Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication

Nico Golde, Kévin Redon, Ravishankar Borgaonkar

Berlin Institute of Technology, Security in Telecommunications
femtocell@sec.t-labs.tu-berlin.de

NDSS 2012, San Diego, 6th February 2012
Introduction

- Mobile data traffic is rapidly increasing (3G, 4G), but coverage often bad

- Operators seek for solutions to offload traffic to other networks

- Introduction of small/cheap cells in residential environments (home)

- As of Q2 2011, 31 operators in 20 countries adopted femtocell technology (Vodafone, AT&T, SFR, NTT DoCoMo, ...)

What is a femtocell (HNB or FAP)?

- Small and cheap base station, small coverage (around 50m)
- Deployed in home environment (no tamper resistance)
- Connected to operator backend via Internet

- Reduce expenditure by offloading traffic from public infrastructure
- Low maintenance and installation costs
- Improved 3G coverage in buildings
- Location based services
Contributions

- **End-User risk assessment**
  - Demonstrate attacks violating confidentiality, integrity and availability of subscriber traffic

- **Femtocell/Infrastructure weakness analysis**
  - Network attacks originating from a femtocell and design shortcomings in current architectures

⇒ Implementation and evaluation in a real network
We assume a rooted device!

More information on the rooting process is available in: Ravishankar Borgaonkar, Kevin Redon and Jean-Pierre Seifert. "Security Analysis of a Femtocell device". 4th ACM International Conference on Security of Information and Networks (SIN)
Home Node B Subsystem (HNS)

HNS : Home Node B Subsystem
AN : Access Network

HNB : Home Node B
SeGW : Serving Gateway
TR-069 : Telecom-069
IPsec : Internet Protocol Security
GAN : Gateway Access Network
Iu,b : Uu interface
Iuh/GAN : Uu interface for GAN
Iu,CS : Uu interface for CS
Iu,PS : Uu interface for PS

RNS : Radio Network Subsystem

Node B
RNC

PSTN
VLR
MSC
CS : Circuit Switched

SGSN
PS : Packet Switched
HSS
CN : Core Network
HLS[AuC]

UICC [USIM]
Uu : User Uu interface
UE : User Equipment
MS : Mobile Station

ME

SecT / TU-Berlin
IMSI-Catching

- IMSI-Catching in GSM easy by just configuring the BTS with correct MCC/MNC
- In 3G subscribers are protected from IMSI-Catching by mutual authentication
- Authentication performed with the home network, not the actual cell
  ⇒ Femtocells by design provide network authenticity!

- Given device access it is possible to:
  - Reconfigure MCC/MNC
  - Open access for all subscribers (roaming allowed by SFR)
Over-the-Air traffic encrypted but **decrypted** on the femtocell

All traffic between femtocell and network is plaintext and only protected by IPsec

Hijacking control flow of IPSec tunnel software

⇒ Decode IPsec traffic, extract voice/SMS
⇒ Femtocells can be a very cheap IMSI-Catcher
What if we change the HNB-GW?
⇒ Full control over all communication

- Modify traffic, impersonating subscribers
- Relay messages to subscriber whenever authentication is required
- Demo implementation based on SMS: Modify messages or inject SMS on behalf of subscriber (will be billed)
Disconnecting subscribers in GSM via IMSI DETACH message (unauthenticated!)

Limited to a certain geographical location!

Femtocell networks have one dedicated VLR
⇒ Limitation vanishes
⇒ DoS against subscribers by detaching the complete femtocell network
Femtocells store various subscriber and location information (registered users, neighbour cells, ...)

3GPP specifications require Node-B's to submit measurement reports to a central entity.

Our device exposed a hidden technician web interface with broken authentication
⇒ Subscriber and femtocell data exposed!
⇒ No filtering for HNB↔HNB communication

Measurement reports are pushed to an FTP server, with a shared account!
Using neighbour cell list, you could, e.g., map femtocells.
Femtocell attack surface

- Attack surface limited:
  - Network protocols: NTP, DNS spoofing (not tested)
  - Services: webserver, TR-069 provisioning (feasible)
  - TR-069 is the de-facto standard for femtocell remote provisioning

- Both HTTP; TR-069 is based on SOAP and XML
  \( \Rightarrow \) Great potential for software vulnerabilities

- All services run as root

- Eventually we found a remote root vulnerability in the webserver (CVE-2011-2900)
  \( \Rightarrow \) Take over femtocell network
  \( \Rightarrow \) End-user threats become a global problem!
Possible infrastructure impact

- Signaling attacks a well known problem, e.g. HLR overload \(^1\)

- TCP/IP based communication allows for easy signaling traffic generation at a high rate
  \[\Rightarrow\] Given a remote root bug this can be amplified with a femtocell botnet

- Connect to femtocell network without femtocell!

- Act as femtocell by using network protocols

---

\(^1\) Traynor et al., On Cellular Botnets: Measuring the impact of Malicious Devices on a Cellular Core Network
This is a big mess

Given the history of rooted femtocells (Vodafone SureSignal, Samsung, SFR) security poorly implemented in practice

Inherent trust in the physical security of these low cost devices may be wrong

Femtocell security strongly affects subscriber privacy, authenticity, availability and operator network
Acknowledgements (in no particular order) & Questions

- Jean-Pierre Seifert
- Collin Mulliner
- Benjamin Michéle
- Dieter Spaar
- K2
- Nicholas Weaver

Thanks for the attention!
Questions?