Cracking GSM

Security Researcher
Cellcrypt Limited

Introduction

- Cellcrypt
  - UK security software company
  - End-to-end encrypted voice calls over IP
- We know GSM is not secure
- Others also know
  - “The GSM Software Project”
  - An independent public group
  - Working to demonstrate the need for improved GSM security

The GSM Software Project

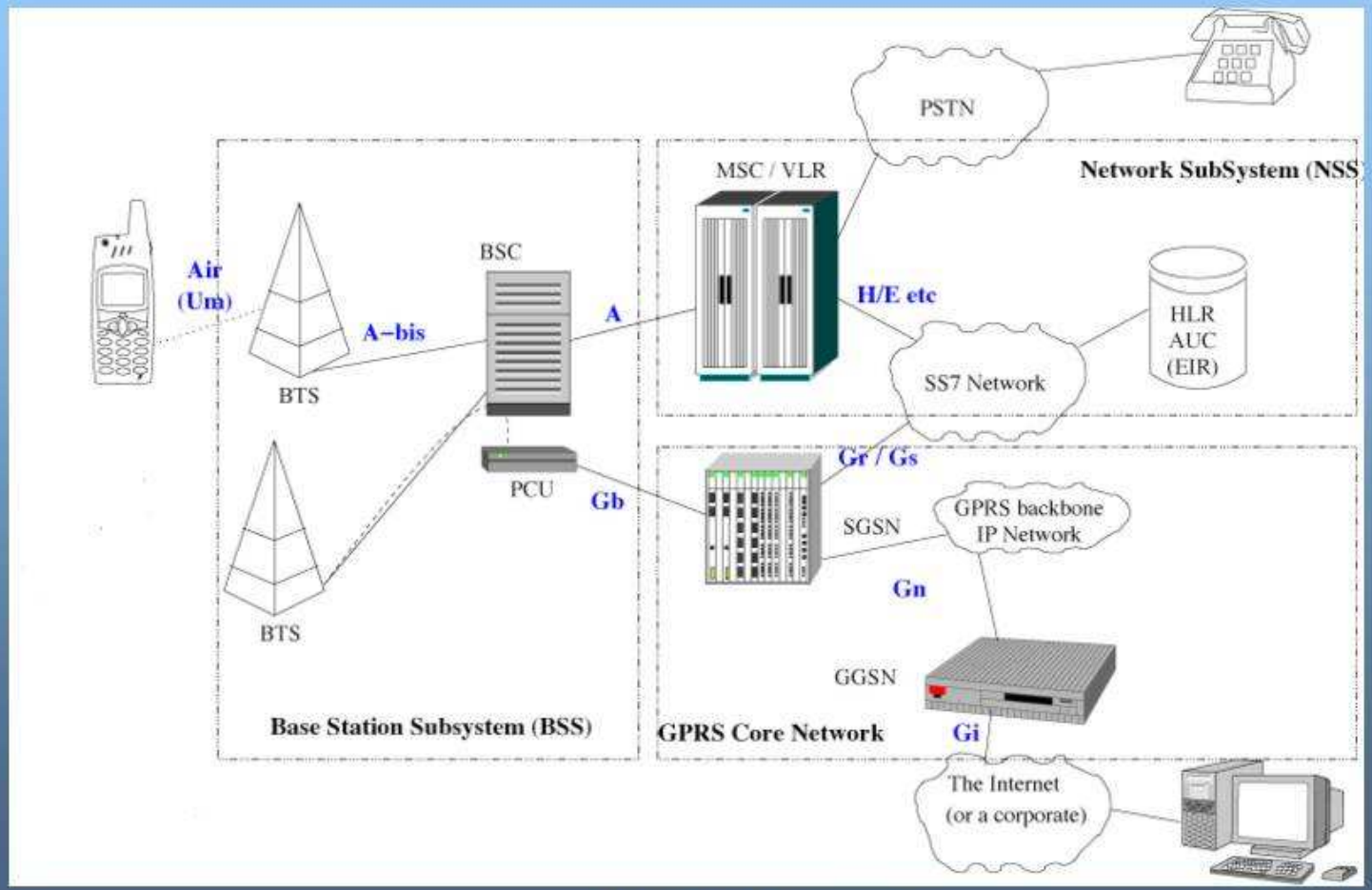
- Objectives of the project
- What the project will do
- An open public project

http://wiki.thc.org/gsm Page 3

Agenda

- Capturing GSM frames
- Security in GSM
- Cracking A5/1

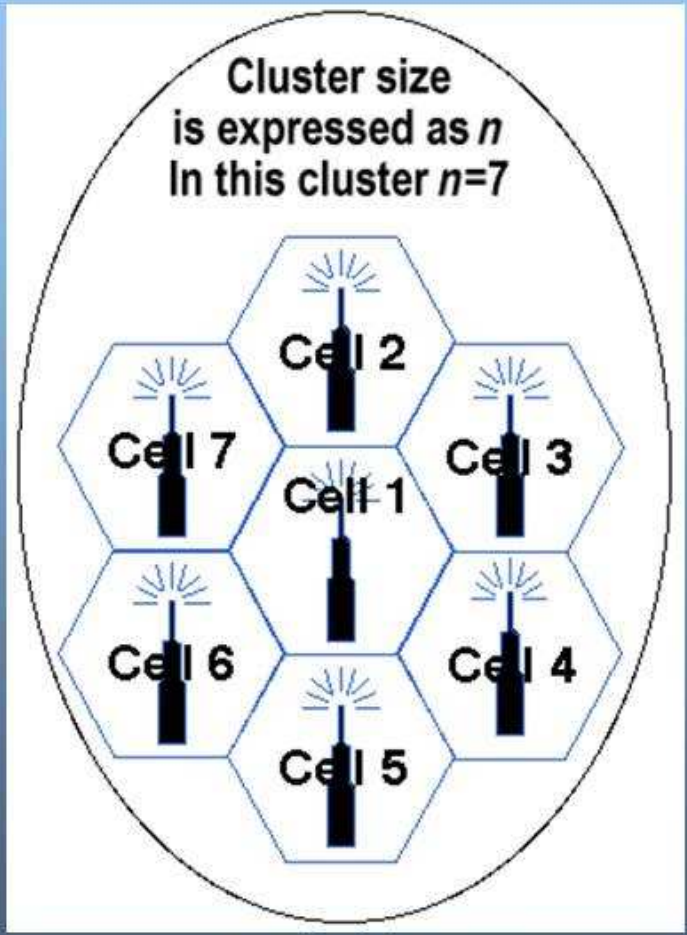
GSM Network



http://wiki.thc.org/gsm

Page 4

Cell Structure



http://wiki.thc.org/gsm

Page 5

BTS

http://wiki.thc.org/gsm

Page 6

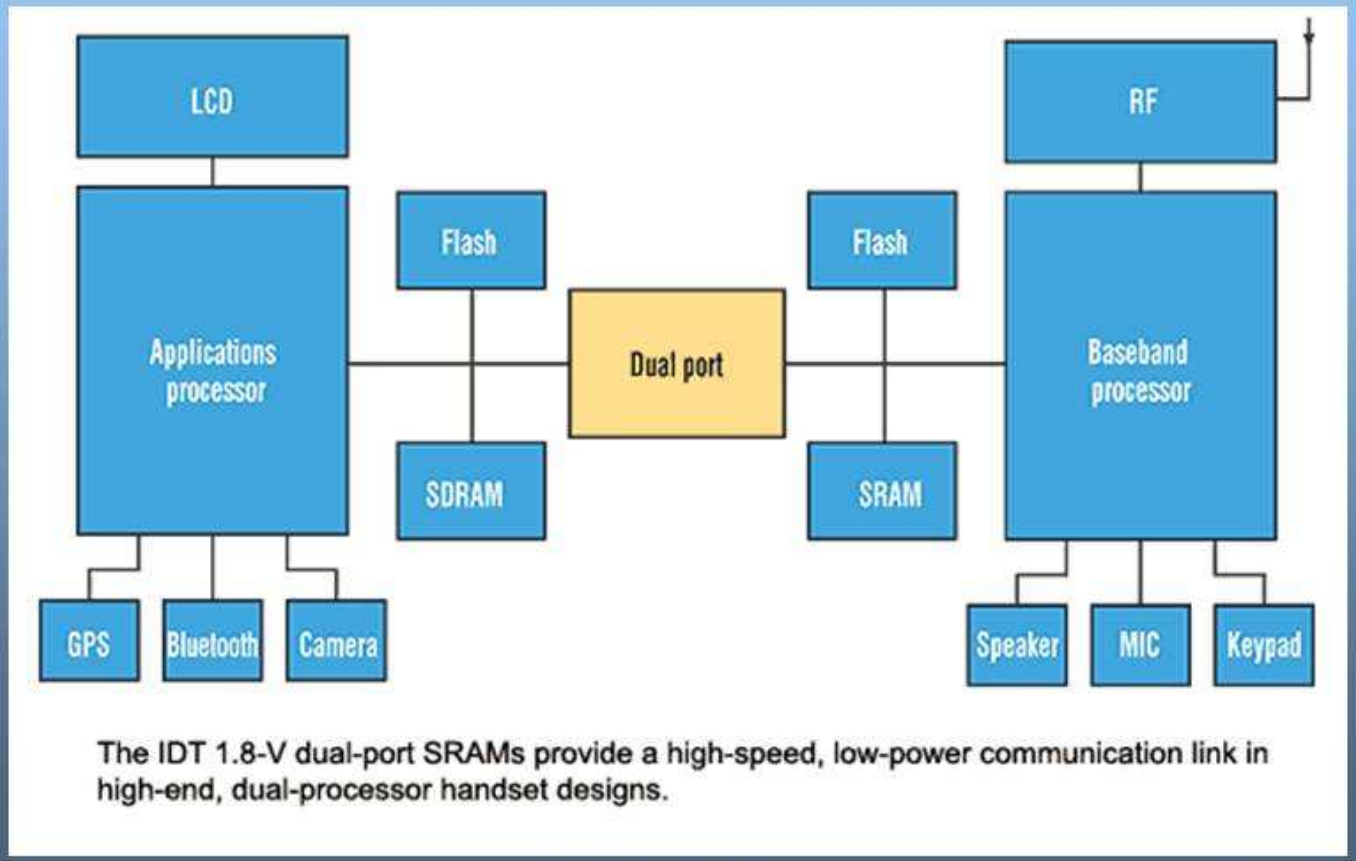
Camouflage BTS

http://wiki.thc.org/gsm Page 7

Summary: GSM

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

Phone Internals



The IDT 1.8-V dual-port SRAMs provide a high-speed, low-power communication link in high-end, dual-processor handset designs.

Capturing GSM Frames

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

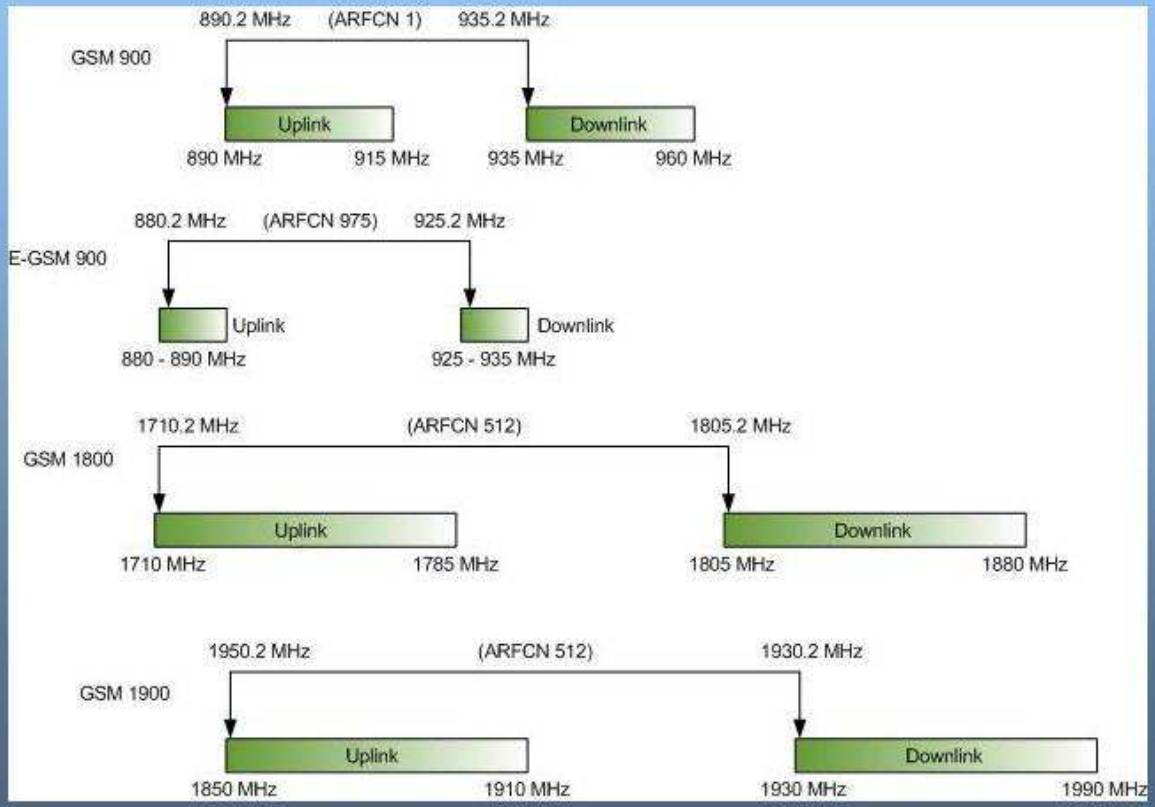
ERICSSON

TEXAS INSTRUMENTS

http://wiki.thc.org/gsm

Page 10

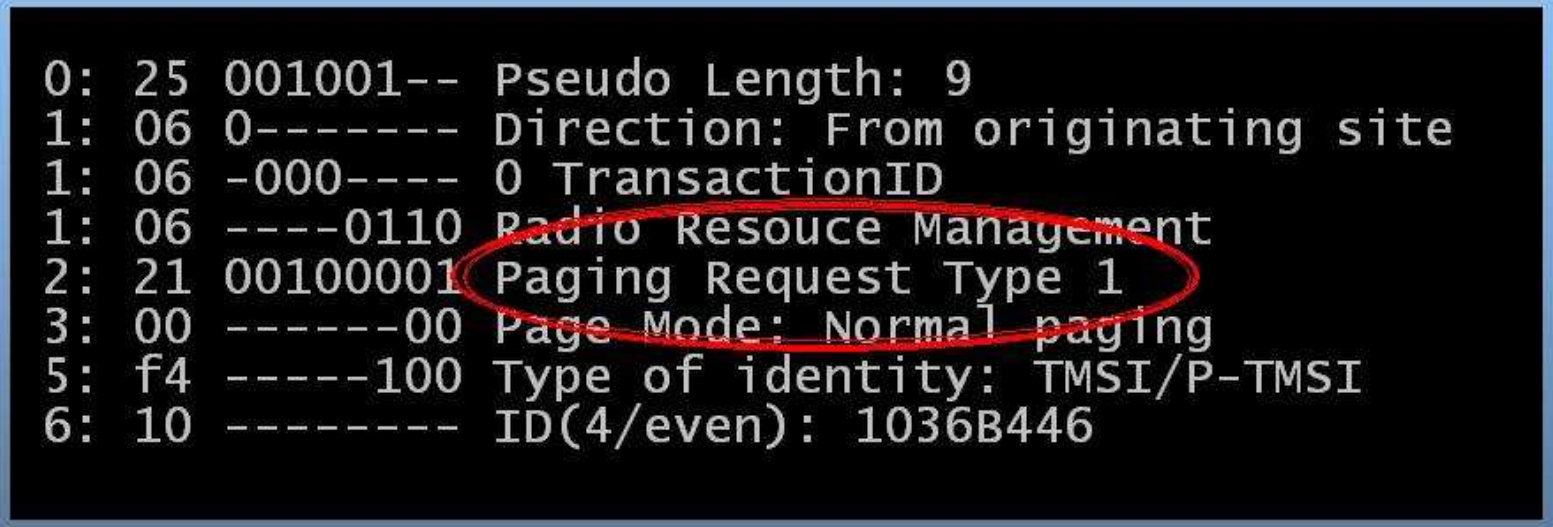
Absolute Radio Freq Number

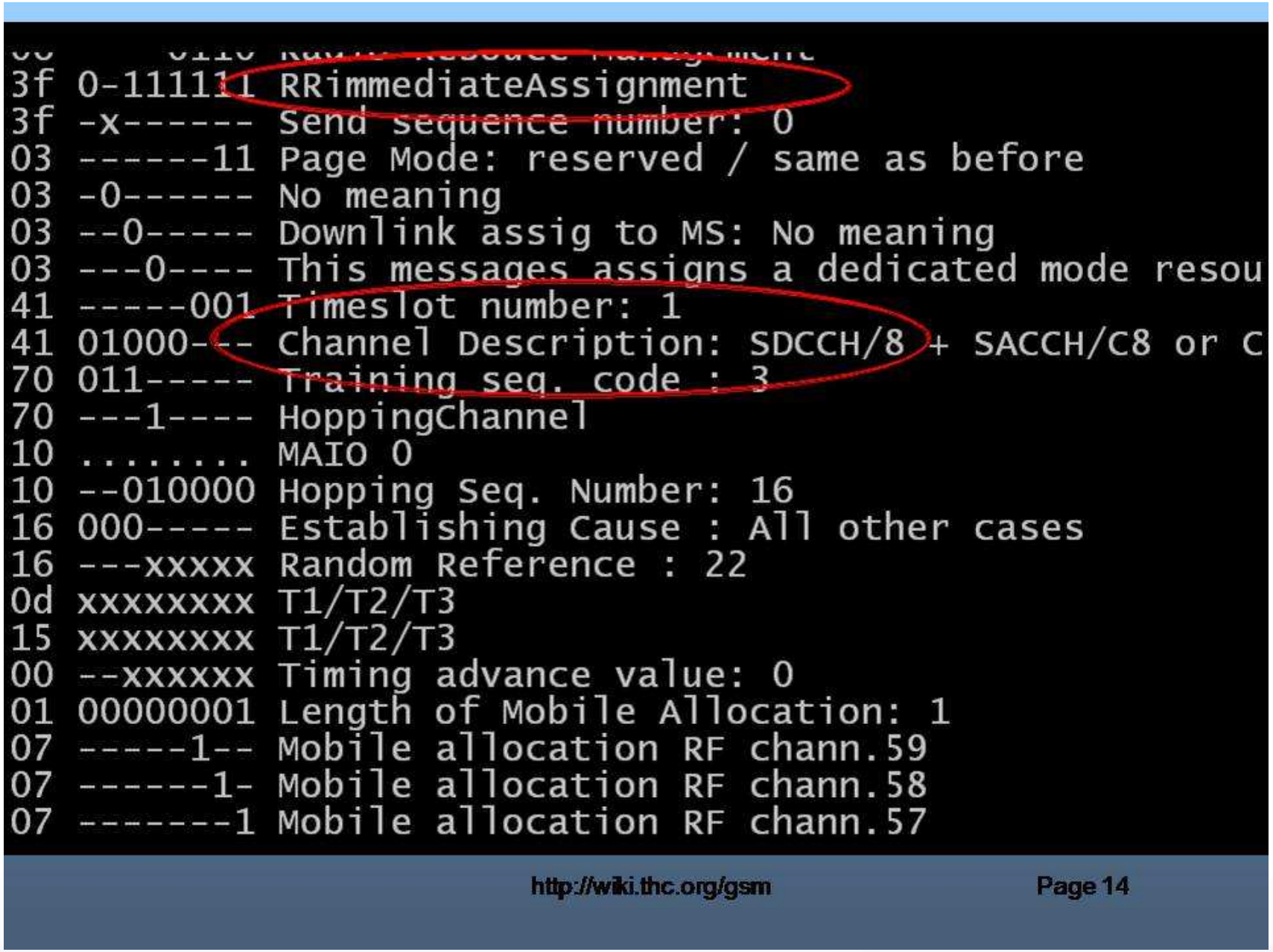


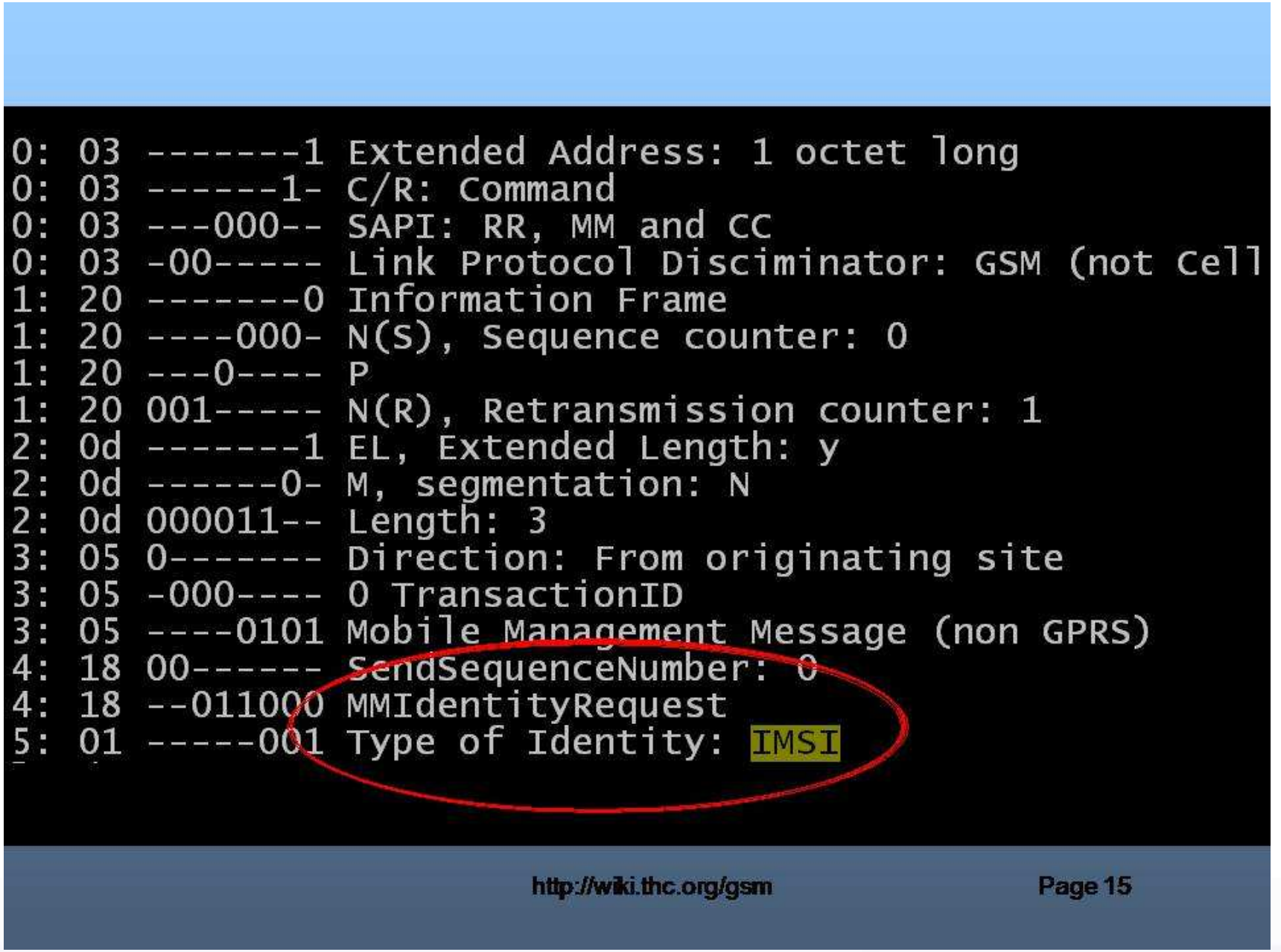
http://wiki.thc.org/gsm Page 11

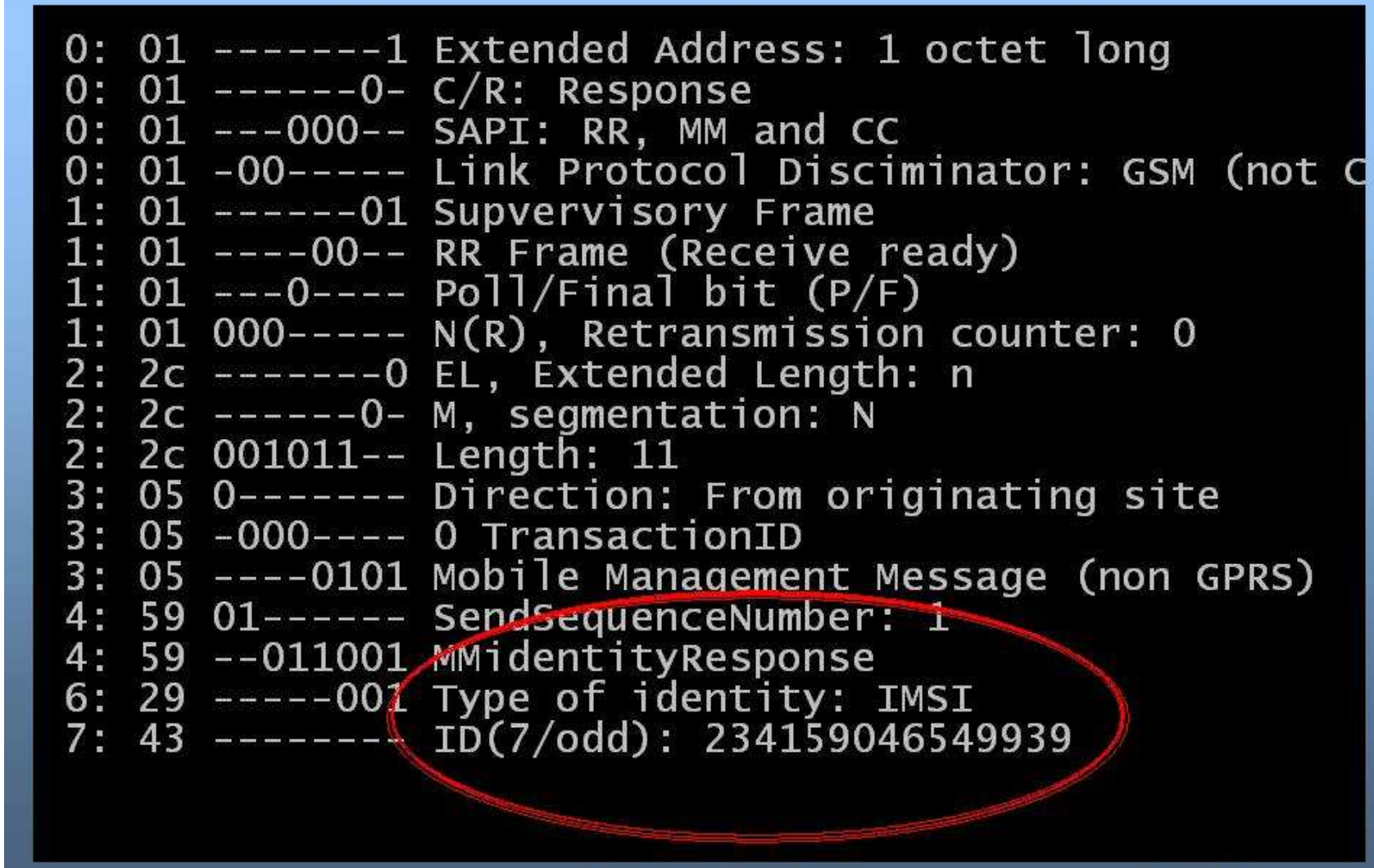
Channels and Bursts

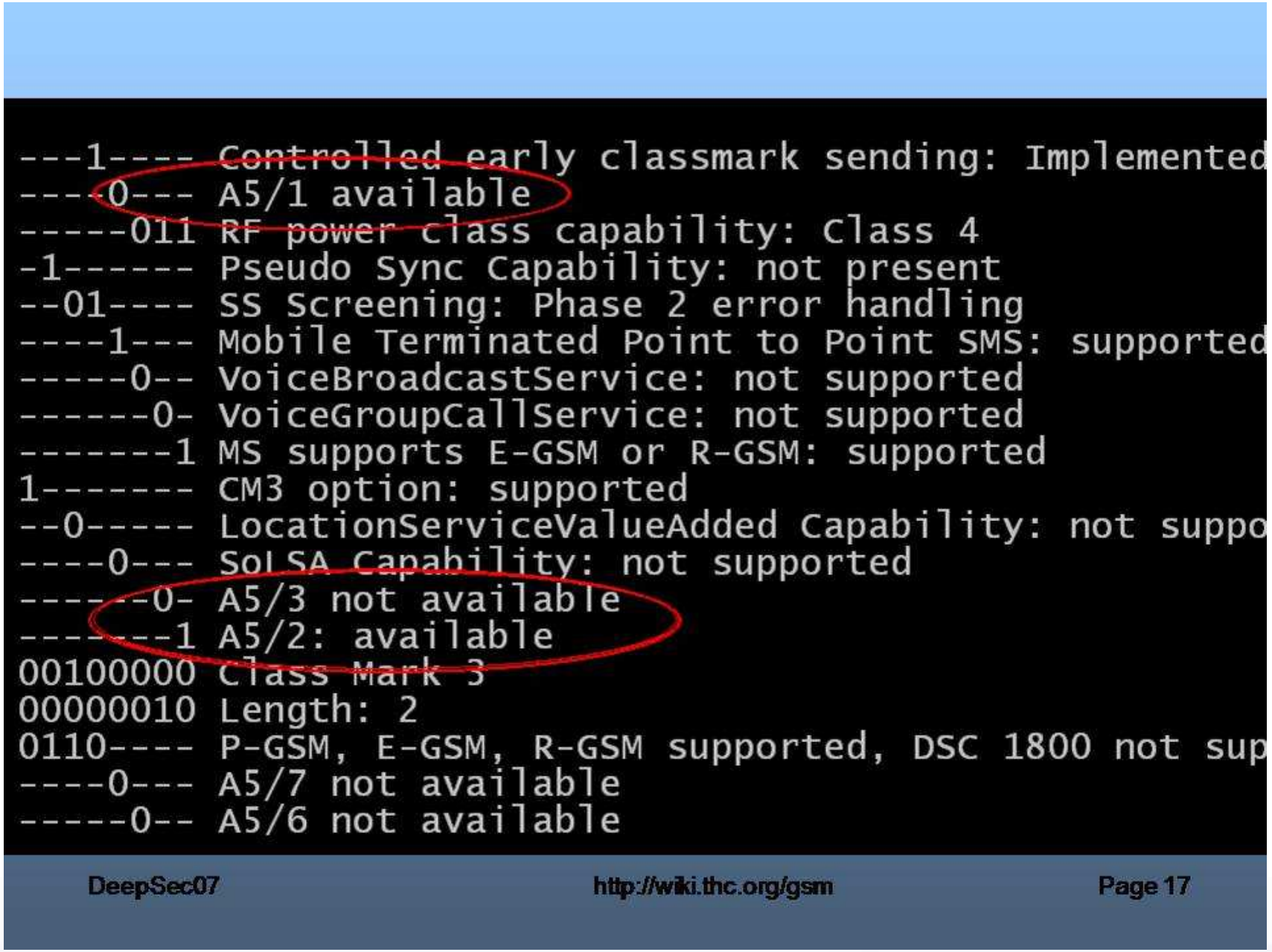
- Rx and Tx on different frequency
- Beacon channel
- SDCCH / TCH
- Channel Hopping
- 1 burst is 156.25 bit long
- 1 burst lasts 0.577ms
- 0..7 timeslots = TDMA frame
- 51 bursts on 1 TS = Multiframe
- 4 bursts = 1 gsm message

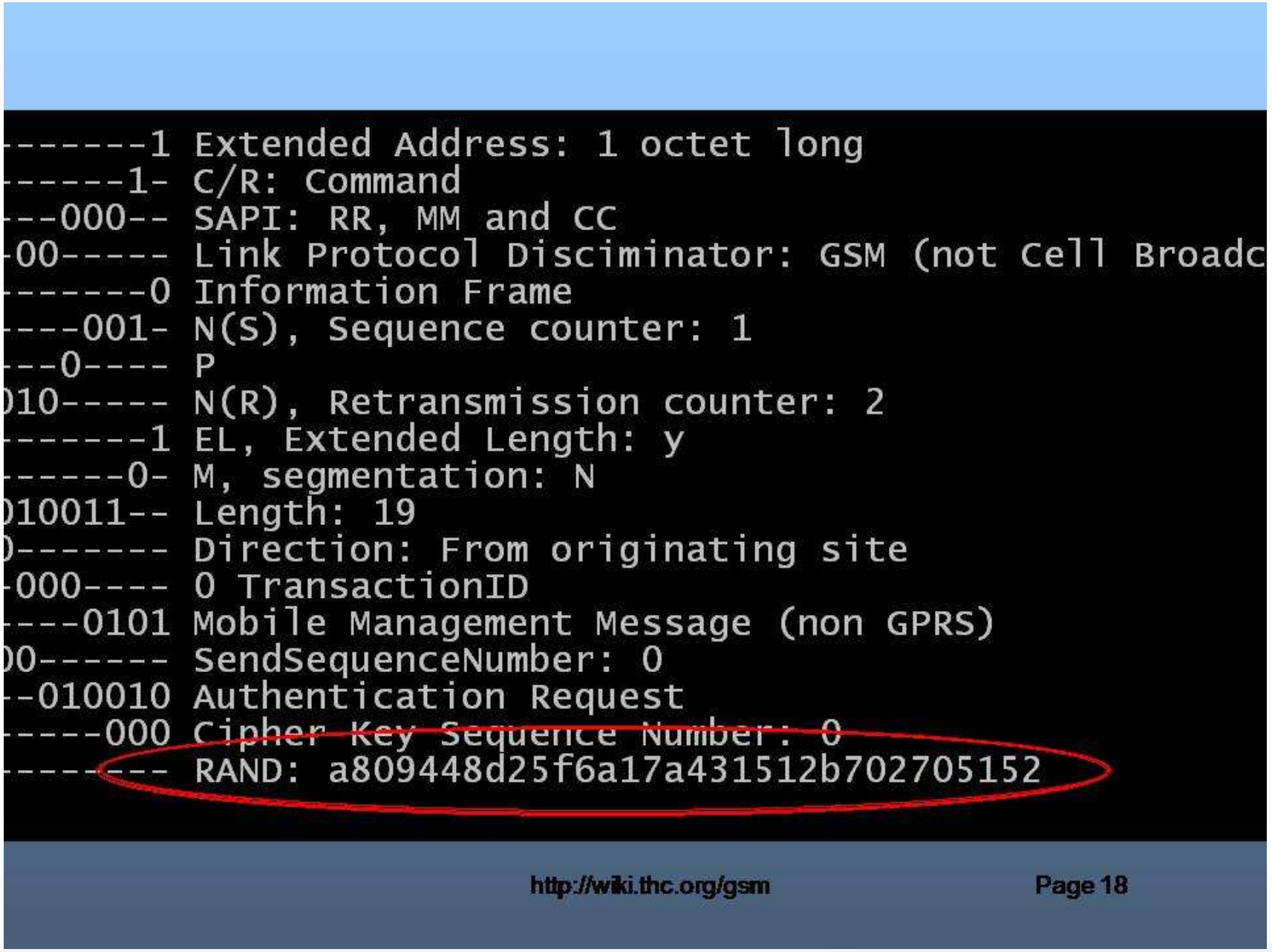

0: 25 001001-- Pseudo Length: 9
1: 06 0------- Direction: From originating site
1: 06 -000---- 0 TransactionID
1: 06 ----0110 Radio Resouce Management
2: 21 00100001 Paging Request Type 1
3: 00 ------00 Page Mode: Normal paging
5: f4 -----100 Type of identity: TMSI/P-TMSI
6: 10 -------- ID(4/even): 1036B446

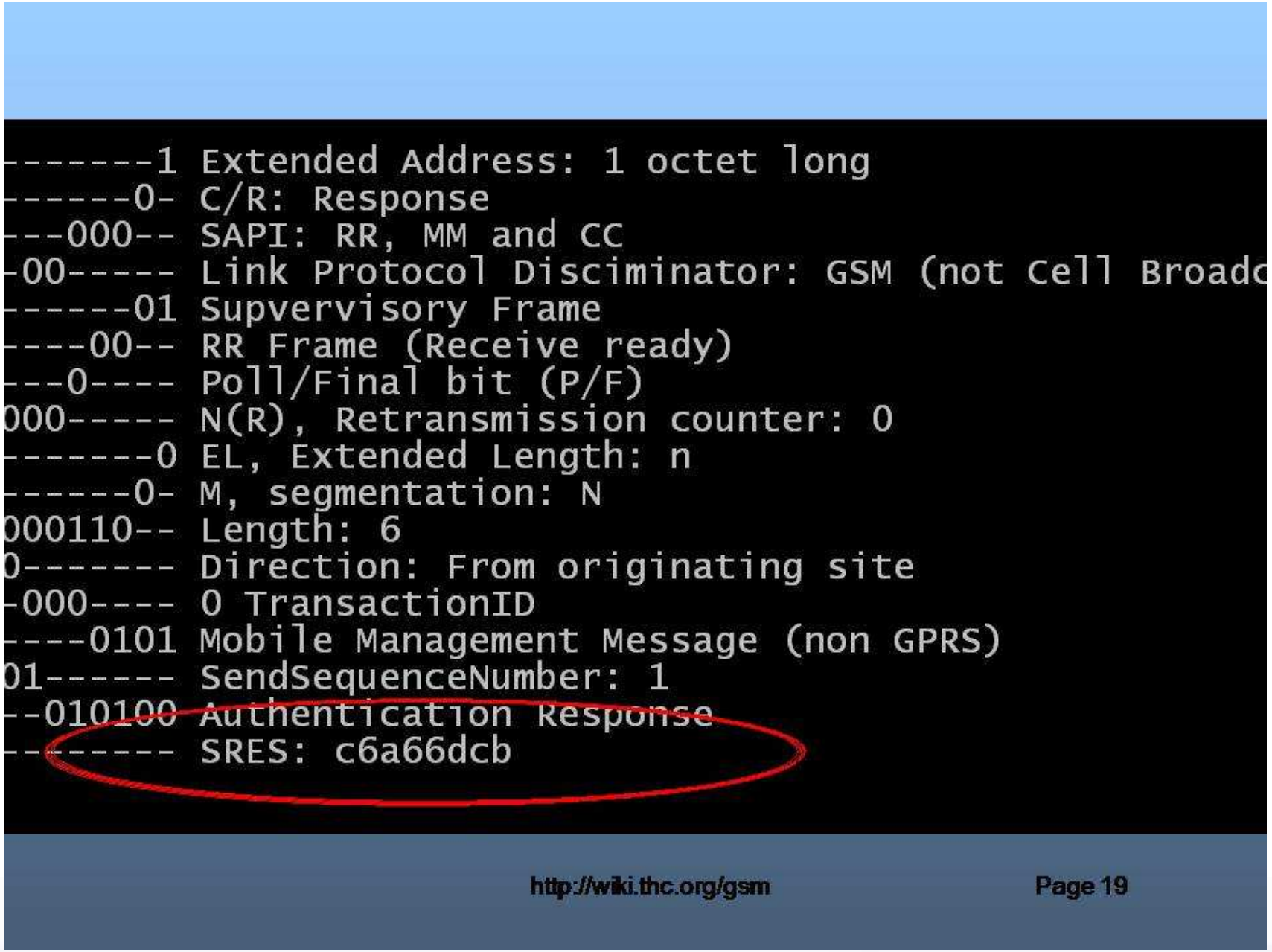

3f 0-111111 RRimmediateAssignment
3f -x------ Send sequence number: 0
03 ------11 Page Mode: reserved / same as before
03 -0------ No meaning
03 --0----- Downlink assig to MS: No meaning
03 ---0---- This messages assigns a dedicated mode resou
41 -----001 Timeslot number: 1
41 01000--- Channel Description: SDCCH/8 + SACCH/C8 or C
70 011----- Training seq. code : 3
70 ---1---- HoppingChannel
10 ..... MAIO 0
10 --010000 Hopping Seq. Number: 16
16 000----- Establishing Cause : All other cases
16 ---xxxxx Random Reference : 22
0d xxxxxxxx T1/T2/T3
15 xxxxxxxx T1/T2/T3
00 --xxxxxx Timing advance value: 0
01 00000001 Length of Mobile Allocation: 1
07 -----1-- Mobile allocation RF chann.59
07 ------1- Mobile allocation RF chann.58
07 -------1 Mobile allocation RF chann.57
http://wiki.thc.org/gsm
Page 14

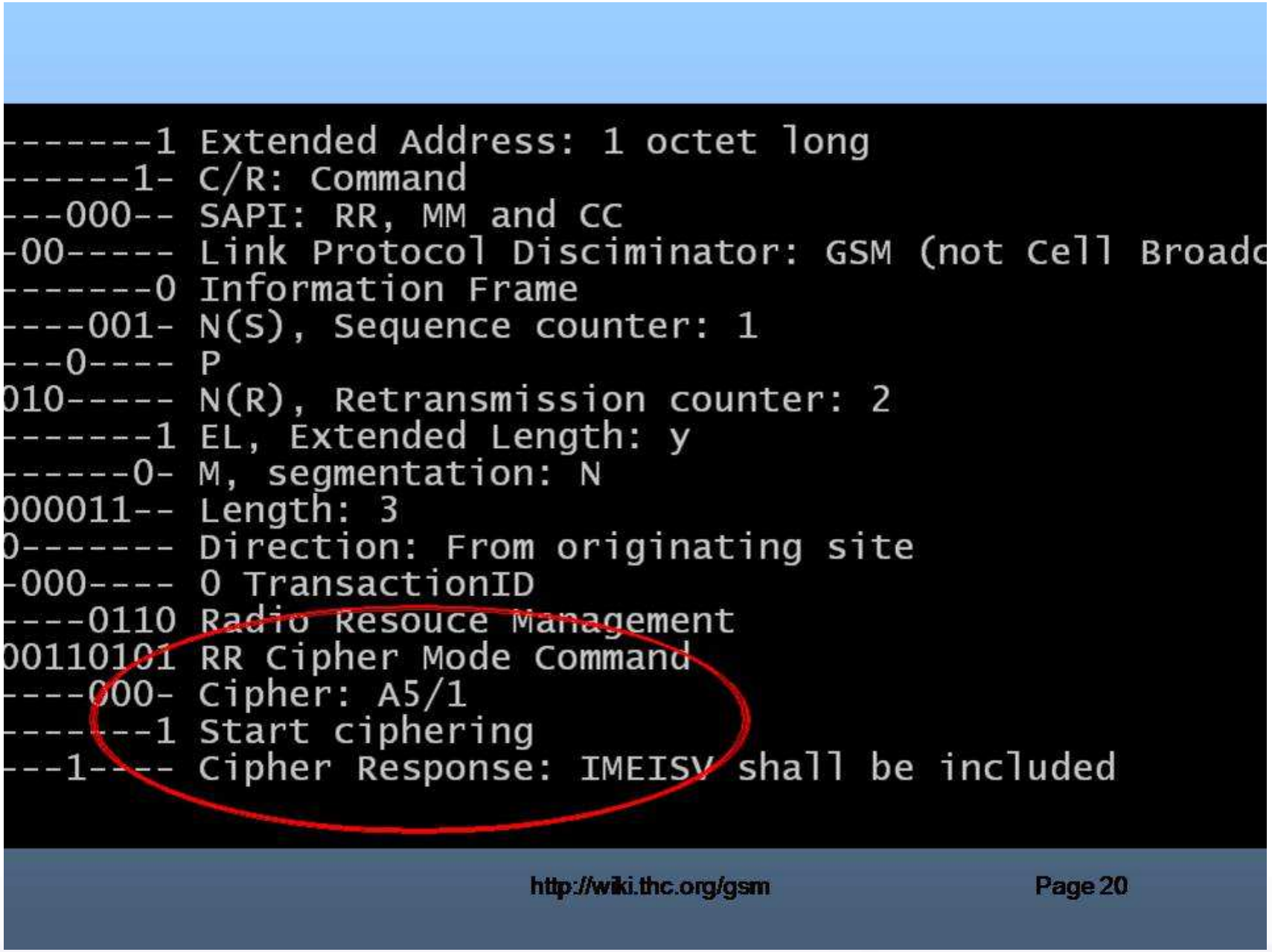

0: 03 -------1 Extended Address: 1 octet long
0: 03 ------1- C/R: Command
0: 03 ---000-- SAPI: RR, MM and CC
0: 03 -00----- Link Protocol Disciminator: GSM (not Cell
1: 20 -------0 Information Frame
1: 20 ----000- N(S), Sequence counter: 0
1: 20 ---0---- P
1: 20 001----- N(R), Retransmission counter: 1
2: 0d -------1 EL, Extended Length: y
2: 0d ------0- M, segmentation: N
2: 0d 000011-- Length: 3
3: 05 0------- Direction: From originating site
3: 05 -000---- 0 TransactionID
3: 05 ----0101 Mobile Management Message (non GPRS)
4: 18 00------ SendSequenceNumber: 0
4: 18 --011000 MMIdentityRequest
5: 01 -----001 Type of Identity: IMSI
http://wiki.thc.org/gsm
Page 15

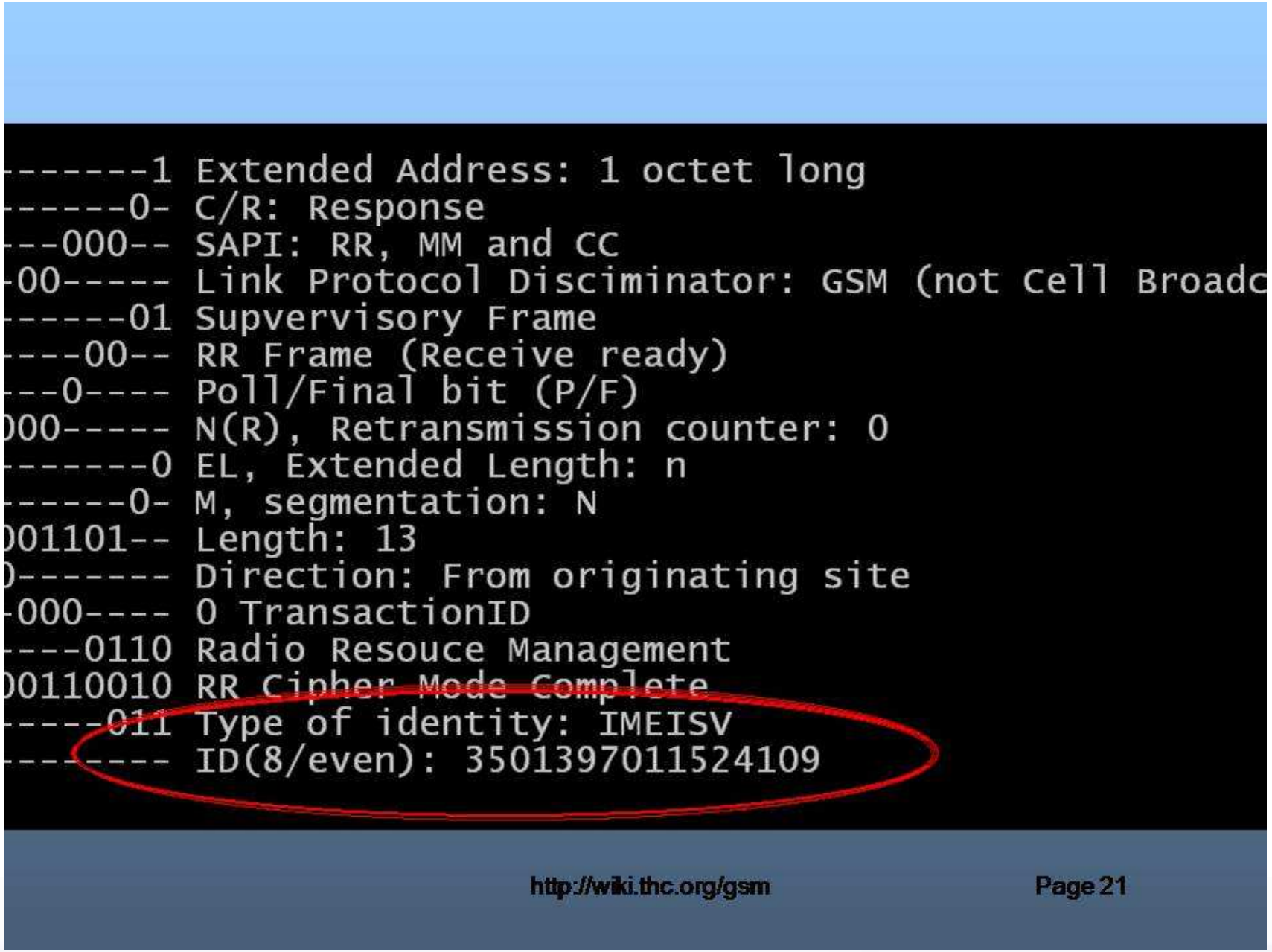

0: 01 -------1 Extended Address: 1 octet long
0: 01 ------0- C/R: Response
0: 01 ---000-- SAPI: RR, MM and CC
0: 01 -00----- Link Protocol Disciminator: GSM (not C
1: 01 ------01 Supvervisory Frame
1: 01 ----00-- RR Frame (Receive ready)
1: 01 ---0---- Poll/Final bit (P/F)
1: 01 000----- N(R), Retransmission 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
http://wiki.thc.org/gsm
Page 16


---1---- Controlled early classmark sending: Implemented
----0--- A5/1 available
-----011 RF power class capability: Class 4
-1------ Pseudo Sync Capability: not present
--01---- SS Screening: Phase 2 error handling
----1--- Mobile Terminated Point to Point SMS: supported
-----0-- VoiceBroadcastService: not supported
------0- VoiceGroupCallService: not supported
-------1 MS supports E-GSM or R-GSM: supported
1------- CM3 option: supported
--0----- LocationServiceValueAdded Capability: not suppo
----0--- SoLSA Capability: not supported
------0- A5/3 not available
-------1 A5/2: available
00100000 Class Mark 3
00000010 Length: 2
0110---- P-GSM, E-GSM, R-GSM supported, DSC 1800 not sup
----0--- A5/7 not available
-----0-- A5/6 not available
DeepSec07
http://wiki.thc.org/gsm
Page 17


-------1 Extended Address: 1 octet long
------1- C/R: Command
---000-- SAPI: RR, MM and CC
-00----- Link Protocol Disciminator: GSM (not Cell Broadc
-------0 Information Frame
---001- N(S), Sequence counter: 1
---0---- P
010----- N(R), Retransmission counter: 2
-------1 EL, Extended Length: y
------0- M, segmentation: N
010011-- Length: 19
0------- Direction: From originating site
-000---- 0 TransactionID
----0101 Mobile Management Message (non GPRS)
00------ SendSequenceNumber: 0
--010010 Authentication Request
-----000 Cipher Key Sequence Number: 0
-------- RAND: a809448d25f6a17a431512b702705152
http://wiki.thc.org/gsm
Page 18


-------1 Extended Address: 1 octet long
------0- C/R: Response
---000-- SAPI: RR, MM and CC
-00----- Link Protocol Disciminator: GSM (not Cell Broadc
------01 Supvervisory Frame
----00-- RR Frame (Receive ready)
---0---- Poll/Final bit (P/F)
000----- N(R), Retransmission counter: 0
-------0 EL, Extended Length: n
------0- M, segmentation: N
000110-- Length: 6
0------- Direction: From originating site
-000---- 0 TransactionID
----0101 Mobile Management Message (non GPRS)
01------ SendSequenceNumber: 1
--010100 Authentication Response
-------- SRES: c6a66dcb
http://wiki.thc.org/gsm
Page 19


-------1 Extended Address: 1 octet long
------1- C/R: Command
---000-- SAPI: RR, MM and CC
-00----- Link Protocol Disciminator: GSM (not Cell Broadc
-------0 Information Frame
----001- N(S), Sequence counter: 1
---0---- P
010----- N(R), Retransmission counter: 2
-------1 EL, Extended Length: y
------0- M, segmentation: N
000011-- Length: 3
0------- Direction: From originating site
-000---- 0 TransactionID
----0110 Radio Resouce Management
00110101 RR Cipher Mode Command
----000- Cipher: A5/1
-------1 Start ciphering
---1---- Cipher Response: IMEISV shall be included
http://wiki.thc.org/gsm
Page 20

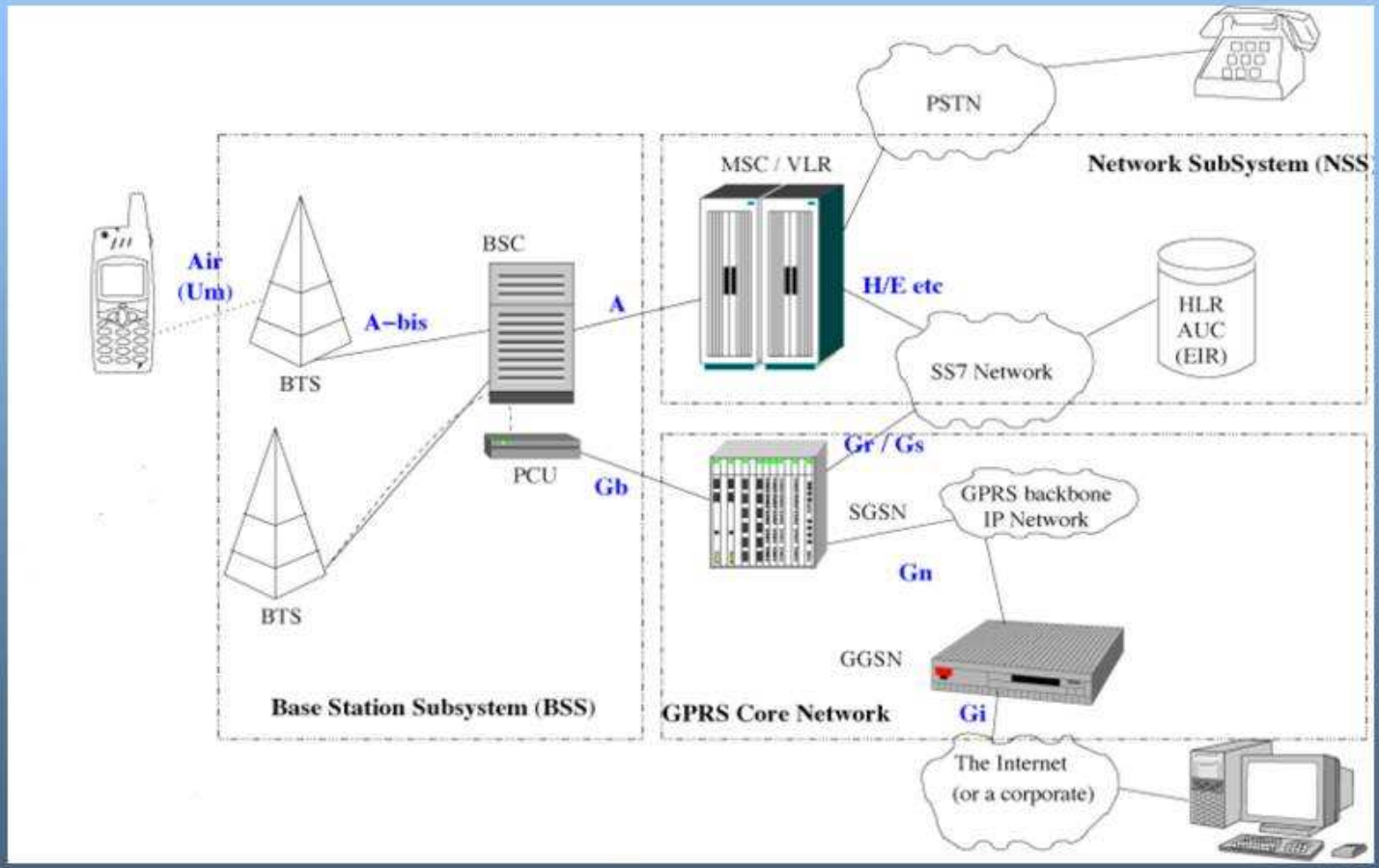

-------1 Extended Address: 1 octet long
------0- C/R: Response
---000-- SAPI: RR, MM and CC
-00----- Link Protocol Disciminator: GSM (not Cell Broadc
------01 Supvervisory Frame
----00-- RR Frame (Receive ready)
---0---- Poll/Final bit (P/F)
000----- N(R), Retransmission counter: 0
-------0 EL, Extended Length: n
------0- M, segmentation: N
001101-- Length: 13
0------- Direction: From originating site
-000---- 0 TransactionID
----0110 Radio Resouce Management
00110010 RR Cipher Mode Complete
-----011 Type of identity: IMEISV
-------- ID(8/even): 350139701152410 9
http://wiki.thc.org/gsm
Page 21

Summary Receiving

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

http://wiki.thc.org/gsm Page 22

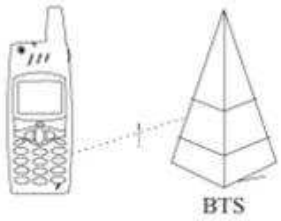
GSM Security



http://wiki.thc.org/gsm

Page 23

GSM Security



http://wiki.thc.org/gsm Page 24

GSM Security

http://wiki.thc.org/gsm

Page 25

Commercial Interception

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

http://wiki.thc.org/gsm Page 26

Radio Security

- A5/1, A5/2, A5/0 (broken in 1998)
- MobOp knows the Pre-Shared Secret.
- Access to BTS
- Past conversation can be decoded with future access to SIM or key.
- Some algorithms proprietary
- IMSI / Location Information clear-text
- Key is artificially weakened
- Key material is reused
- No indication to user
- Key Recover Systems available

http://wiki.thc.org/gsm Page 27

SIM Toolkit Madness

- 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, ….

Summary Security

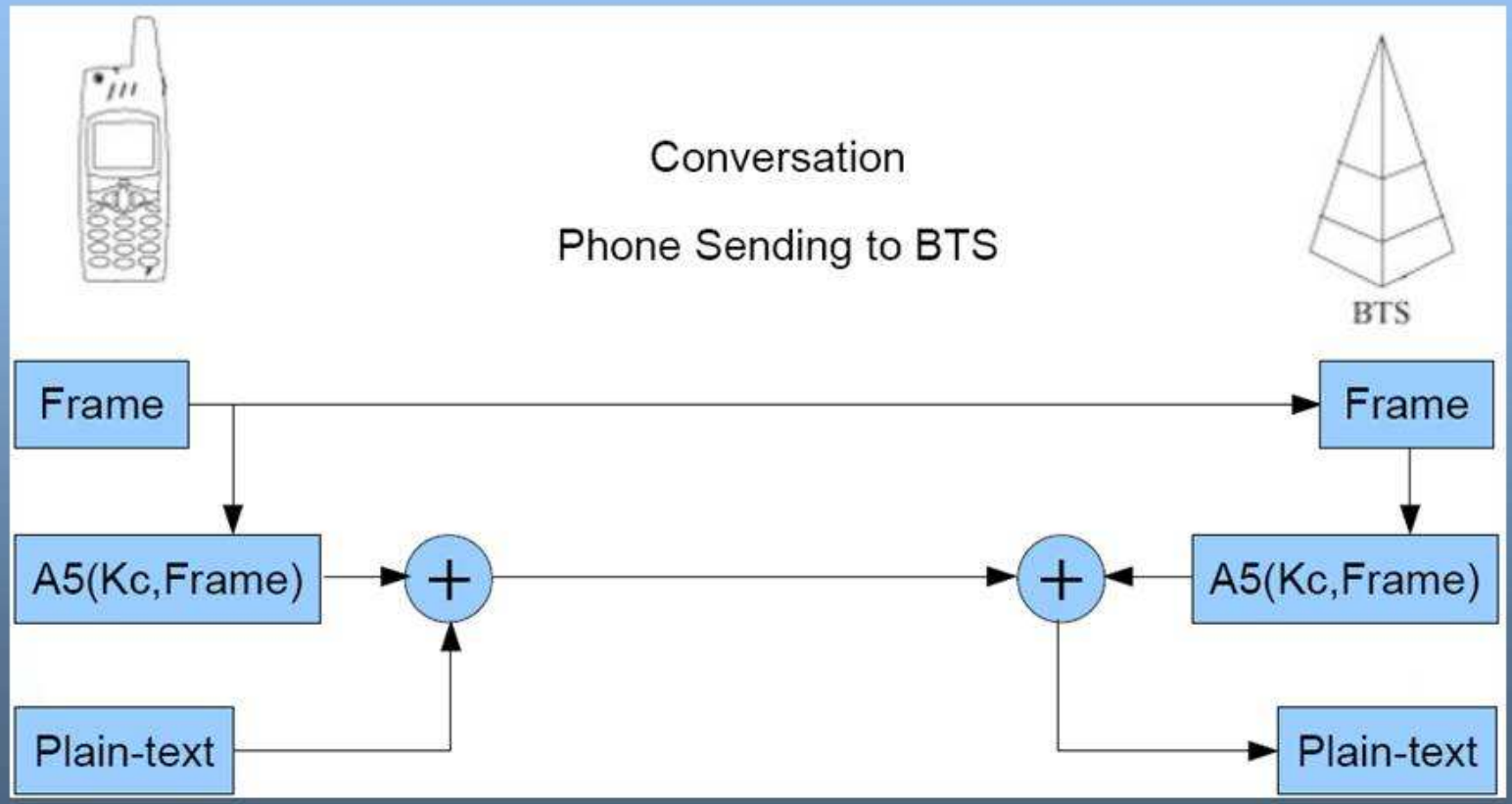
- NONE

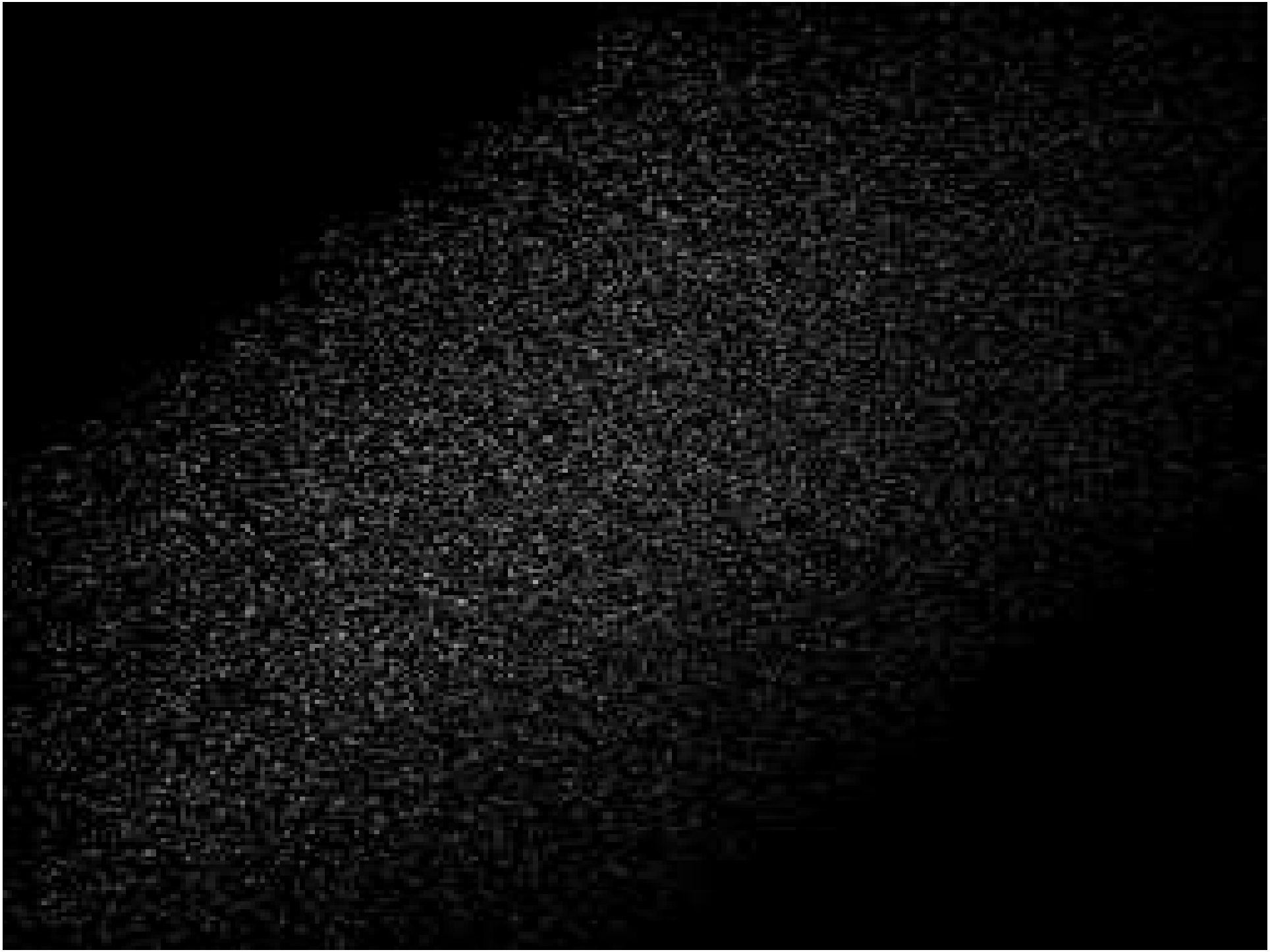
GSM Ciphers

- Ki = 128 Bit
- RAND = 128 Bit
- SRES = 32 Bit
- Kc = 64 Bit

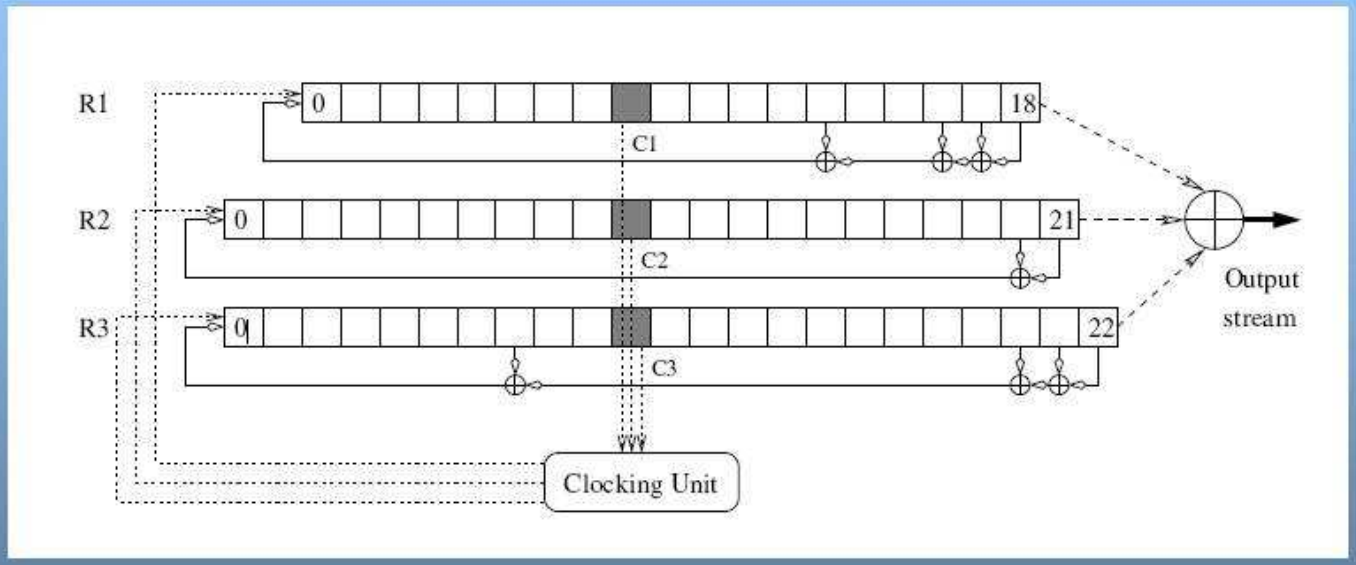
- A3(Ki, RAND) => SRES
- A8(Ki, RAND) => Kc
- A5(Kc, FN) => 114 bit cipherstream

A5/1


Conversation
Phone Sending to BTS
BTS
Frame
Frame
A5(Kc,Frame)
A5(Kc,Frame)
Plain-text
Plain-text
http://wiki.thc.org/gsm
Page 31



How A5/1 works



- Clock in 64 bit Kc + 22 bit Frame Number
- Clock for 100 times
- Clock for 114 times to generate 114 bit

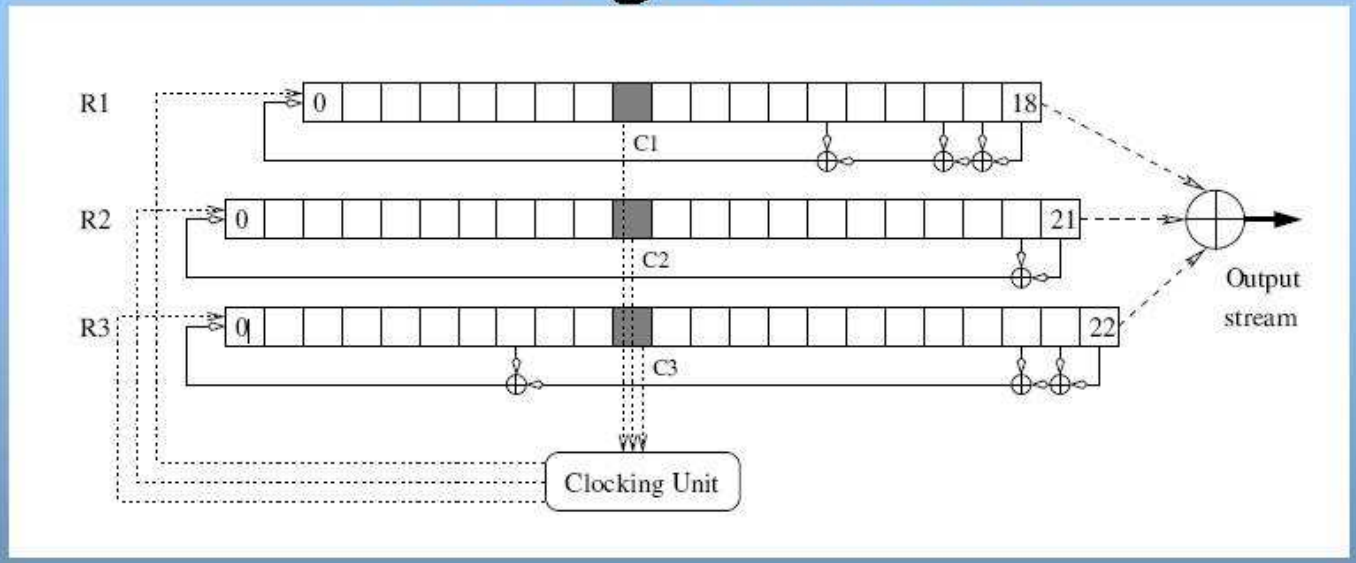
http://wiki.thc.org/gsm Page 32

Cracking A5/1

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

http://wiki.thc.org/gsm Page 33

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 .....]

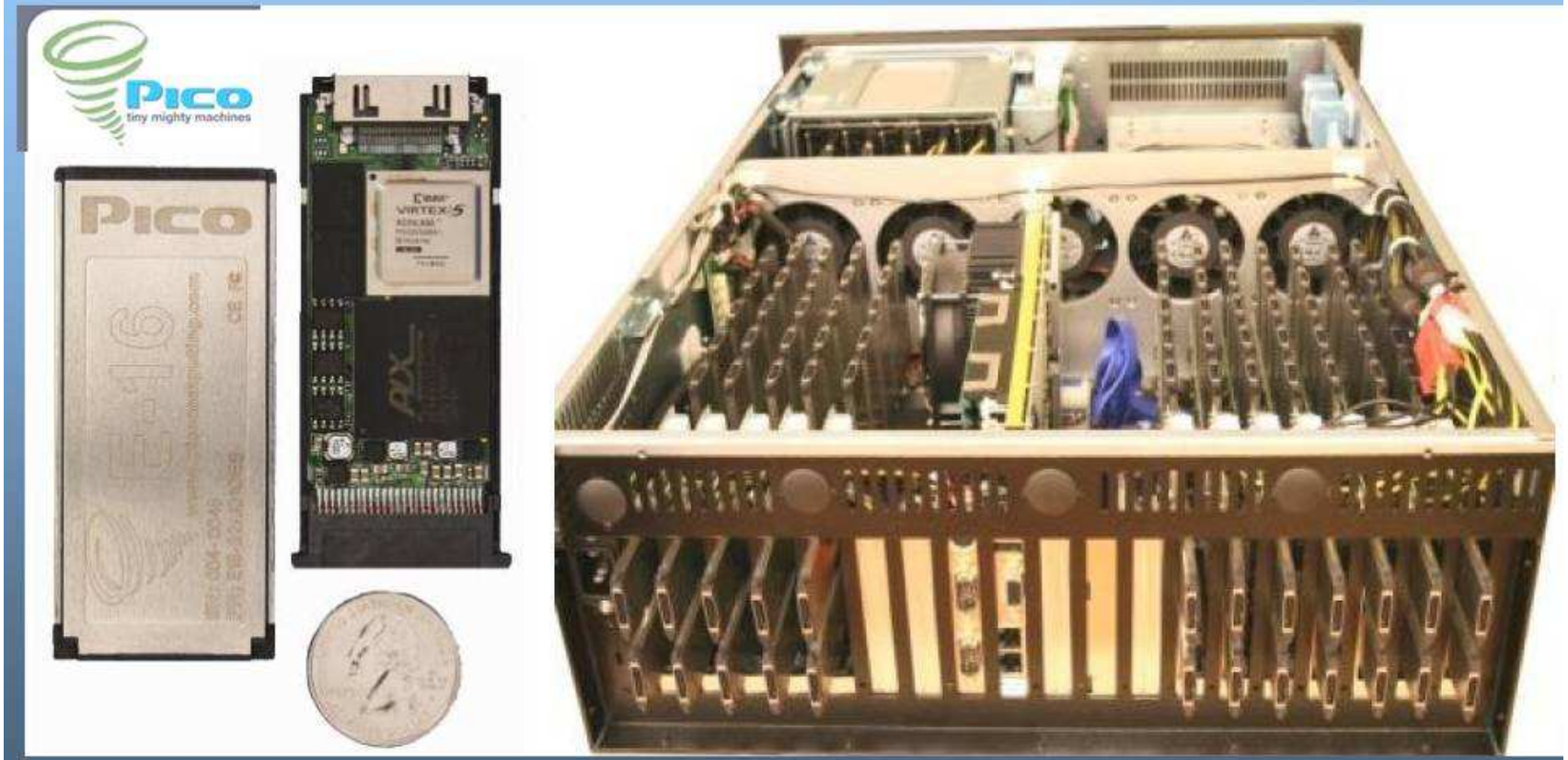
http://wiki.thc.org/gsm Page 34

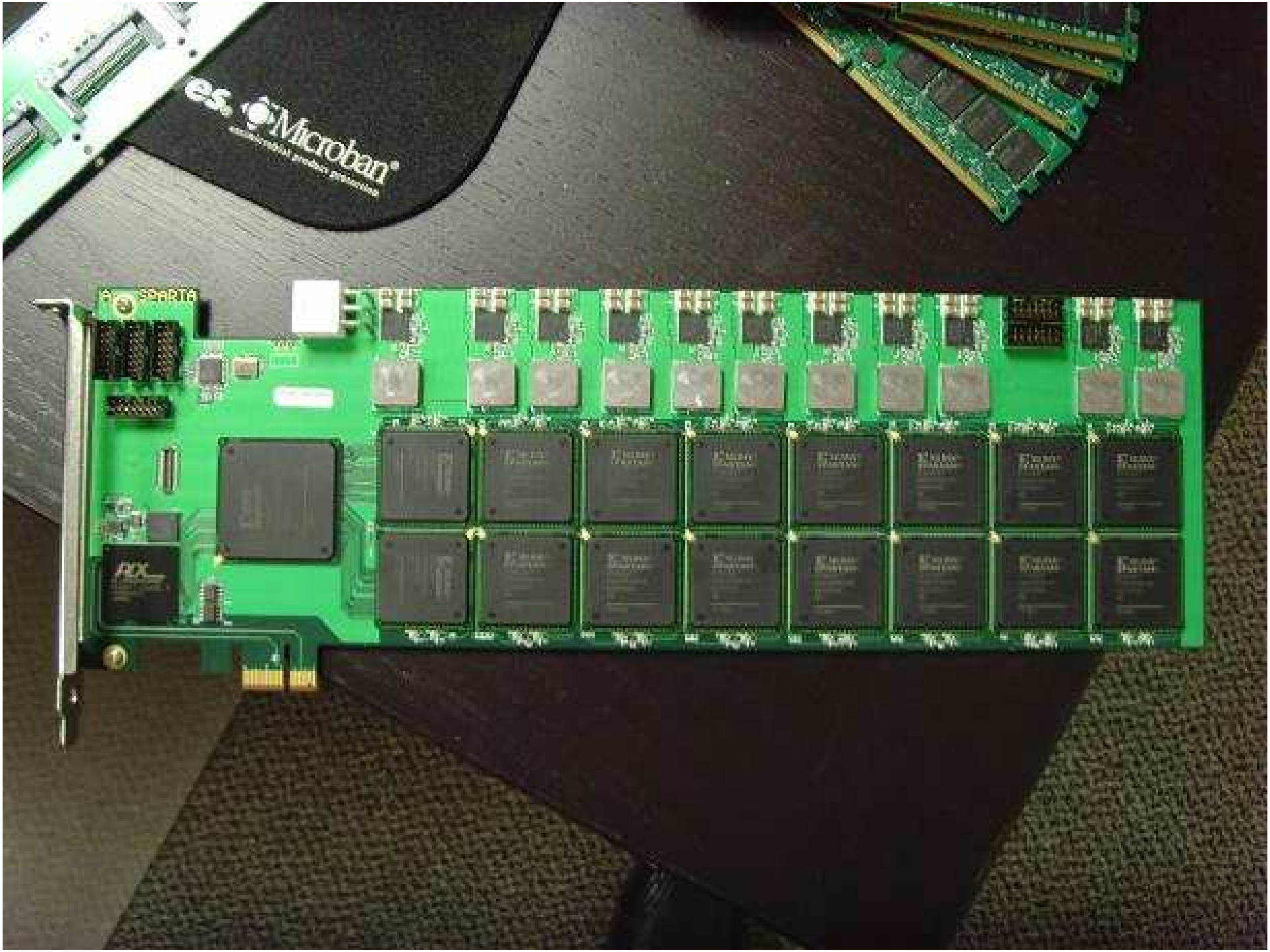
What are TMTO

- Solves problem of storing 2^64 'password' -> output combinations
- Famous since Rainbow Table attacks
- Invented in the 80s.
- Having 204 data points means we only need 1/64th of the entire keyspace.
- 2^58 = 288,230,736,151,711,744
- About 120,000 times larger than the largest Rainbow Table

http://wiki.thc.org/gsm Page 35

FPGA




Microban
SPARTA
PLX

Generating the Table

- FPGA Cluster for 60 days
- 1 FPGA == 1800x faster than my laptop
- 100 FPGAs (60 days instead of 29670 years

- <30 seconds
- 95%+ probability

http://wiki.thc.org/gsm Page 37

Threats & Future

- Sending / Pirate GSM / OpenTSM
- BabyCell
- MitM
- Track
- Phone Number scan
- Brute Force, access to DB
- Free calls
- 3G/UMTS, Femtocells, Picocells

http://wiki.thc.org/gsm Page 38

Further information

- About The GSM Software Project
  - http://wiki.thc.org/gsm
- About Cellcrypt voice encryption
  - http://www.cellcrypt.com