A Student Grade Man in the Middle Attack on the GSM Air Link

Janis Danisevskis (TU-Berlin SECT)
janis@sec.t-labs.tu-berlin.de

TU-Berlin (SECT)
Spring 2010 SIDAR - Graduierten-Workshop über Reaktive Sicherheit

7. Juli 2010

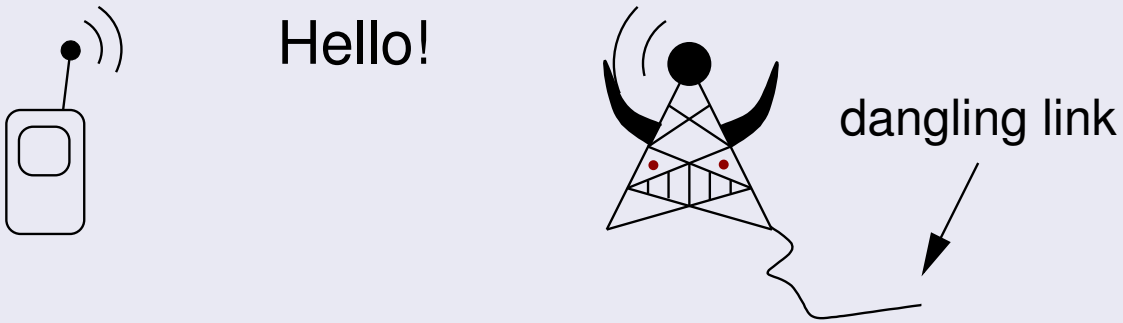
Outline

Some Basics

Some interesting Facts about GSM

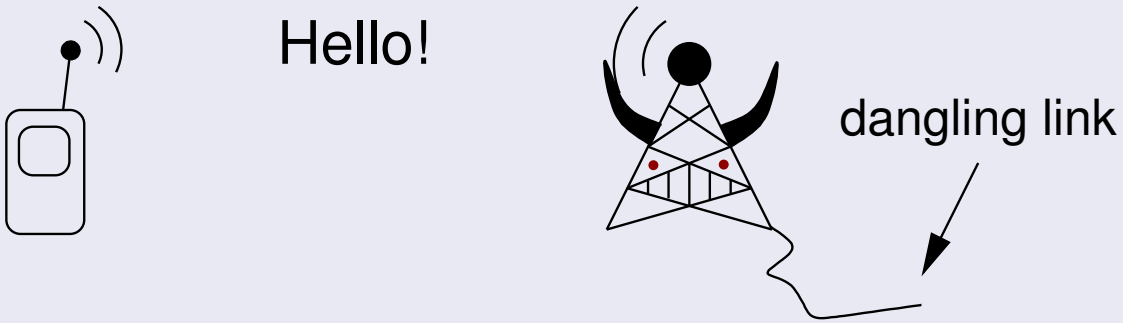
- no authentication needed towards Mobile Stations (MS)
- unencrypted air-links must always be supported by MS

Example: IMSI Catcher



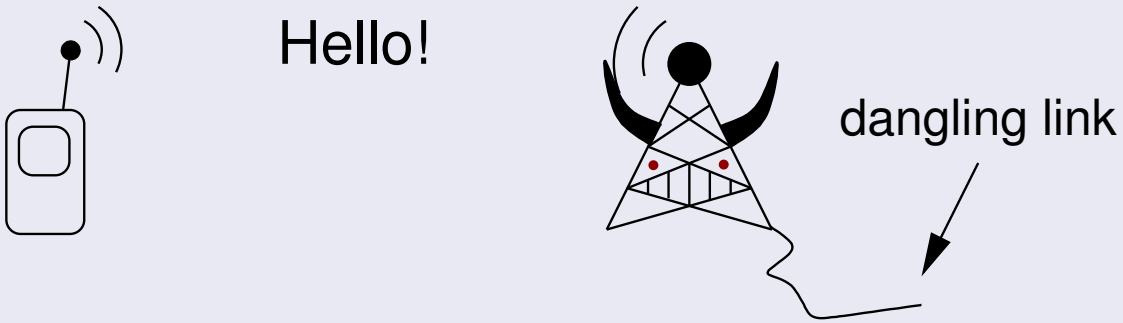
- Lure the victim into connecting to our Base station
- Tell it to use no encryption
- Reroute our victim's phone call
- Impersonate the callee

Example: IMSI Catcher



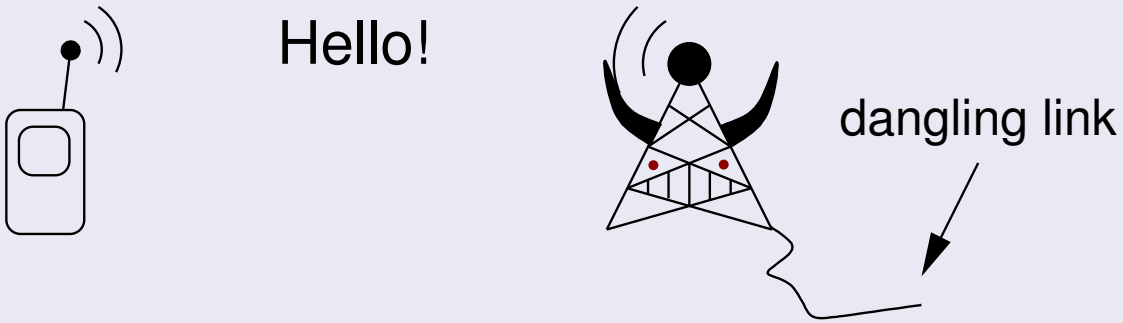
- Lure the victim into connecting to our Base station
- Tell it to use no encryption
- Reroute our victim's phone call
- Impersonate the callee

Example: IMSI Catcher



- Lure the victim into connecting to our Base station
- Tell it to use no encryption
- Reroute our victim's phone call
- Impersonate the callee

Example: IMSI Catcher

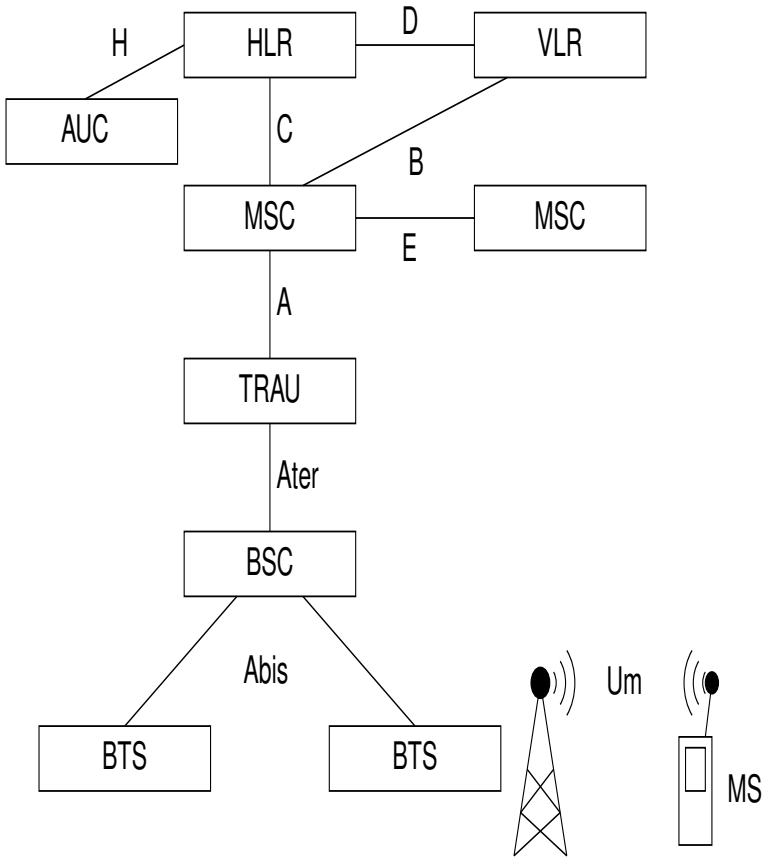


- Lure the victim into connecting to our Base station
- Tell it to use no encryption
- Reroute our victim's phone call
- Impersonate the callee

Drawbacks

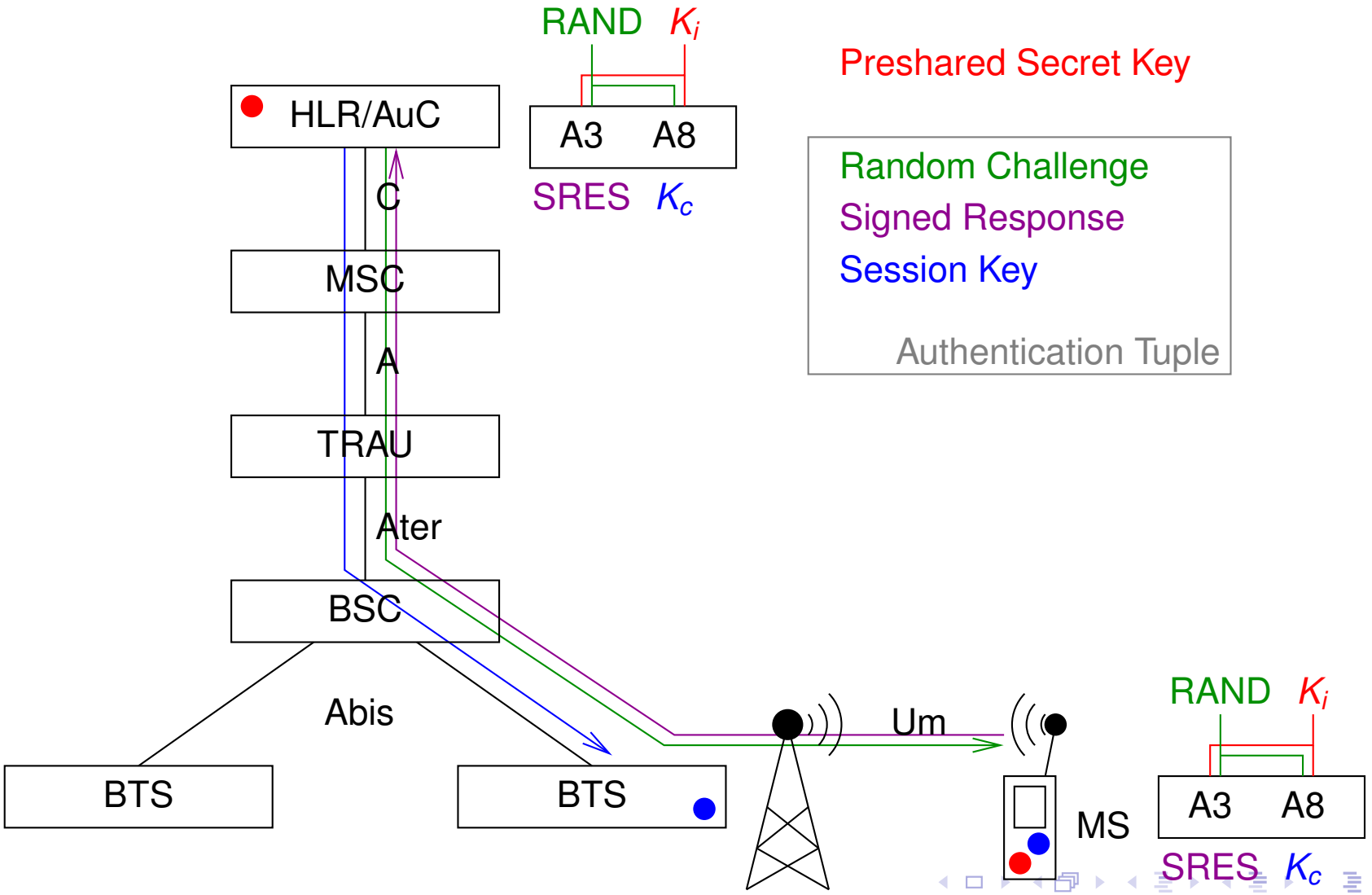
- The victim is not registered with his home network
  $\rightarrow$ can not be called
- The callee will not see the caller's phone number
- Not transparent

More GSM Basics



HLR	:	Home Location Register
AUC	:	Authentication Center
VLR	:	Visitor Location Register
MSC	:	Mobile Switching Center
TRAU	:	Transcoder Rate Adaptation Unit
BSC	:	Base Station Controller
BTS	:	Base Transceiver Station
MS	:	Mobile Station

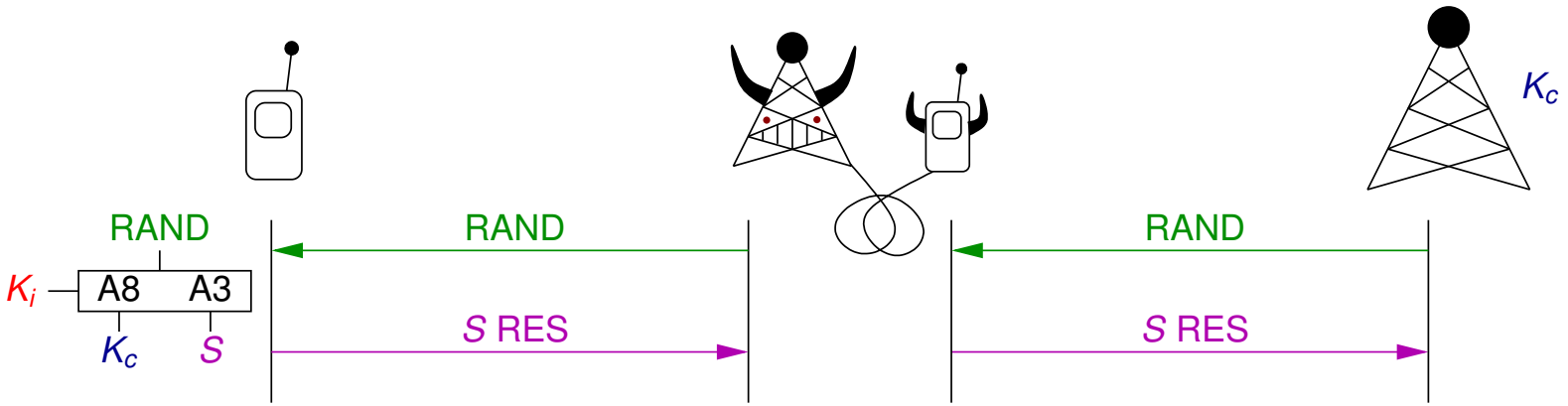
Authentication Tuple

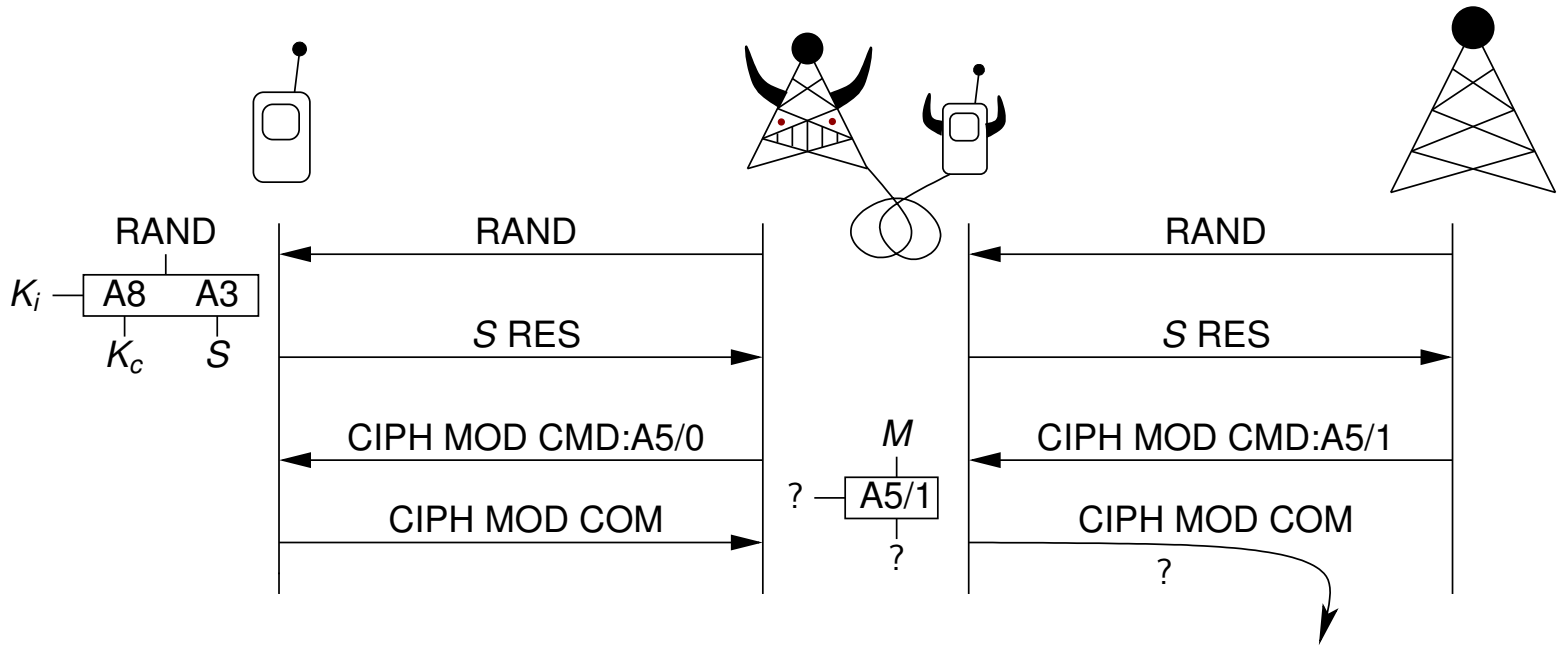


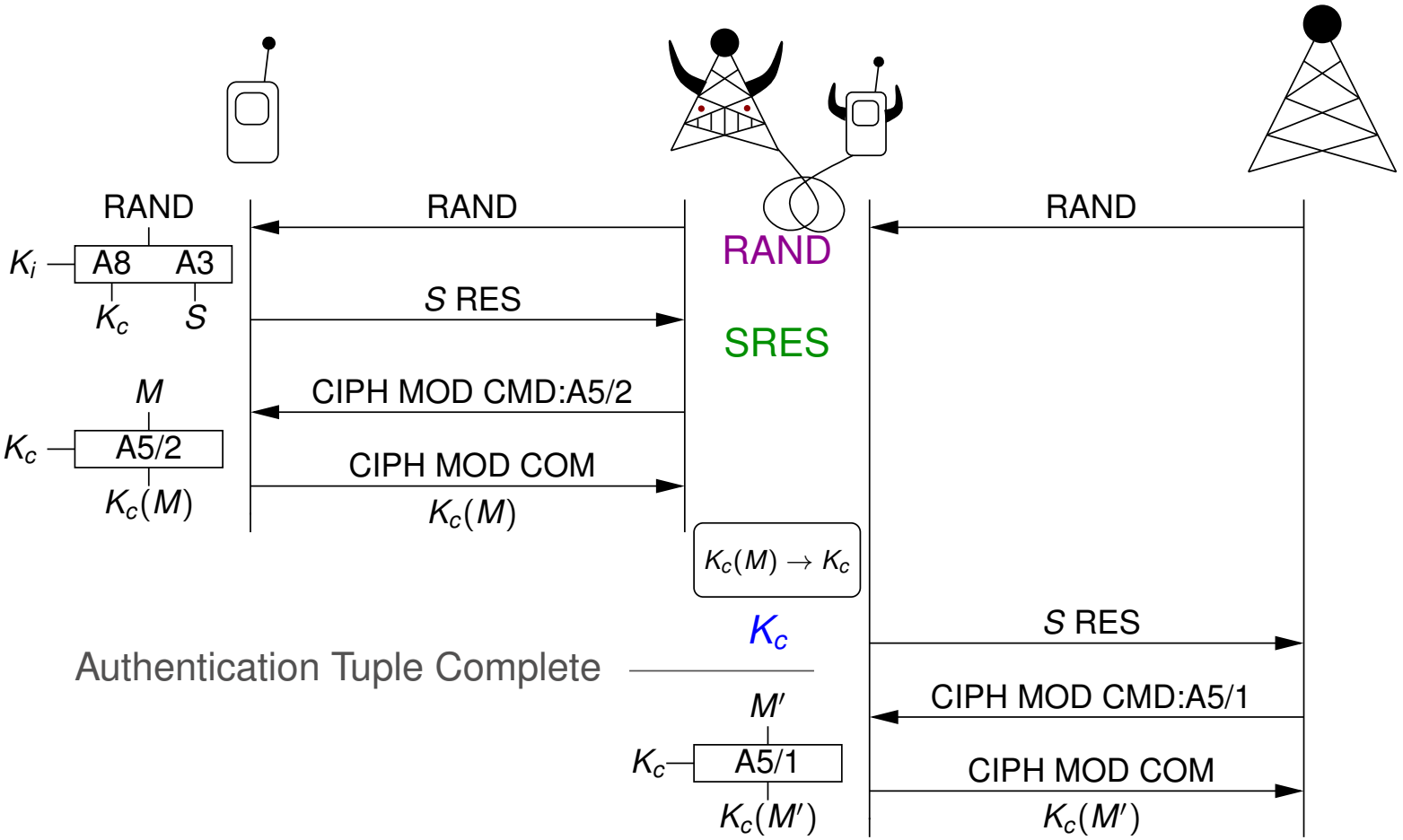
Preshared Secret Key

Random Challenge
Signed Response
Session Key

Authentication Tuple


RAND
RAND
RAND
K_i
A8
A3
K_c
S
S RES
S RES
K_c


RAND
RAND
RAND
K_i
A8
A3
K_c
S
S RES
S RES
CIPH MOD CMD:A5/0
CIPH MOD CMD:A5/1
M
?
A5/1
?
CIPH MOD COM
CIPH MOD COM
?


RAND
RAND
RAND
RAND
K_i
A8
A3
K_c
S
S RES
SRES
M
CIPH MOD CMD:A5/2
K_c
A5/2
CIPH MOD COM
$K_c(M)$
$K_c(M)$
$K_c(M) \rightarrow K_c$
K_c
S RES
Authentication Tuple Complete
M'
CIPH MOD CMD:A5/1
K_c
A5/1
CIPH MOD COM
$K_c(M')$
$K_c(M')$

Consequences

We can do anything the victim could do without her having a clue (untill her monthly phonebill arrives).

- Dynamic cloning

Extras

1. Wiretapping (including incoming calls)
2. Call hijacking (impersonate the victim)
3. On the fly modification (e.g. of SMS)
4. Receive SMS on the victim's behalf (think of mTAN)

Why?

Because ...

- Raise public awareness of GSM weaknesses
- These weaknesses are being exploited
- No governmental/corporate funding needed

Why?

Because ...

- Raise public awareness of GSM weaknesses
- These weaknesses are being exploited
- No governmental/corporate funding needed

The End

The End

Questions?