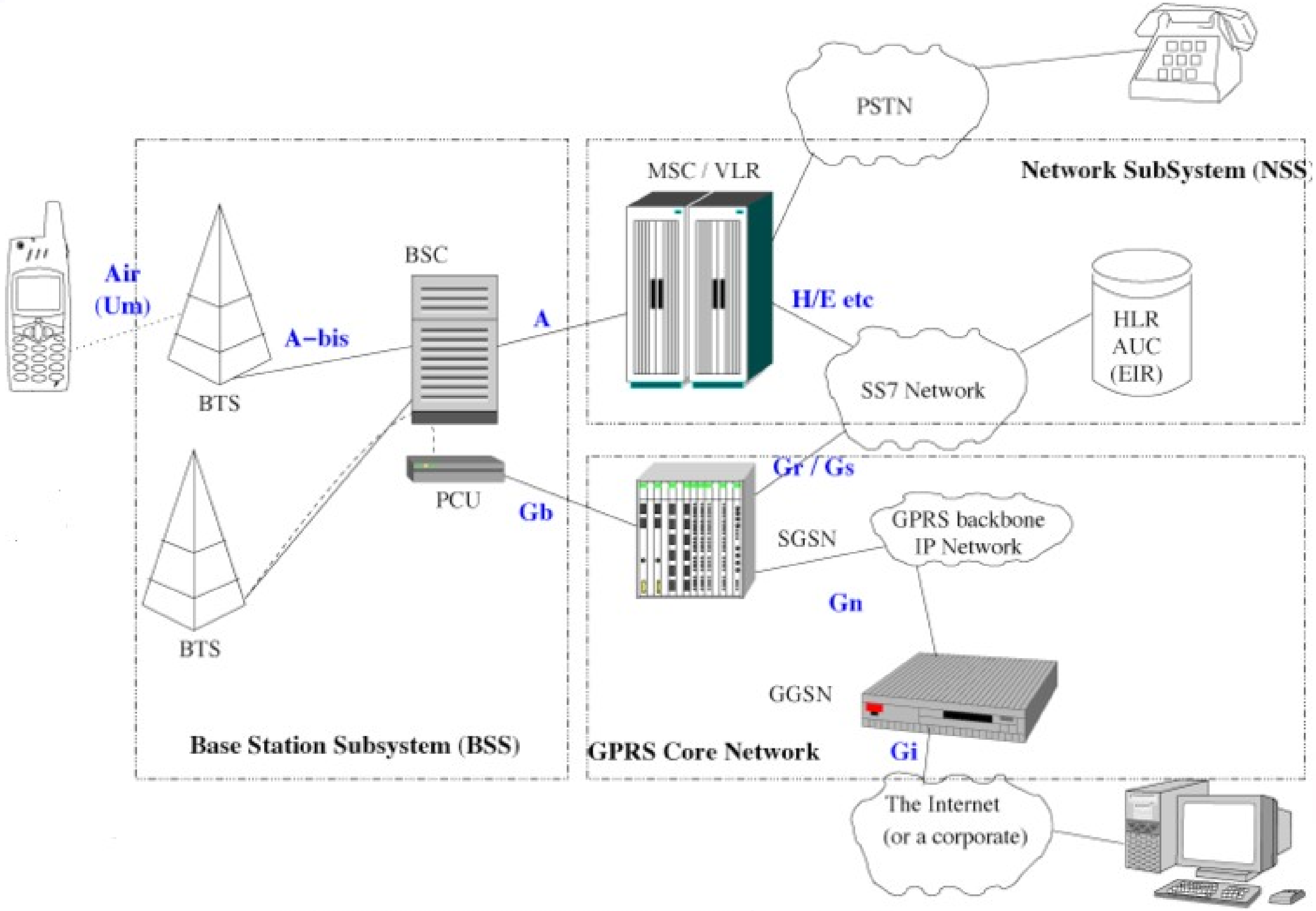
Intercepting GSM traffic

Agenda

- Receiving GSM signals
- Security
- Cracking A5/1

GSM Network


PSTN
Network SubSystem (NSS)
MSC / VLR
BSC
Air
(Um)
A−bis
A
H/E etc
HLR
AUC
(EIR)
SS7 Network
BTS
PCU
Gb
Gr / Gs
SGSN
GPRS backbone
IP Network
Gn
BTS
GGSN
Base Station Subsystem (BSS)
GPRS Core Network
Gi
The Internet
(or a corporate)

BTS

Camouflage BTS

Summary GSM

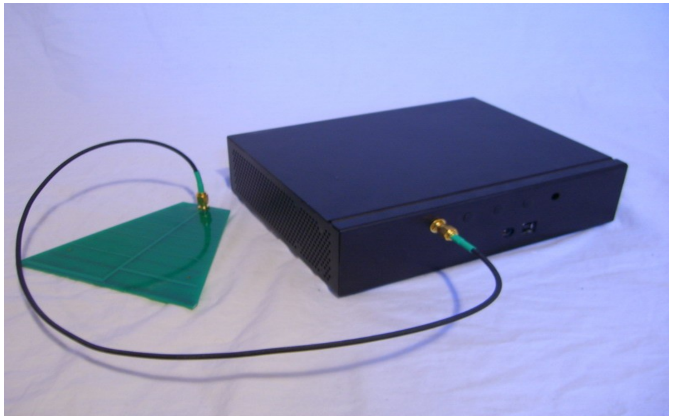
- GSM is old
- GSM is big
- GSM / 3G / UMTS / EDGE / WCDMA / .
- Base stations all over the place

Receiving

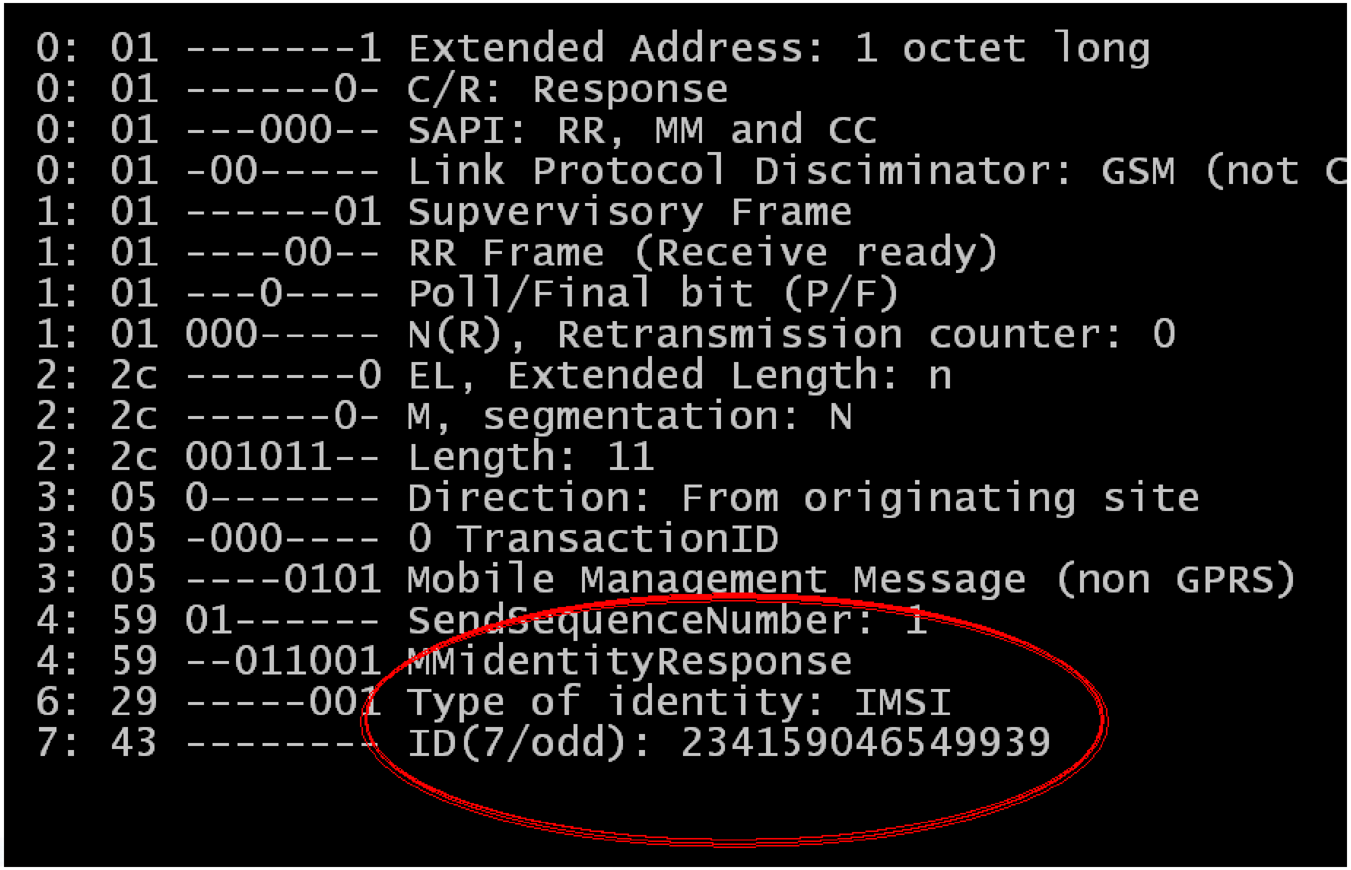
- Nokia 3310 / Ericsson / TSM
- USRP
- TI's OMAP dev kit
- Commercial Interceptor

ERICSSON

TEXAS INSTRUMENTS

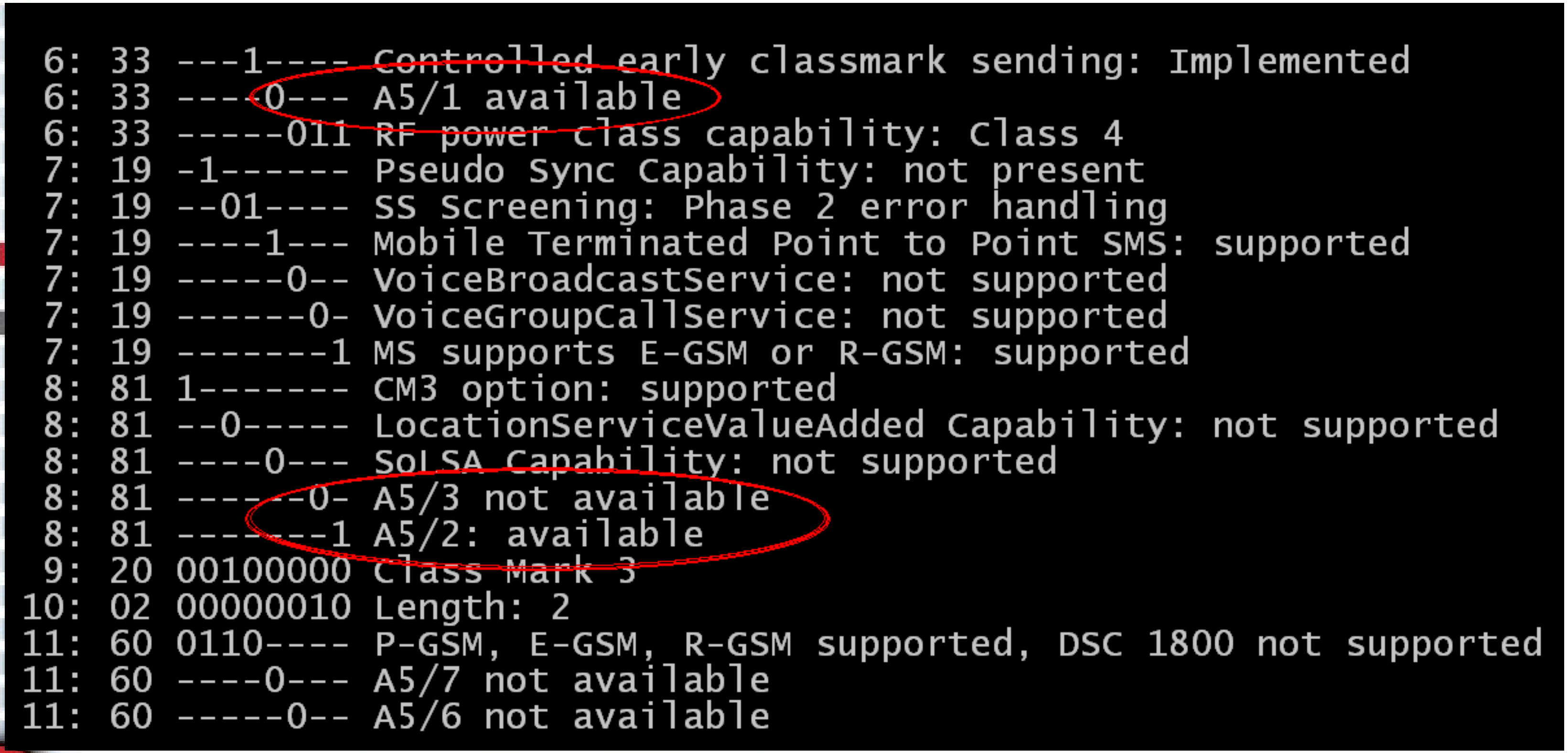


Example 1



```
0: 01 -------1 Extended Address: 1 octet long
0: 01 ------0- C/R: Response
0: 01 ---000-- SAPI: RR, MM and CC
0: 01 -00----- Link Protocol Disciminator: GSM (not C
1: 01 ------01 Supvervisory Frame
1: 01 ----00-- RR Frame (Receive ready)
1: 01 ---0---- Poll/Final bit (P/F)
1: 01 000----- N(R), Retransmission counter: 0
2: 2c -------0 EL, Extended Length: n
2: 2c ------0- M, segmentation: N
2: 2c 001011-- Length: 11
3: 05 0------- Direction: From originating site
3: 05 -000---- 0 TransactionID
3: 05 ----0101 Mobile Management Message (non GPRS)
4: 59 01------ SendSequenceNumber: 1
4: 59 --011001 MMidentityResponse
6: 29 -----001 Type of identity: IMSI
7: 43 -------- ID(7/odd): 234159046549939
```

Example 2

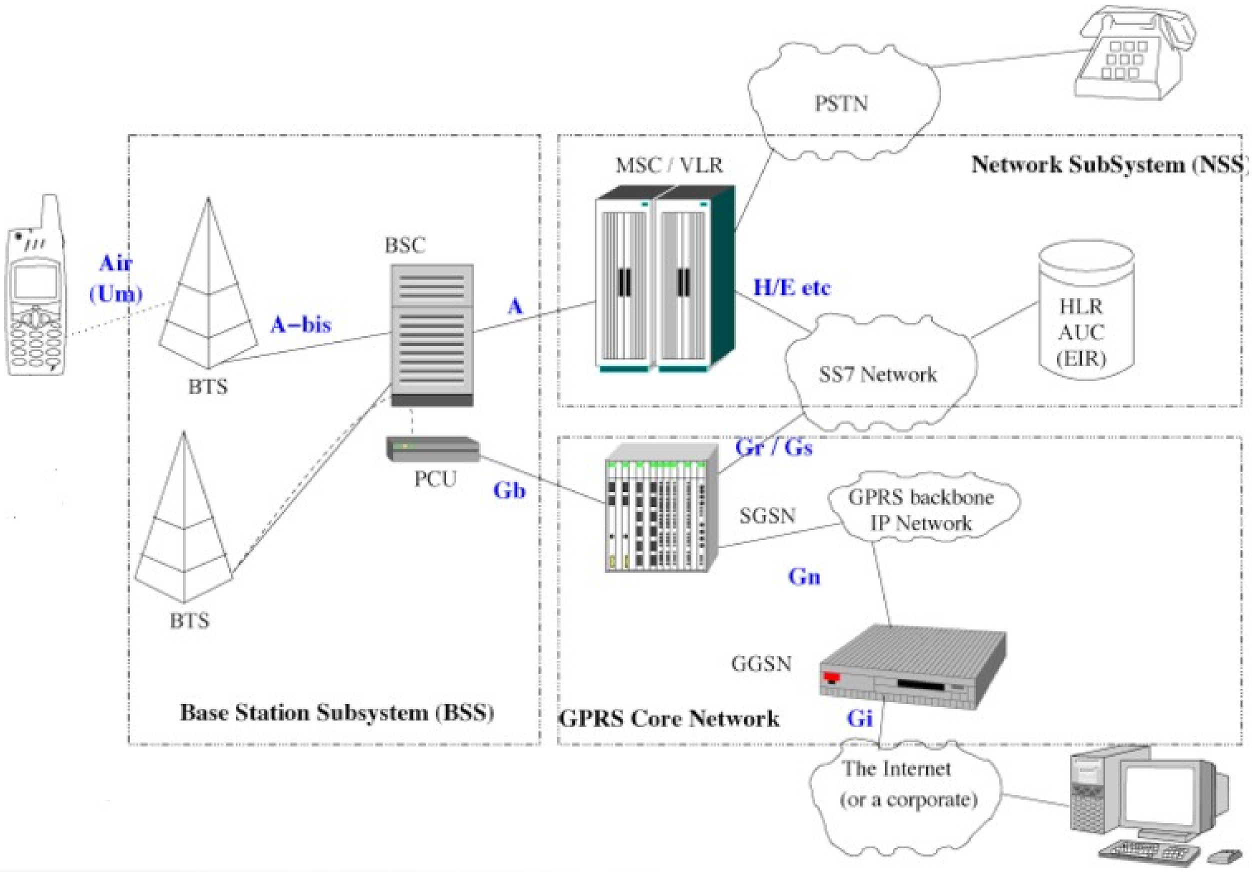


```
 6: 33 ---1---- Controlled early classmark sending: Implemented
 6: 33 ----0--- A5/1 available
 6: 33 -----011 RF power class capability: Class 4
 7: 19 -1------ Pseudo Sync Capability: not present
 7: 19 --01---- SS Screening: Phase 2 error handling
 7: 19 ----1--- Mobile Terminated Point to Point SMS: supported
 7: 19 -----0-- VoiceBroadcastService: not supported
 7: 19 ------0- VoiceGroupCallService: not supported
 7: 19 -------1 MS supports E-GSM or R-GSM: supported
 8: 81 1------- CM3 option: supported
 8: 81 --0----- LocationServiceValueAdded Capability: not supported
 8: 81 ----0--- SoLSA Capability: not supported
 8: 81 ------0- A5/3 not available
 8: 81 -------1 A5/2: available
 9: 20 00100000 Class Mark 3
10: 02 00000010 Length: 2
11: 60 0110---- P-GSM, E-GSM, R-GSM supported, DSC 1800 not supported
11: 60 ----0--- A5/7 not available
11: 60 -----0-- A5/6 not available
```

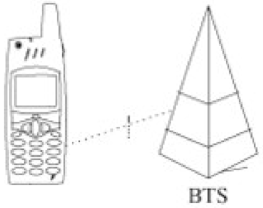
Summary Receiving

- It's cheap
- It's easy
- It's getting easier

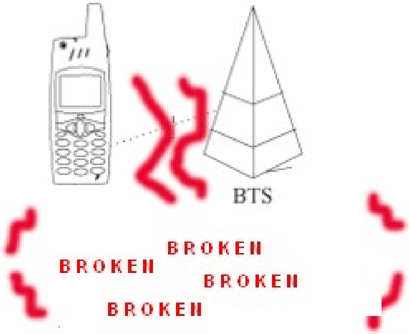
Security


PSTN
Network SubSystem (NSS)
MSC / VLR
Air
(Um)
BSC
A
H/E etc
HLR
AUC
(EIR)
A–bis
BTS
SS7 Network
Gr / Gs
PCU
Gb
SGSN
GPRS backbone
IP Network
Gn
BTS
GGSN
Base Station Subsystem (BSS)
GPRS Core Network
Gi
The Internet
(or a corporate)

Security



Security



Commercial Interception

- Active Equipment:
  - – $70k - $500k. Order via internet.
- Passive Equipment:
  - – $1M

Radio Security

- A5/0, A5/2, A5/1. All broken in 1998.
- Some algorithms proprietary
- IMSI / Location Information clear-text
- Key is artificially weakened
- Key material is reused
- No indication to user
- Key Recovery Systems available

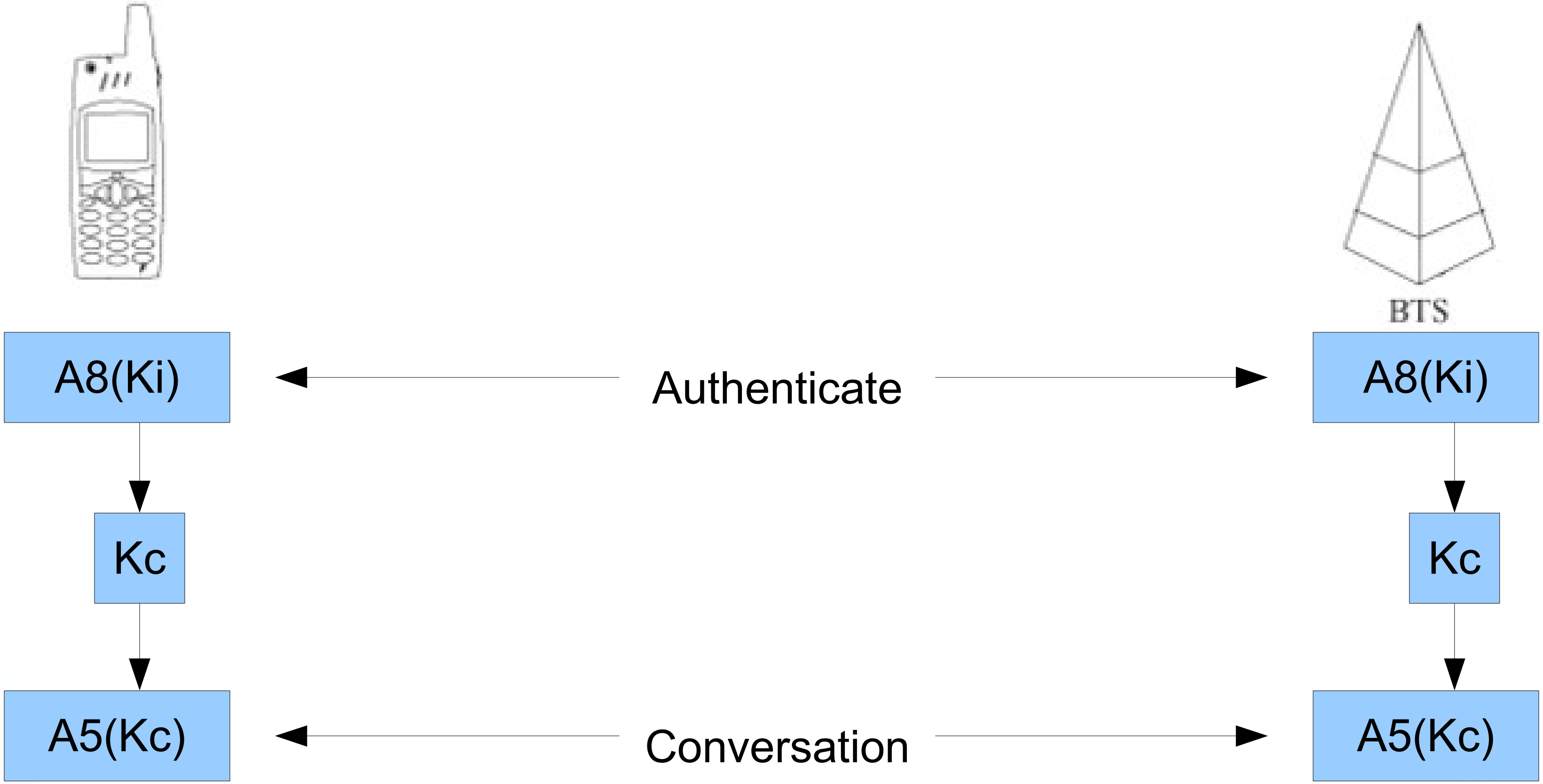
SIM Toolkit

- There is a JVM on your SIM!
- The Operator can install programs via OTA (== remotely, without you knowing)
- Scary standard: Invisible flags, binary updates, call-control, proprietary, ...

Security Summary

- None

A5/1 Cracking



A8(Ki)

Authenticate

A8(Ki)

Kc

Kc

A5(Kc)

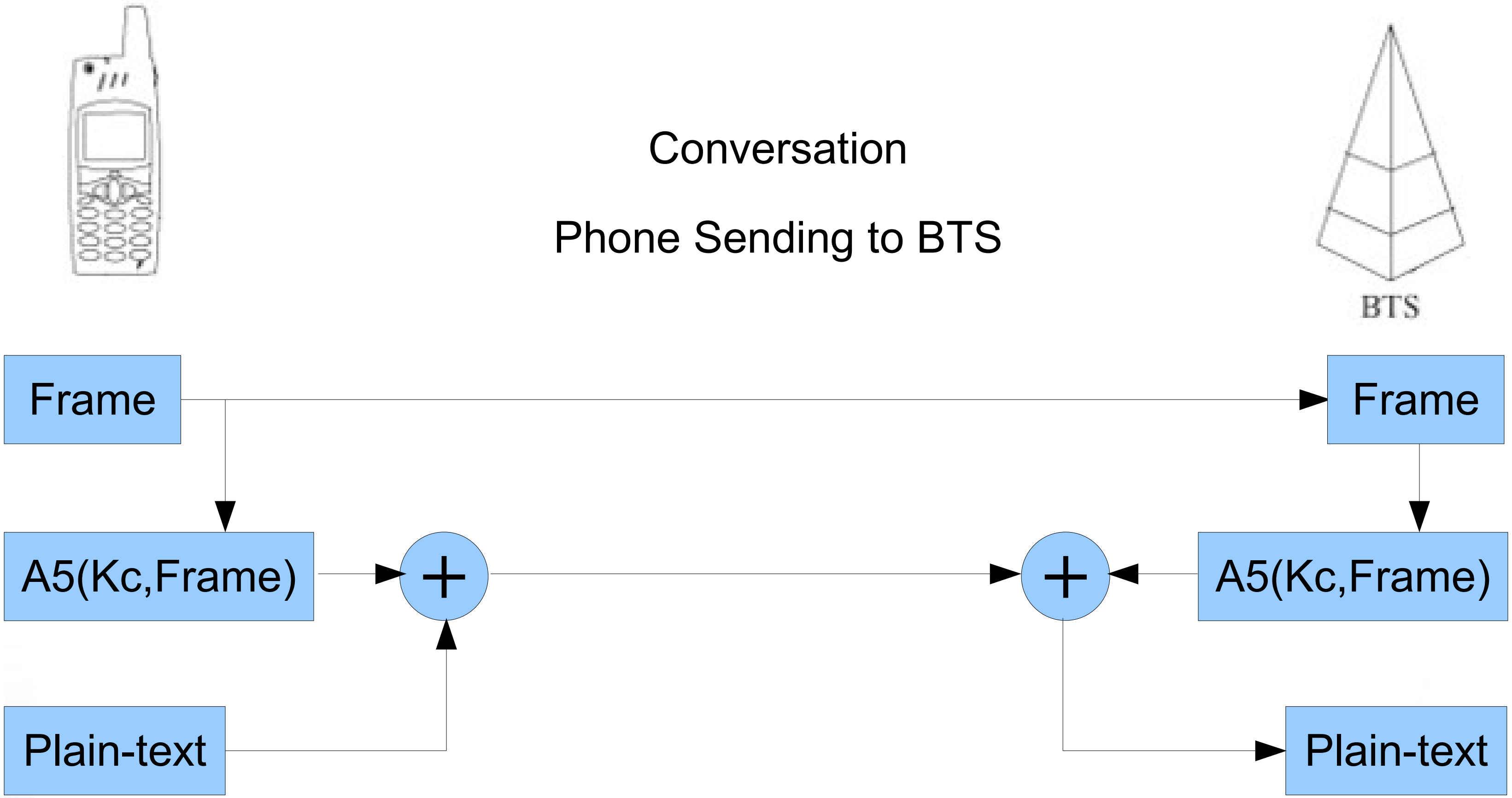
Conversation

A5(Kc)

A5/1 Cracking

Conversation

Phone Sending to BTS



Frame

A5(Kc,Frame)

+

Plain-text

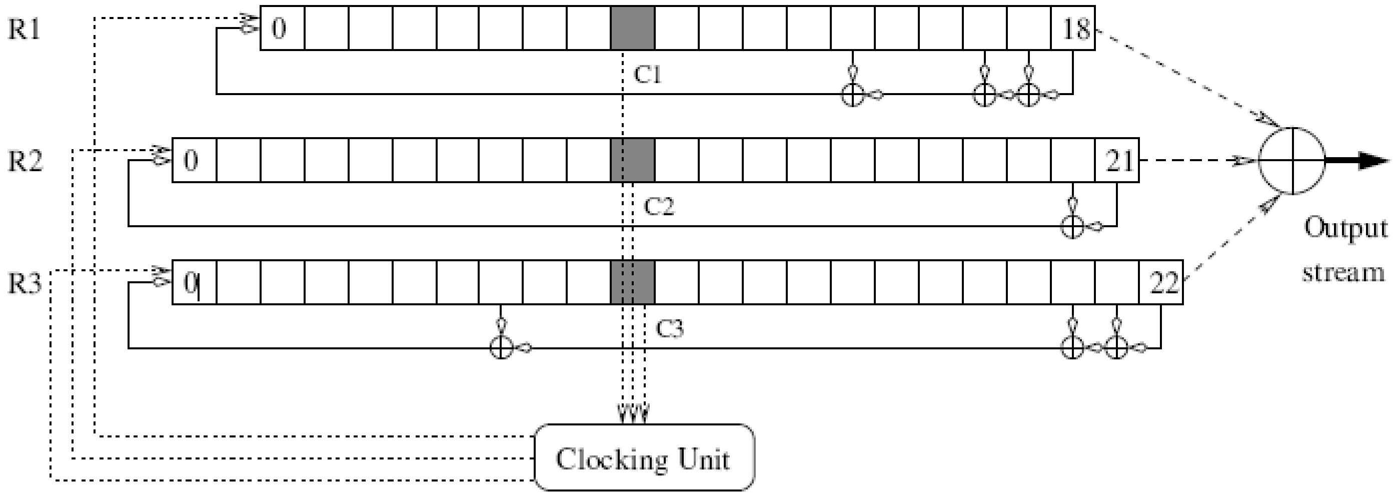
Frame

A5(Kc,Frame)

+

Plain-text

A5/1 Cracking



- Clock in 64-bit Kc and 22-bit frame number
- Clock for 100 cycles
- Clock for 114 times to generate 114-bits

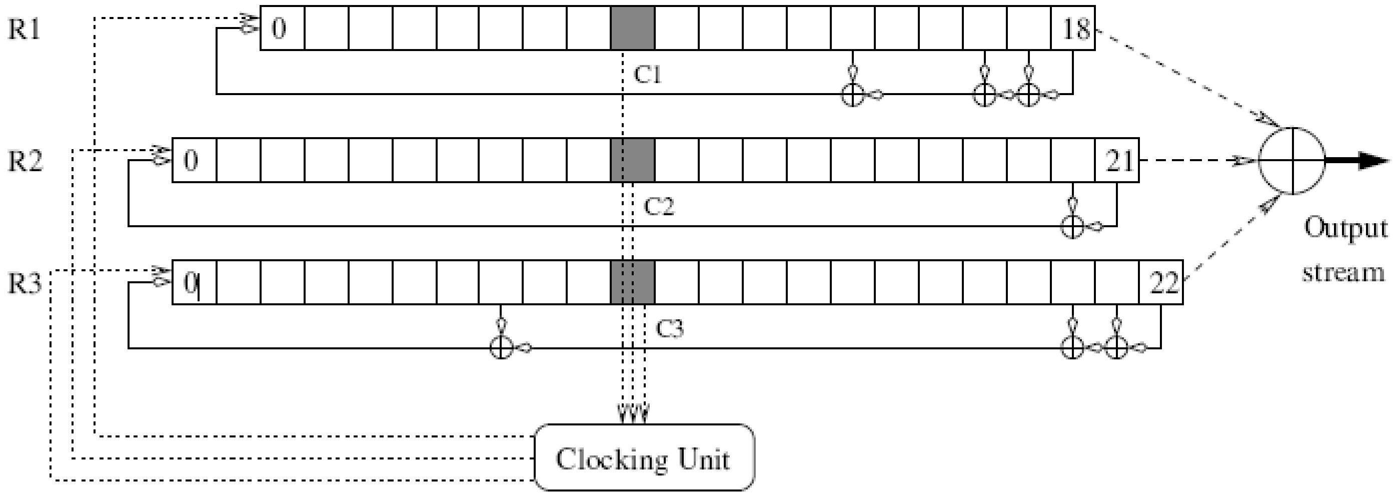
Cracking A5/1

- Other attacks are academic BS.
- 3-4 Frames. Fully passive.
- Combination of Rainbow Table attack and others.

Cracking A5/1

- 4 frames of known-plaintext
- A5/1 is a stream cipher
- We can derive 4 frames of keystream output

Sliding Window



[0|1|1|0|1|0…………………………………………|1|0|1|1]

[64 bit Cipherstream 0 ……….]

[64 bit Cipherstream 1 ………...]

[64 bit Cipherstream 2 ...………]

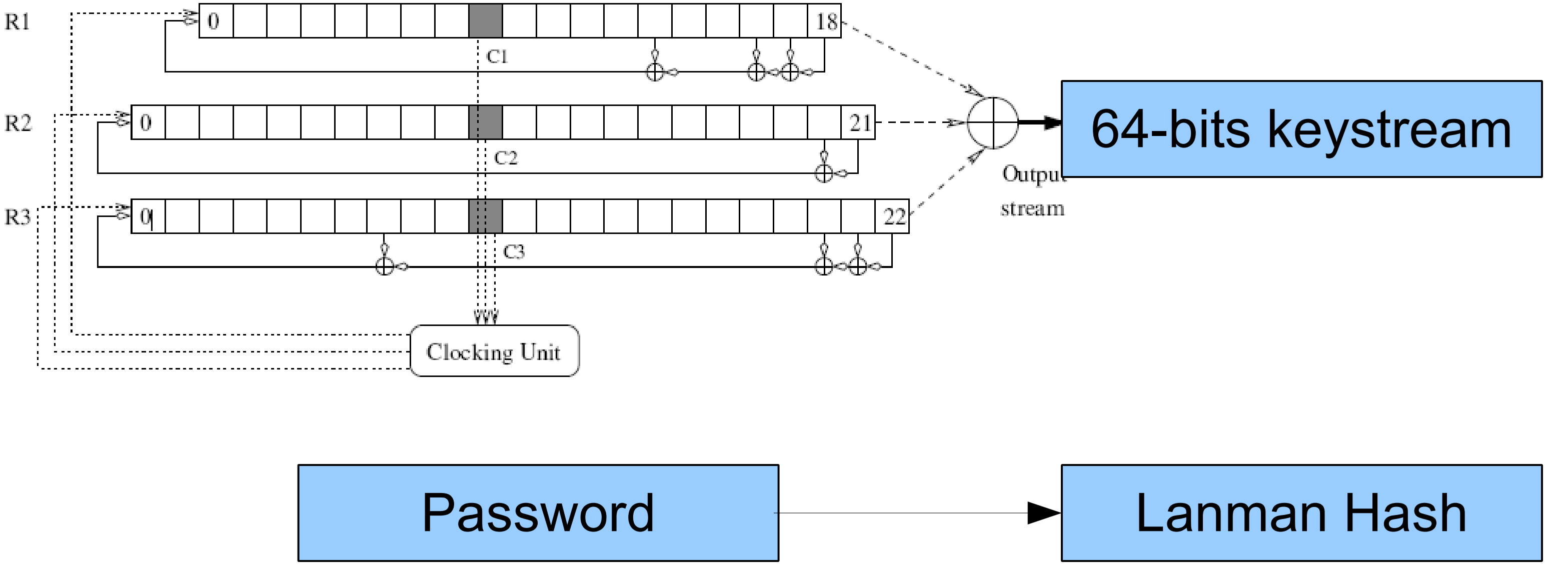
……………………………

[64 bit Cipherstream 50 …………]

Sliding Window

- Total of 4 frames with 114-bits
- 114 – 64 + 1 = 51 keystreams per frame
- 51 x 4 frames = 204 keystreams total

Rainbow Table



64-bits keystream

Password

Lanman Hash

Rainbow Table

- Build a table that maps 64-bits of keystream back to 64-bits of internal A5/1 state
- 204 data points means we only need 1/64th of the whole keyspace
- 2^{58} = 288,230,376,151,711,744
- About 120,000 times larger than the largest Lanman Rainbow Table

How do we do this??

- 1 PC
  - 550,000 A5/1's per second
  - 33,235 years
- Currently using 68 Pico E-16 FPGAs
  - 72,533,333,333 A5/1's per second
  - 3 months
- Building new hardware to speed this up

Hardware

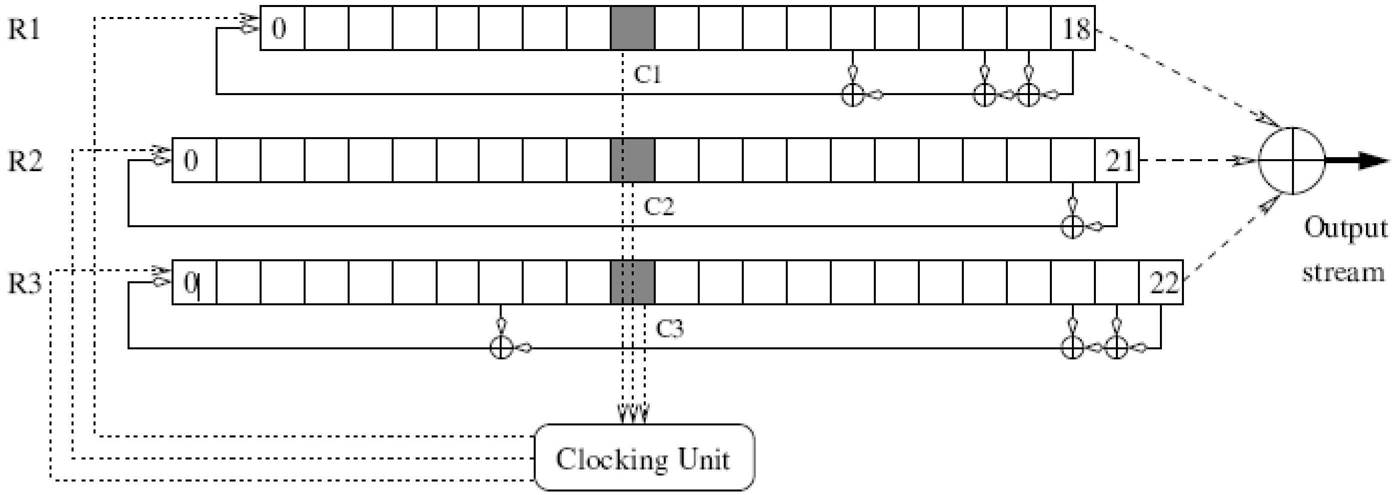
Rainbow Table

- Cheap Attack (~30 min)
  - 6 350GB Hard Drives (2TB)
  - 1 FPGA (or a botnet)
- Optimal Attack (~30 sec)
  - 16 128GB Flash Hard Drives (2TB)
  - 32 FPGAs
  - Can speed it up with more FPGAs

Rainbow Table

- 204 data points will give us 204 / 64 = 3 A5/1 internal states
- So what do you do now?

Reverse Clocking



- Load A5/1 internal state
- Reverse clock with known keystream back to after Kc was clocked in
- Will resolve to multiple possible A5/1 states

Reverse Clocking

- Reverse all 3 A5/1 internal states
- The common state will be the correct one
- Use the internal state and clock forward to decrypt or encrypt any packet
- Can solve linear equations to derive key
- But isn't really necessary

Conclusions

- Tables will be finished in March
- Commercial version in Q2/08
- Will be scalable to whatever decryption time period is required

Threats & Future

- GSM security has to become secure.
- Data/Identity theft, Tracking
- Unlawful interception
- Attacks on GSM Infrastructure
- Receiving and cracking GSM will become cheaper and easier

Thank You!

- Steve
  - http://wiki.thc.org/gsm
- David Hulton
  - http://www.picocomputing.com
  - http://www.openciphers.org
- Questions?