3GPP SA3#33
Beijing, China
10-14 May 2004

S3-040389

Another Countermeasure for the Barkan-Biham-Keller Attack on A5/2

Jean-Philippe Wary jean-philippe.wary@fr.sfr.com

SFR Contributors :
Frédéric Bukal - NSS Expert *frederic.bukal@fr.sfr.com*
Paul Wanner - Radio Expert *paul.wanner@fr.sfr.com*
Jean-Philippe Wary - Security Expert *Jean-Philippe.wary@fr.sfr.com*

groupe cegetel

Barkan-Biham-Keller Attack on A5/2 -

- GSM standards permit the use of various encryption algorithms over the radio air interface to provide support for confidentiality:
  - A5/1 (all handset should support)
  - A5/2 (all handset produced in the last few years should also support)
  - A5/3 (recently specified but not implemented in any handsets yet)
- On 21st August 2003 a new attack (real time attack) on A5/2 was published at a conference by academics from the Israel Institute of Technology
- Previous attacks on A5/2 relied upon prior knowledge of the plaintext speech to break the encryption algorithm.
- This new attack provides a means to break A5/2 using only several milliseconds of encrypted GSM signalling data by exploiting error correction codes in SACCH (Slow Associated Control Channel) : the attacker recovers Kc (Cipher Key) which is used by all A5 algorithms.
- This attack remains difficult (and expensive) to implement but the costs could decrease quickly if the first frauds appear.

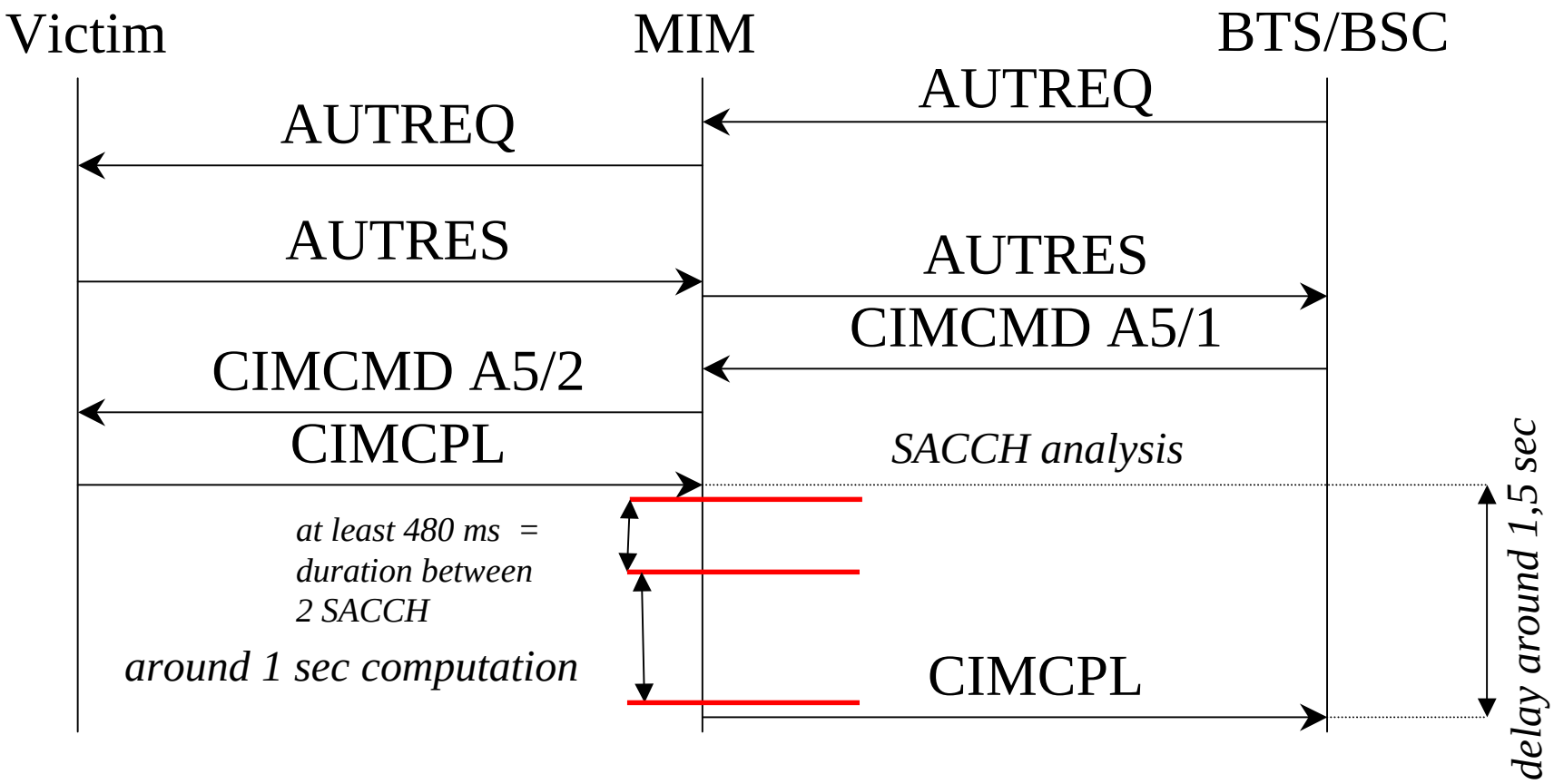
Another countermeasure

- The principle of this countermeasure is based on the detection by BSC (Base Station Controller) of an unusual duration of 2 phases during a “Man in the Middle (MIM)” attack :
  - SIM authentication (AUTREQ - AUTRES)
  - Negotiation of ciphering mode (CIMCMD/CIMCPL)

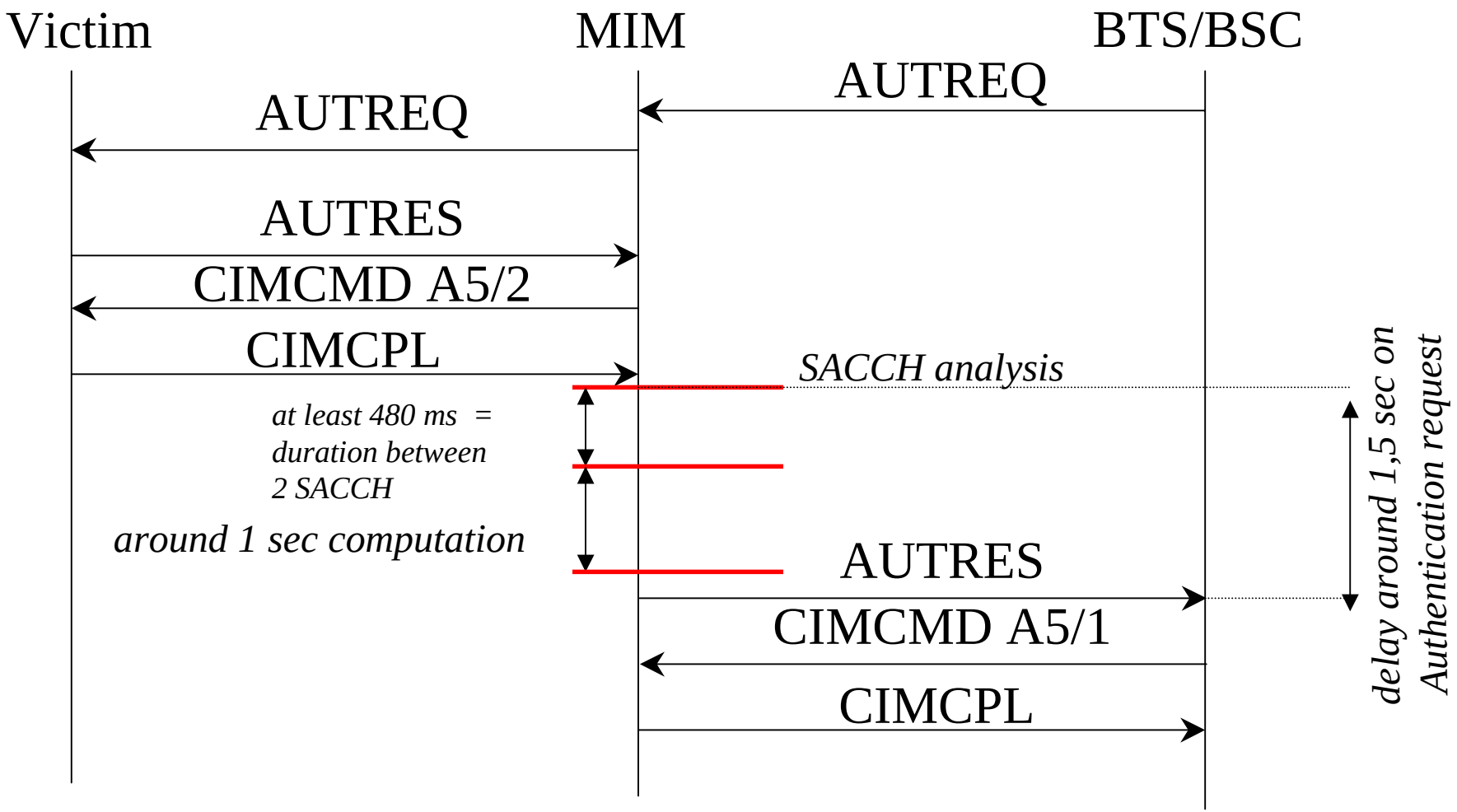
- All of our measurements are done inside BSC.

- The first step was the feasibility analysis in SFR network (measurements done in Dec. 03 and Jan. 04) : the results are favourable on the BSC analysed (based on more than 1000 measurements).

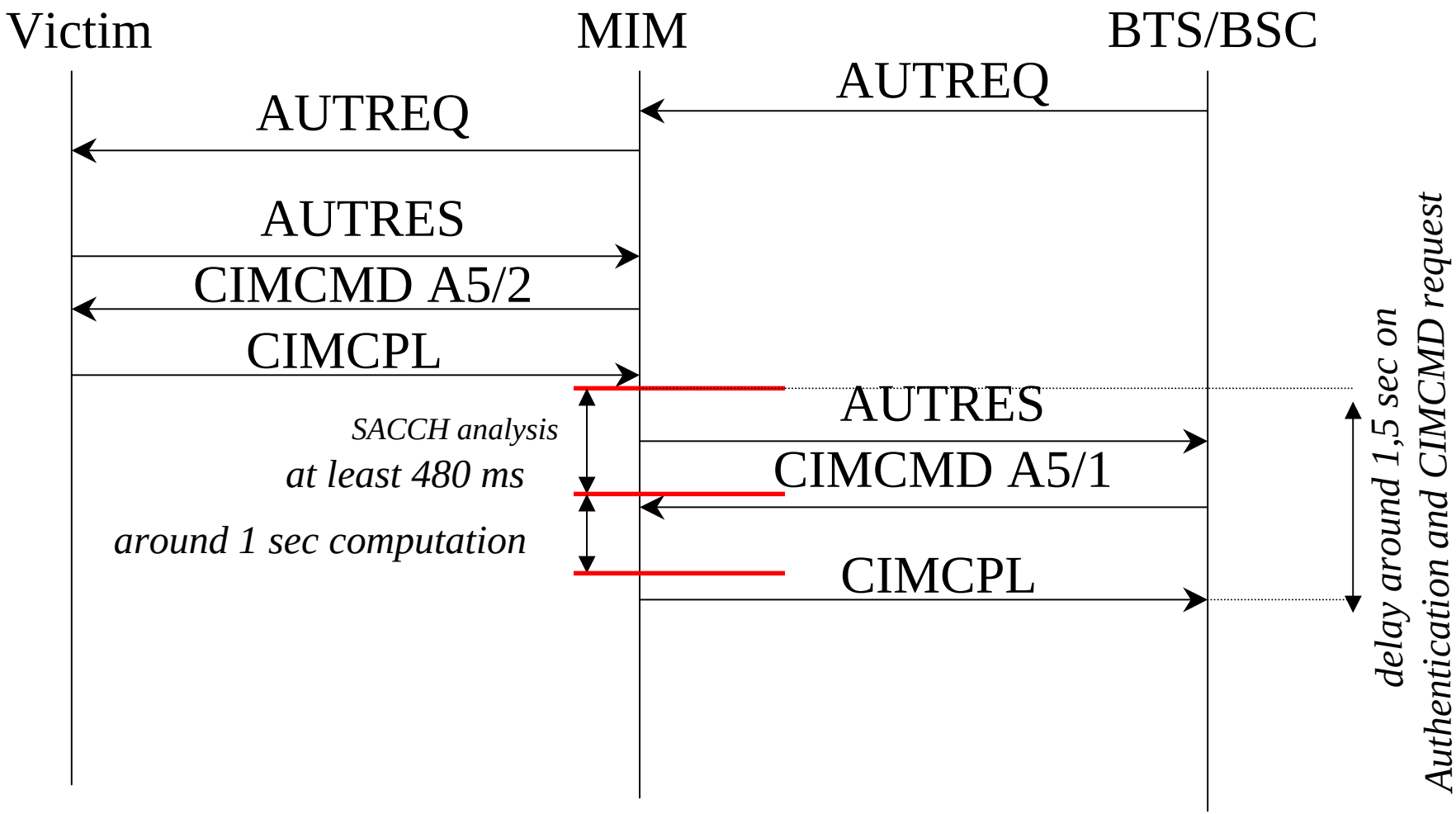
simple attack



attack hidden inside Authentication request

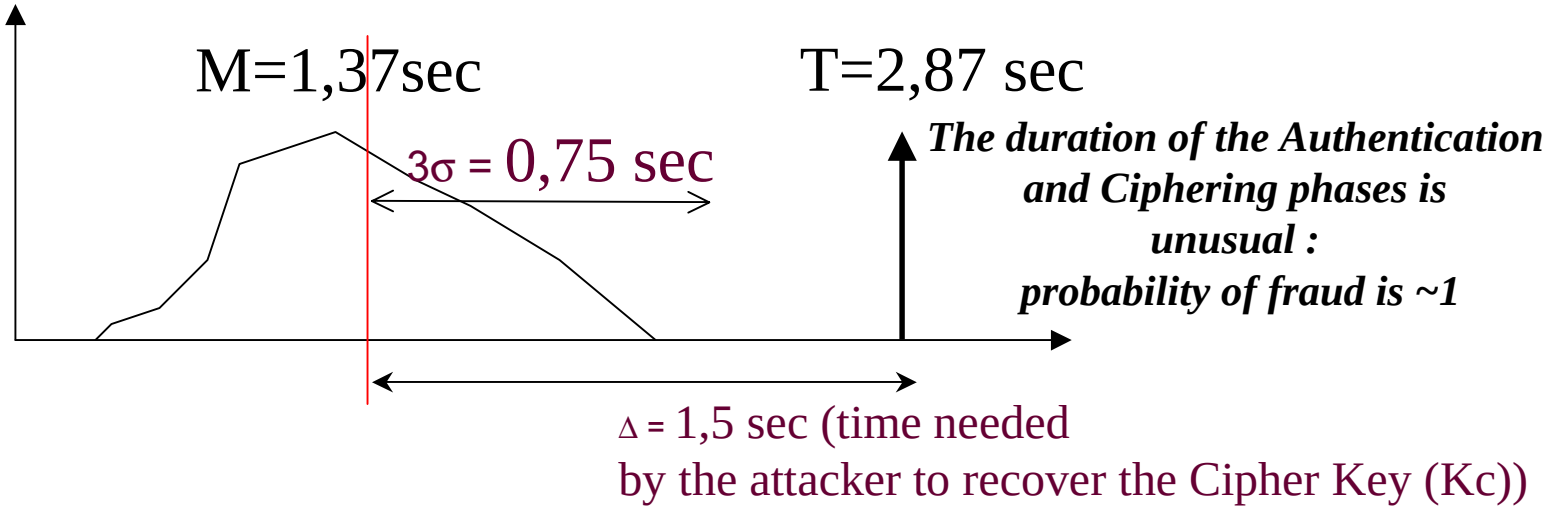


Attack hidden inside Authentication and Cipher Mode requests



Principles (1)

- a MIM attack needs at least 1,5 sec to be achieved after the CIMCPL message is sent by the SIM of the victim (2 SACCH are necessary to recover the Kc (Ciphering Key) ,
- the meantime measured on the BSC before the start of the ciphering is equal to 1,37 sec (AUTREQ & CIMCPL) in our network. The standard deviation for this measure is equal to 0,25 sec. (3x standard deviation corresponds to 99% of legitimate duration = 0,75 sec)



The detection of these abnormal events are theoretically easy.

Principles (2)

- In order to cover the 3 precedent attacks, we propose to follow 3 statistics based on response time. The measurements are set directly in the BSC for each communication context. We measure :
  - AUTREQ/AUTRES
  - CIMCMD/CIMCPL
  - AUTREQ/AUTRES + CIMCMD/CIMCPL
- Adaptive mode : the statistics are adaptive and may automatically follow local modifications.
- We propose to maintain histogram or statistic knowledge on the 10K last responses for each BSC (sliding window). Each valid communication (based on statistical test of reject) may be inserted in the statistic.

Manufacturer M1

- Network statistics delay
  - AUTH m = 1,04 sec σ = 0,261 sec
  - CIMCMD m = 0,29 sec σ = 0,15 sec
  - AUTH + CIMCMD m = 1,43 sec σ = 0,23 sec
  - 2 SACCH frames m = 720 sec [480 - 960]
- Delay for the optimised attack
- [auth + CIMCMD] + (overhead) + acq of 2 SACCH frames + CPU time for hacking
  - min : 0,87+(0,02)+0,480+1 = 2,37 sec
  - max : 2,55+ (0,02)+0,960+1 = 4,53 sec
  - mean : 1,44+ (0,02)+0,720+1 = 3,18 sec

	AUTRES-REQ	CIMCPL-CMD	CIMCPL-AUTRES
min	0,452	0,209	0,873
max	4,401	5,188	2,549
mean	1,049	0,393	1,438
standard deviation	0,261	0,151	0,227

2,12sec

Manufacturer M1

- 5699 measures
- 11 measures rejected on 3 sigma test (size of the dynamic sample : 500)
  - Test for each point of measure the condition : mean + 1,720sec (hyp : 1 sec of CPU + mean of 2 SACCH 720 ms)
- ***No point rejected***

Statistic for Manufacturer M2

Network statistics delay

- AUTH m = 0,84 sec σ = 0,30 sec
- CIMCMD m = 0,40 sec σ = 0,21 sec
- AUTH + CIMCMD m = 1,30 sec σ = 0,261 sec
- 2 SACCH frames m = 720 sec [480 - 960]

Delay for the optimised attack

[auth + CIMCMD] + (overhead) + acq of 2 SACCH frames + CPU time for hacking

- min : 0,79+(0,02)+0,480+1 = 2,29 sec
- max : 5,43+ (0,02)+0,960+1 = 7,41 sec
- mean : 1,30+ (0,02)+0,720+1 = 3,04 sec

	AUTRES-REQ	CIMCPL-CMD	CIMCPL-AUTRES
min	0,41	0,160	0,79
max	6,403	5,80	5,43
mean	0,845	0,40	1,301
standard deviation	0,3	0,209	0,261

2,084sec

Manufacturer M2

- 6863 measures
- 270 measures rejected on 3 sigma test (size of the dynamic sample : 500)
- Test for each point of measure the condition : mean + 1,720sec (hyp : 1 sec of CPU + mean of 2 SACCH 720 ms)
  - ***Only 57 points rejected***
- Modify the protocol for asking a complete new re-authentication phase for these 57 rejected points (offer a chance to communicate for allowed subscribers).

Conclusion

- Only BSC software needs to be modified (transparent for handsets),
- no (re)configuration is needed, the system computes its own statistical parameters (adaptive mode).
- It is easy to monitor the level of reject (attack profile) by modifying the scale of SD, (choose 2,6 SD (standard deviation) and not 3 SD to be more restrictive in your network and by example 3,4SD to be less restrictive)
- The test base on mean time + 1,720sec seems to be efficient
- Each rejected subscriber may be completely re-authenticate (2 times and drop ??)
- No problem of performances on BSC, it takes a very short time to compare the duration of each (AUTREQ-CIMCPL) with the “attack profile”.
- to extend the measurements, Opco can realise them on other BSC