GSM SECURITY: FACT AND FICTION
BruCON 2010

Fabian van den Broek

Radboud University Nijmegen
Institute for Computing and Information Sciences (iCIS)

24 September 2010
Some Numbers

- $600 Billion
• $600 Billion
• 90% of population has coverage
• $600 Billion
• 90% of population has coverage
• 4.1 billion mobile users
• $600 Billion
• 90% of population has coverage
• 4.1 billion mobile users

But has GSM been properly tested?
Outline of this talk

• GSM overview
• GSM security
• Attacks
• Conclusion
GSM overview
Cellular technology
Cellular technology
Phone call routing
Phone call routing

- **MSC**
- **BSC**
- **BTS**

The diagram illustrates the structure of a mobile network, showing how calls are routed through base station controllers (BSCs) and base transceiver stations (BTSs) to manage call routing efficiently.
GSM system overview
GSM system overview
GSM system overview
Some important identifiers

- IMSI
- IMEI
- Phone number
- Secret key: Ki
GSM security
• Authentication
  • A3
  • A8
  • COMP128

• Encryption
  • A5/0
  • A5/1
  • A5/2
  • A5/3
GSM security

- Authentication
  - A3
  - A8
  - COMP128

- Encryption
  - A5/0
  - A5/1
  - A5/2
  - A5/3
GSM security

- Authentication
  - A3
  - A8
  - COMP128
- Encryption
  - A5/0
  - A5/1
  - A5/2
  - A5/3
GSM authentication
GSM authentication

AuC

IMSI -> (Ki,A3,A8)

MSC

GMSC

BSC

BTS

IMSI, Ki, A3, A8
GSM authentication

IMSI -> (Ki,A3,A8)
RAND = Random
SRES := A3(Ki,RAND)
Kc := A8(Ki,RAND)

(RAND, SRES, Kc)

IMSI, Ki, A3, A8
GSM authentication

IMSI -> (Ki, A3, A8)
RAND = Random
SRES := A3(Ki, RAND)
Kc := A8(Ki, RAND)

(RAND, SRES, Kc)

RAND

MSC

BSC

BTS

IMSI, Ki, A3, A8

GMSC

AuC
GSM authentication

IMSIE -> (Ki, A3, A8)
RAND = Random
SRES := A3(Ki, RAND)
Kc := A8(Ki, RAND)

(RAND, SRES, Kc)

MSC

AuC

GMSC

BSC

BTS

SRES := A3(Ki, RAND)
Kc := A8(Ki, RAND)
IMSI, Ki, A3, A8
GSM authentication

IMSI -> (Ki, A3, A8)
RAND = Random
SRES := A3(Ki, RAND)
Kc := A8(Ki, RAND)

(RAND, SRES, Kc)

MSC

AuC

GMSC

BSC

SRES := A3(Ki, RAND)
Kc := A8(Ki, RAND)

IMSI, Ki, A3, A8
GSM Encryption

The diagram illustrates the GSM encryption process involving several key components:

- **MSC (Mobile Switching Center)**
- **BSC (Base Station Controller)**
- **BTS (Base Transceiver Station)**
- **AuC (Authentication Center)**
- **GMSC (Gateway Mobile Switching Center)**

The diagram shows how encryption keys (Kc) are used in the communication between these components, ensuring secure data transmission.
GSM Encryption

The diagram illustrates the GSM Encryption system, where

- MSC (Mobile Switching Center) is the central node.
- BSC (Base Station Controller) connects to BTS (Base Transceiver Station).
- BTSs are connected to the BSCs and provide the interface between the landline network and the mobile devices.
- The encryption keys (Kc1 and Kc2) are used at the BTS level to protect the communication between the BSC and the mobile devices.
GSM Encryption
Attacks
Attack 1: Eavesdropping
1. Capture bursts
2. Decrypt captured bursts
3. Interpret decrypted bursts
3: Interpret decrypted bursts

You have several options here:

- GSMDecode (AirProbe)
- WireShark
- OpenBTS / OpenBSC
2: Decrypt captured bursts

Release the Kraken!
• Reverse engineered in 1994
• Academic breaks
• Time-Memory-Trade-Off attacks
• Currently:
  • Berlin set & Kraken
Capture a burst  
“Guess” contents  
Compute keystream  
Look-up corresponding session key
1: Capture burst

USRP + GNU Radio + AirProbe

Receive Channel RF Interface
Altera FPGA
Transmit Channel RF Interface
DC Power
USB 2.0 Port
Analog Devices Mixed Signal Processor
The Um interface
Frequency band
An example cell
No Frequency hopping
Frequency hopping
Frequency hopping
Message Sequence
Message Sequence

Paging

Request channel

Assign channel
Message Sequence

Paging

Request channel

Assign channel

exchange info
Message Sequence

Paging
---
Request channel
Assign channel
Exchange info
Start Ciphering
Ciphering started

BTS
Message Sequence

Paging
Request channel
Assign channel
exchange info
Start Ciphering
Ciphering started
exchange info
Message Sequence

Paging

Request channel

Assign channel

exchange info

Start Ciphering

Ciphering started

exchange info

Ass. speech chn.

Conversation
Hopping Problem
Attack 2: the MITM attack
The Man-In-The-Middle Attack

Paging
Request channel
Assign channel
exchange info
Start Ciphering
Ciphering started
exchange info
Ass. speech chn.
Conversation
The Man-In-The-Middle Attack

Paging

Request channel

Assign channel

Exchange Info

Start Ciphering A5/x

Start Ciphering A5/2

Ciphering started

exchange info

Ass. speech chn.

Conversation

Ciphering started

exchange info

Ass. speech chn.

Conversation
The Man-In-The-Middle Attack

Ingredients:

- BTS: OpenBTS / OpenBSC
- Phone: OsmocomBB

Problems:

- Hopping problem
- Time window
- Detectable
Just link OpenBTS to Asterisk

Downsides:

- No incoming calls
- Calling number obscured

Upside:

- It already works
MITM the easy way

Just link OpenBTS to Asterisk

Downsides:
- No incoming calls
- Calling number obscured

Upside:
- It already works
Yet another way

A sort of hybrid attack between MITM and eavesdropping

1. Capture challenge
2. Capture conversation
3. Fake BTS attack with challenge
Some other attacks
Other attacks

- IMSI catchers
- Attacks on other parts of the network
- Nokia 1100
- Locations revealed
- DoS attacks
There's hope still

GSM was 2G

3G uses mutual authentication

4G might use AES
What can you do now?

GSM will be around for a long time.

- Use **solely** 3G
- Use crypto solutions
Conclusions
• Eavesdropping, full-MITM and hybrid still need work
• Easy-MITM works
• Many other attacks are possible
The weakest link is probably your phone!

See The Monkey Steals the Berries
The weakest link is probably your phone!

See The Monkey Steals the Berries
References

USRP www.ettus.com
GNU Radio http://gnuradio.org/
OpenBTS http://openbts.sourceforge.net/
OpenBSC
http://openbsc.osmocom.org/trac/wiki/OpenBSC
AirProbe
https://svn.berlin.ccc.de/projects/airprobe/wiki
A5/1, Kraken http://www.reflextor.com/trac/a51
OsmocomBB http://bb.osmocom.org/trac/