedes the accuracy and speed provided by Artemis. Proprietary and sensitive signal processing techniques empower the user with unsurpassed geolocation capabilities.

Figure : From MRT, Inc. public web pages

# Backhaul security

In classic GSM,

- design goal: provide same confidentiality/security as wired telephony
- wired telephony networks typically run without any encryption
- encryption is only on Um, i.e. between MS and BTS
- backhaul interface (Abis on BTS-BSC link) originally designed to run over E1
- backhaul between BTS and BSC has no encryption
- attacker requires physical access to E1 line in wired E1

# Backhaul security

Running A-bis backhaul over microwave

- E1 over microwave radio typically unencrypted (e.g. MINI-LINK)
- tuning into microwave links relatively easy
  - side-lobes of microwave antenna
  - propagation of signal beyond receiving antenna
  - main obstacle: proprietary coding/synchronization of microwave link
- passive eavesdropping of backhaul link provides easy option to full signalling and traffic

# The Subscriber Identity Module (SIM)

- Basic idea was to store cryptographic identity of subscriber inside smart card
- User can thus migrate identity from one device to another
- User can furthermore use different SIM in same device (e.g. local prepaid SIM while travelling)
- Original SIM card design mostly ISO 7816-4 filesystem and single command to execute A3/A8 algorithm inside card
  - This could even be done in logic, no processor required

# The modern SIM

The modern SIM is an entirely different beast

- Cryptographic processor smart card
  - Symmetric cryptography such as DES, 3DES, AES
  - Public key cryptography such as RSA, ECC
- Java Card including a small Java VM and Java RE
- Multiple application support
- Ability to download applications (Applets) into card

# SIM Application Toolkit (SAT)

- Ability for card to run applications that have UI on the phone
  - Display menu items on-screen
  - Get user input from keypad/touch-screen
- Described in TS 11.14 and 11.11

# SAT – Proactive SIM

The *Proactive SIM* features

- Sending a short message
- Setting up a voice call
- Playback of a tone in earpiece
- Providing location information from ME to SIM
- Have ME execute timers on behalf of SIM
- Sending DTMF to network
- Running an AT command received from SIM, sending result back to SIM
- Ask ME to launch browser to SIM-provided URL

# SAT – Call and SMS Control

- ME passes MO call setup attempts to SIM for approval
- SIM can then
  - approve or decline the MO call
  - modify the call details such as phone number
  - replace the call with USSD message
- ME passes USSD requests similar to Call Control
- Similar mechanism exists for all MO SMS

# SAT – Provide local information

The SIM can inquire the ME about

- MCC / MNC / LAC / Cell ID
- IMEI of ME
- Network Measurement Results
- BCCH channel list
- Date, Time, Timezone
- ME language setting
- Timing Advance

# SAT – Event download

The SIM is notified by ME about certain events such as

- Call Connected / Disconnected
- Location Status (Location Area change)
- User activity (keyboard input)
- Idle screen available
- Browser termination

# SAT - Data download

- Enables Operator to exchange arbitrary data with the SIM
- Could be RFM (Remote File Management)
  - Read or modify phone book entries
  - Even change the IMSI of the SIM (!)
- In case of Java Card, can be download of card applets
  - Applets are stored permanently on SIM
  - Can later use SAT procedures to interact with ME
  - TS 03.19 specifies Java API to access SAT from Java RE

# SAT - Data download

SAT Data Download can happen via

- via SMS or Cell Broadcast
  - Uses TS 03.40 TP-PID *SIM DATA Download*
  - ME forwards such SMS to the SIM in `ENVELOPE` APDU
  - Response from SIM is sent back as MO-SMS or DELIVERY REPORT
- via BIP (Bearer Independent Protocol)
  - Dedicated CSD call between network and SIM
  - GPRS session between network and SIM

# SAT - Data download

## Data download security

- GSM TS 03.48 specifies secure messaging for data download
- Includes replay protection
- Supports DES and 3DES
- SMS chaining for long commands / large data

# SIM card abuse by hostile operator

- Even if the phone might be considered trusted, the SIM card is owned and controlled by the operator
- Using SAT features, the operator can control many aspects of the phone
- Examples
  - Remotely reading address book / stored SMS
  - Monitor user behavior (browser termination, idle screen, ...)
  - Ask phone to establish packet data session

# SIM card re-programming by attacker

- If the SIM is not properly secured (auth + encryption keys, ...) a third party attacker can send SAT envelope SMS to the card and install resident Java applets
- The attacker can then
  - Obtain detailed location information and send it via SMS
  - Intercept/log outgoing calls
  - Sending copies of incoming + outgoing SMS elsewhere
- Even using SIM card channel to exploit baseband stack is feasible

# SIM card proxy / MITM by attacker

As soon as an attacker has temporary physical access to a phone, he can

- Insert a proxy-SIM between real SIM and phone
- Do everything a Java applet could do, but even with a securely configured SIM as he does not modify the existing SIM
- Sniff current Kc and send it out e.g. via SMS or even UDP/TCP packets over GPRS
- ... by only using standard interfaces that are common among all phones (as opposed to baseband software hacking which is very model-specific)

Most users would never notice this as they rarely check their SIM slot

# Defending against SIM based attacks

- SIM cards are Operator issued, Ki is on the SIM
  - SIM card can thus not be replaced, but original SIM must be used
- Configure telephone to not store contacts or SMS on SIM
- Communication between SIM and ME is not encrypted/authenticated
- Solution: Proxy SIM between SIM and ME to break STK / OTA
  - Filter all STK/OTA/Proactive commands like ENVELOPE
  - Indicate lack of STK support to ME (EF.Phase)

# Proxy SIM with firewall

- There are no known commercial products that implement STK/OTA filtering
- But there are a number of shim SIM cards that are plugged between SIM and SIM slot
- Most of them are used for SIM unlocking modern phones
- Some vendors produce freely (re)programmable proxy SIMs:

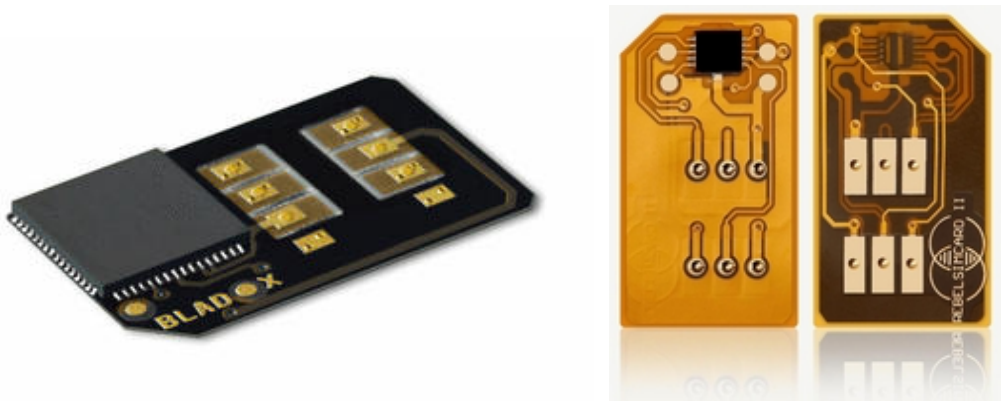



Figure : Bladox TurboSIM (AVR) and RebelSIM II (8051)

# Analyzing SIM toolkit applications is hard

- Regular end-user phone does not give much debugging
- SIM card itself has no debug interface for printing error messages, warnings, etc.
- However, as SIM-ME interface is unencrypted, sniffing / tracing is possible
- Commercial / proprietary solutions exist, but are expensive (USD 5,000 and up)
- Technically, sniffing smard card interfaces is actually very simple

# Introducing Osmocom SIMtrace

- Osmocom SIMtrace is a passive (U)SIM-ME communication sniffer
- Insert SIM adapter cable into actual phone
- Insert (U)SIM into SIMtrace hardware
- SIMtrace hardware provides USB interface to host PC
- `simtrace` host PC program encapsulates APDU in GSMTAP
- GSMTAP is sent via UDP to localhost
- wireshark dissector for GSM TS 11.11 decodes APDUs

# Osmocom SIMtrace Hardware