Time-Memory Trade-Offs Sound the Death Knell for GPRS and GSM

Gildas Avoine[1], **Xavier Carpent**[2], **Tristan Claverie**[3], **Christophe Devine**[4], **Diane Leblanc-Albarel**[5]

[1]INSA de Rennes, IRISA, CNRS, France
[2]University of Nottingham, UK
[3]ANSSI, INSA de Rennes, IRISA, France
[4]ANSSI, France
[5]KU Leuven, Belgium

Crypto'24, August 19th, 2024

Contributions

- Functions to attack GPRS <u>and</u> GSM with TMTOs
- Apply to all 2G ciphers
- Practical passive attack on A5/3 and GEA-3, 128 bits of known plaintext
- Experimental validation on implementations

Introduction to 2G

- 2G = GSM[1] + GPRS[2]
- GSM : Calls and SMS
- GPRS : IP packets

Use :

- 2G-only connected devices
- No coverage of 3/4/5G

1. Global System for Mobile communications
2. General Packet Radio Service

2G encryption

- GSM encryption : mobile to base station, A5/*
- GPRS encryption : mobile to SGSN[3], GEA-*

Passive attacker model

3. Serving GPRS Support Node

2G encryption status

Technology	Algorithm	Key size	Implementation	Attack	TMTO
GSM	**A5/0 (no encryption)**	N/A	Mandatory	N/A	N/A
GSM	**A5/1**	64	Mandatory	Srlabs, ∼2011	Y
GSM	**A5/2**	64	Forbidden	Barkan et al. 2011	N
GSM	**A5/3**	64	Mandatory	Dunkelman et al. 2010 (theoretical)	N
GSM	**A5/4**	128	Optional	Dunkelman et al. 2010 (theoretical)	-
GPRS	**GEA-0 (no encryption)**	N/A	Mandatory	N/A	N/A
GPRS	**GEA-1**	64	Forbidden	Beierle et al. 2021	N
GPRS	**GEA-2**	64	Mandatory	Beierle et al. 2021	N
GPRS	**GEA-3**	64	Mandatory	Dunkelman et al. 2010 (theoretical)	N
GPRS	**GEA-4**	128	Optional	Dunkelman et al. 2010 (theoretical)	N
GPRS	**GEA-5**	128	Optional	-	-

2G encryption status

Technology	Algorithm	Key size	Implementation	Attack	TMTO
GSM	**A5/0 (no encryption)**	N/A	Mandatory	N/A	N/A
GSM	**A5/1**	64	Mandatory	Srlabs, ∼2011	Y
GSM	**A5/2**	64	Forbidden	Barkan et al. 2011	N
GSM	**A5/3**	64	Mandatory	Dunkelman et al. 2010 (theoretical)	N
GSM	**A5/4**	128	Optional	Dunkelman et al. 2010 (theoretical)	-
GPRS	**GEA-0 (no encryption)**	N/A	Mandatory	N/A	N/A
GPRS	**GEA-1**	64	Forbidden	Beierle et al. 2021	N
GPRS	**GEA-2**	64	Mandatory	Beierle et al. 2021	N
GPRS	**GEA-3**	64	Mandatory	Dunkelman et al. 2010 (theoretical)	N
GPRS	**GEA-4**	128	Optional	Dunkelman et al. 2010 (theoretical)	N
GPRS	**GEA-5**	128	Optional	-	-

Can Time-Memory Trade-Offs be used beyond A5/1 ?

Time-Memory Trade-Offs

Introduction to TMTOs

Use : Invert a one-way function

Given $h : x \mapsto y$ and y,
find x such that $h(x) = y$

Steps :

- Precomputation : compute a table covering possible inputs x
- Attack : from y, find x

Applying TMTOs to stream ciphers

Stream cipher : $e(K, \text{IV}) \oplus p = c$

Example one-way function :

$$h(x) = e(x, \text{cst})$$

Conditions :

- Condition 1 : determine a constant IV *cst*
- Condition 2 : know 128 bits of plaintext p encrypted using *cst*

GPRS

GPRS encryption

$$c = p \oplus \mathrm{GEA}(K_c, \texttt{Input, D})$$

$$\texttt{Input} = ((\texttt{IOV-UI} \oplus \mathsf{SX}) + \mathsf{LFN} + \mathsf{OC}) \mod 2^{32}$$

⇒ IV freshness depends on IOV-UI freshness

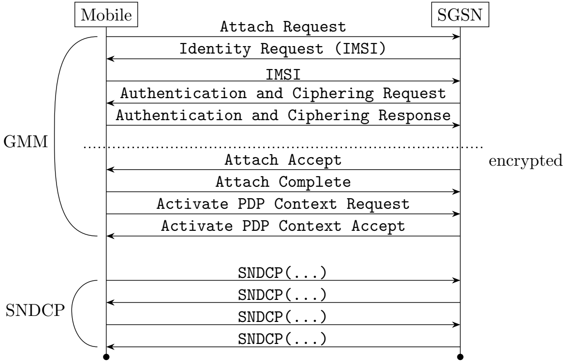
GPRS encryption

$$c = p \oplus \mathrm{GEA}(K_c, \texttt{Input, D})$$

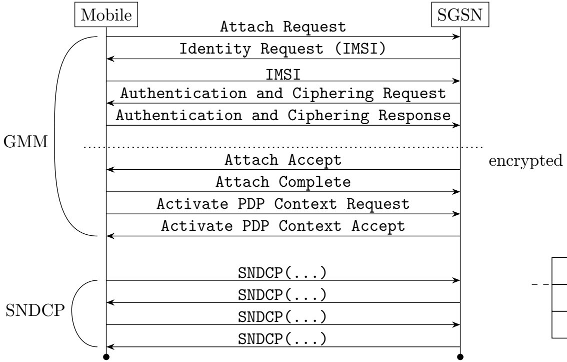
$$\texttt{Input} = ((\texttt{IOV-UI} \oplus \mathsf{SX}) + \mathsf{LFN} + \mathsf{OC}) \mod 2^{32}$$

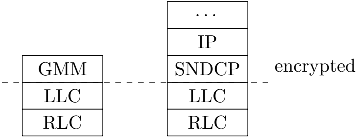
⇒ IV freshness depends on IOV-UI freshness
IOV-UI initialized with 0, may be changed by the network. (**Condition 1**)

Start of a GPRS session



Start of a GPRS session





Known plaintext bits in GPRS

- Signalling messages : known bits, positions vary
- Data message : 32 known bits in SNDCP header[4] (**Condition 2**)

4. Validated experimentally

Known plaintext bits in GPRS

- Signalling messages : known bits, positions vary
- Data message : 32 known bits in SNDCP header[4] (**Condition 2**)

Function to invert :

$$h_{\text{GPRS}}(K_c) = \text{GEA}(K_c, \texttt{0x98000000}, 0)[\texttt{0:31}] \| \text{GEA}(K_c, \texttt{0x98000001}, 0)[\texttt{0:31}] \| \text{GEA}(K_c, \texttt{0x98000002}, 0)[\texttt{0:31}] \| \text{GEA}(K_c, \texttt{0x98000003}, 0)[\texttt{0:31}].$$

4. Validated experimentally

Applicability of TMTOs to GPRS

Network misconfigured (i.e., IOV-UI = 0) : all new sessions can be attacked.

Network well-configured (random IOV-UI) :

- Passive attacker : probability 2^{-32} to attack a session
- Active attacker : all new sessions can be attacked

Practical tests

Inside a controlled environment :

- 2G test network (Osmocom)
- Professional/commercial implementations tested
- Development SIM card

Log collection

- Instrumented mobile handsets
- Instrumented open-source components
- Network sniffing
- Over-the-air sniffing (modified gr-gsm)

SNDCP headers in GPRS

Test : Do SNDCP headers vary ?

Tested mobiles :

- Motorola V171
- Xiaomi Redmi Note 8T
- Generic Mediatek MTK6762 phone
- Crosscall Core-X5
- Samsung Galaxy A8
- iPhone SE 2020

SNDCP headers in GPRS

Test : Do SNDCP headers vary ?

Tested mobiles :

- Motorola V171
- Xiaomi Redmi Note 8T
- Generic Mediatek MTK6762 phone
- Crosscall Core-X5
- Samsung Galaxy A8
- iPhone SE 2020

$\Rightarrow$ SNDCP header always predictable

IOV-UI renewal in implementations

Test : Do implementations always renew IOV-UI ?

Testing tool : FreeCalypso FCDEV3B Board, custom firmware

Some implementation(s) :

- Do not renew IOV-UI ;
- Send a new IOV-UI, random ;
- Send a "new" IOV-UI, all zeros.

IOV-UI renewal in implementations

Test : Do implementations always renew IOV-UI ?

Testing tool : FreeCalypso FCDEV3B Board, custom firmware

Some implementation(s) :

- Do not renew IOV-UI ;
- Send a new IOV-UI, random ;
- Send a "new" IOV-UI, all zeros.

$\Rightarrow$ There exist vulnerable implementations

Applicability of TMTOs to GSM

Function to invert :

$$h_{\mathsf{GSM}}(K_c) = \mathtt{A5}(K_c, \mathtt{256})[\mathtt{114:227}] \| \mathtt{A5}(K_c, \mathtt{298})[\mathtt{114:127}].$$

Probability to attack a session : $\frac{1}{2} \times \frac{\mathsf{session\_duration}}{\mathsf{3h28}}$

Proportional to the duration of the session !

Scenarios

TMTO parameters

Studied TMTOs : Rainbow tables

Parameters :

- P : Precomputation complexity
- T : Attack complexity
- M : Memory complexity
- p : Success probability
- l : Number of tables

Rainbow table benchmarks

Time estimate : benchmark KASUMI[5] efficiency.

Precomputation : CUDA on GPU (Nvidia RTX 3090)

Attack step :

- CPU implementation (Intel Core i7-10510U) : C, Golang, Assembly, AVX and AVX2
- SSD for storage (Samsung 980 NVMe M.2 1TB) : distributed implementations

5. A5/3 and GEA-3 rely on the KASUMI block cipher

Scenarios

Precomputation Phase		Attack phase				
Number of GPUs	Time (days)	Servers	Memory (TB)	Success probability		Time (min)
				GPRS session [6]	30-min GSM call	
600	289	2	100	0.25	0.04	5
1200	348	5	125	0.5	0.07	13
2400	348	10	200	0.75	0.11	14

6. Assuming a misconfigured network

Communication with GSMA

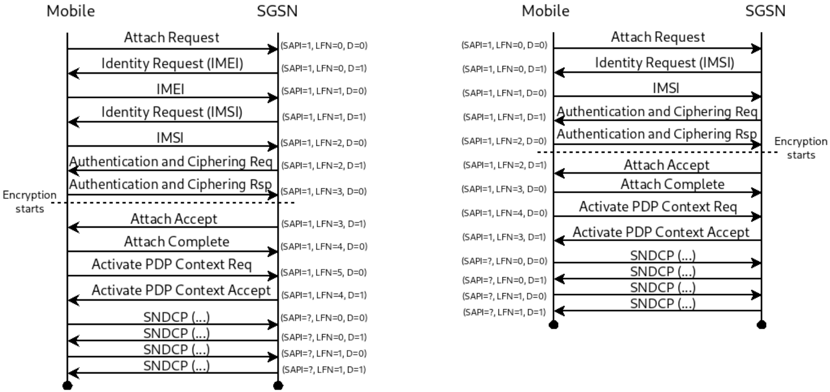
Responsible disclosure to GSMA :

- Acknowledged all problems
- Will clarify the role of IOV-UI in the specification
- A5/4 and GEA-4 will be made mandatory in mobiles
- Communication with worldwide operators to verify their IOV-UI randomization

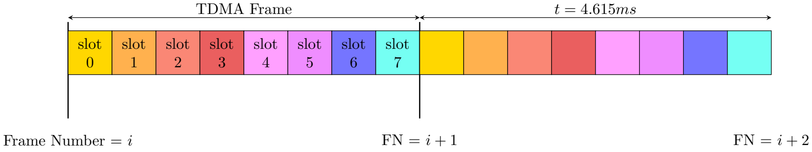
Mitigations : enable padding randomization (GSM), renew IOV-UI (GPRS), enable frequency hopping (both), disable 2G in mobiles (both).

Backup Slides

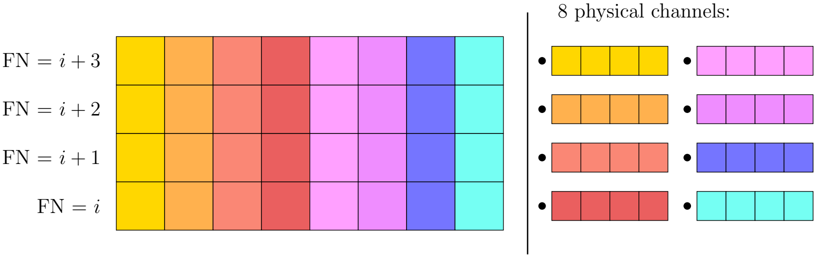
Possible GPRS session setup



GSM timeslots



GSM physical channels



GSM logical channels

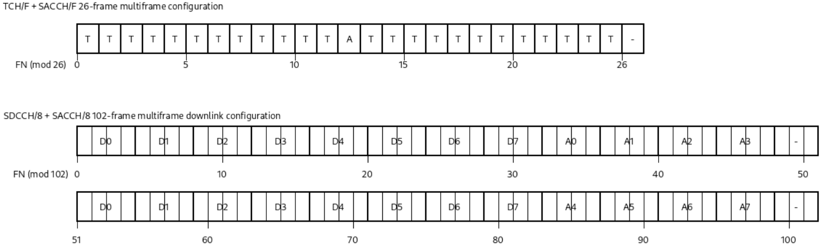
One physical channel may carry several logical channels :

- TCH/F+SACCH/F
- SDCCH/8+SACCH/8
- ...

Each standardized channel combination obeys its defined multiframe structure.

Channel combination used by a BTS is up to the network configuration.

Example multiframe



SACCH

SACCH channel always contains SIT5 or SIT6 messages.

Exhaustive search on FN values showed that some FNs always contain a SACCH timeslot, for any possible channel combination.

GSM padding

Process of GSM coding and encryption of LAPDm frames :

1. messages are fragmented into 184-bits blocks
2. a 40-bits CRC is added to the message (184 -> 224 bits)
3. Two convolutional codes are applied, independently (224 -> 2*228 = 456 bits)
4. Bits are interleaved (i.e., rearranged) (456 -> 456 bits)
5. The resulting message is split into 4 114-bits bursts (456 -> 4*114 bits)
6. Each burst is scheduled in a different timeslot, with a distinct TDMA Frame Number
7. Before transmission, each burst is xored with the keystream for this Frame Number

GSM padding

⇒ The burst transmitted contains a linear combination of plaintext and padding bits.

⇒ If plaintext and padding known -> burst known

⇒ If plaintext known but not padding -> burst unknown