Femtocells: a Poisonous Needle in the Operator's Hay Stack

Ravishankar Borgaonkar, Nico Golde, Kévin Redon

Technische Universität Berlin, Security in Telecommunications
femtocell@sec.t-labs.tu-berlin.de

Black Hat 2011, Las Vegas, 3rd August 2011
Agenda

- mobile telecommunication
- end-user attacks
- network attacks
1. UMTS architecture, femtocell definition, femtocell architecture
2. taking control over the device, reconfigure as IMSI-catcher, MitM 1: call interception, MitM 2: alter communication, MitM 3: inject traffic
3. collect information about the others, reconfigure other femtocells, taking control over other femtocells, playing with the operator network
UMTS architecture (complex)

Structure of an UMTS network

- ME: Mobile Equipment
- MT/TE: Mobile Terminal Equipment
- UE: User Equipment
- MS: Mobile Station
- USIM: Universal Subscriber Identity Module
- UICC: User Identity Module
- Node B
- RNC
- UTRAN: Universal Terrestrial Radio Access Network
- RNS: Radio Network System
- AN: Access Network
- PSTN: Public Switched Telephone Network
- VLR: Visitor Location Register
- HLR: Home Location Register
- AuC: Authentication Center
- GPRS: General Packet Radio Service
- GPRS PS: Packet Switched
- SGSN: Gateway GPRS Support Node
- GGSN: Gateway GPRS Support Node
- GMSC: Gateway Mobile Switching Center
- MGW: Mobile Gateway
- MSC: Mobile Switching Center
- HSS: Home Subscriber Server
- EIR: Equipment Identity Register
- CN: Core Network
1. UMTS is the 3G technology used in Europe (mainly), equivalent to CDMA2000 in USA
2. UMTS and CDMA2000 both 3G, UMTS made by 3GPP, CDMA2000 by 3GPP2
3. UMTS architecture is quite complex, with a lot of one lettered elements and interfaces
4. diagramm should scare the audience
5. UML link multiplexing used in diagramm
6. the hay are all these elements (on letter), forming the haystack (operator network)
UMTS architecture

UMTS architecture (simplified)

- ME: Mobile Equipment
- UICC: Universal Integrated Circuit Card
- UE: User Equipment
- MS: Mobile Station
- Uu: Signaling connection
- Cells
- NodeB
- RNC
- AN: Access Network
- UTRAN: Universal Terrestrial Radio Access Network
- RNS: Radio Network Subsystem
- CS-MGW: Circuit Switched Media Gateway
- CS: Circuit Switched
- IuCS: CS signaling connection
- SGSN: Serving GPRS Support Node
- PS: Packet Switched
- IuPS: PS signaling connection
- CN: Core Network

SecT / TU-Berlin
1. the three main components to keep in mind are:
2. MS (mobile station) ⇔ end-user equipment: the mobile phone
3. AN (access network) ⇔ link between MS and CN
4. CN (core network) ⇔ back-end for communication routing. critical infrastructure
5. CN is further divided into CS (Circuit Switched) for voice and PS (Packet Switched) for data traffic
What is a femtocell?

- a small access point
- connects the mobile phone to the 3G/UMTS network
- compatible with every UMTS enabled mobile phone
- small cell, with a coverage of less than 50m
- low power device
- easy to install: you only have to provide power and Internet access
- technical name in 3G: Home Node B (HNB)
definition and use of femtocell technology

1. coverage area depends on exact model, operator and residential/business/...
2. sometimes called FAP (Femtocell Access Point)
advantages provided to users:

- can be installed at home to improve 3G coverage
- high bandwidth, and high voice quality
- location based services
1. femtocell is an personal base station, not shared with the rest of the public
2. location service example: kids arriving at home
advantages for mobile operators:

- traffic offload from public operator infrastructure → reduce expenditure
- cheap hardware compared to expensive 3G equipment
- no installation and maintenance cost
- IP connectivity
operator advantages

advantages for mobile operators:
- traffic offload from public operator infrastructure → reduce expenditure
- cheap hardware compared to expensive 3G equipment
- no installation and maintenance cost
- IP connectivity

1. the user has to buy the equipment and provide power/network
2. location-based services and high dedicated bandwidth offer new revenue possibilities
3. TCP/IP is well known, easy and cheap. The equipment tends to use this protocol
4. femtocells are a great opportunity for the operators
5. but now a part of their infrastructure is in the user's hand
Home Node B Subsystem (HNS)

- **RNS**: Radio Network Subsystem
- **Node B**
- **I_{ub}**
- **I_{uh/}**
- **GAN**
- **IPsec**
- **SeGW**
- **TR-069**
- **HNB-GW**
- **HMS**
- **OAMP**
- **I_{u}CS**
- **I_{u}PS**
- **PSTN**
- **VLR**
- **MSC**
- **CS**: Circuit Switched
- **SGSN**
- **PS**: Packet Switched
- **HSS**: [HLS, AuC]
- **CN**: Core Network
- **Internet**
1. HNS is equivalent to the RNS in the AN
2. HNB ⇔ Node-B (entry node for phone connection), HNB-GW ⇔ RNC (connected to the CN)
3. unlike the Node-B, a HNB is physically accessible by the user
4. the SeGW is required to provide privacy due to the use of the internet connection. It provides access control and encryption for communication
5. the HNB is the needle (in the haystack), we will make it poisonous
advantages

small cells

macrocells

<table>
<thead>
<tr>
<th>Scale</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$10^0$</td>
<td>cell</td>
</tr>
<tr>
<td>$10^{-3}$</td>
<td>mini</td>
</tr>
<tr>
<td>$10^{-6}$</td>
<td>micro</td>
</tr>
<tr>
<td>$10^{-9}$</td>
<td>nano</td>
</tr>
<tr>
<td>$10^{-12}$</td>
<td>pico</td>
</tr>
<tr>
<td>$10^{-15}$</td>
<td>femto</td>
</tr>
<tr>
<td>$10^{-18}$</td>
<td>atto</td>
</tr>
</tbody>
</table>
1. femtocells are very small cells (as the scale shows)
2. a cell is defined by the antenna and the area covered by its signal
3. attocells have been presented at the World Mobile Congress (http://ubiquisys.com/femtocell-blog/what-is-an-attocell-new-personal-femtocell-technology/)
### HNB threats listed by the 3GPP

<table>
<thead>
<tr>
<th>Group</th>
<th>#</th>
<th>Threat</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compromise of H(e)NB Credentials</td>
<td>1</td>
<td>Compromise of H(e)NB authentication token by a brute force attack</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>via a weak authentication algorithm</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>Compromise of H(e)NB authentication token by local physical intrusion</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>User cloning the H(e)NB authentication Token. User cloning the H(e)NB</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>authentication Token</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>Inserting valid authentication token into a manipulated H(e)NB</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>Booting H(e)NB with fraudulent software (&quot;re-flashing&quot;)</td>
<td>up to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>disastrous</td>
<td></td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>Physical tampering with H(e)NB</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>26</td>
<td>Environmental/side channel attacks against H(e)NB</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>21</td>
<td>Radio resource management tampering</td>
<td>harmful</td>
</tr>
<tr>
<td>Attacks on Radio resources and management</td>
<td>5</td>
<td>Man-in-the-middle attacks on H(e)NB first network access</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>15</td>
<td>Denial of service attacks against H(e)NB</td>
<td>annoying</td>
</tr>
<tr>
<td></td>
<td>17</td>
<td>Compromise of an H(e)NB by exploiting weaknesses of active network</td>
<td>extremely</td>
</tr>
<tr>
<td></td>
<td></td>
<td>services</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>25</td>
<td>Manipulation of external time source</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>27</td>
<td>Attack on OAM and its traffic</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>28</td>
<td>Threat of H(e)NB network access</td>
<td>harmful</td>
</tr>
<tr>
<td>Protocol attacks on a H(e)NB</td>
<td>11</td>
<td>Changing of the H(e)NB location without reporting</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Software simulation of H(e)NB</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>Traffic tunnelling between H(e)NB</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>Misconfiguration of the firewall in the modem/router</td>
<td>annoying</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>Denial of service attacks against core network</td>
<td>annoying</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>H(e)NB announcing incorrect location to the network</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Eavesdropping of the other user’s UTRAN or E-UTRAN user data</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Masquerade as other users</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>User’s network ID revealed to Home (e)NodeB owner</td>
<td>breaking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>users privacy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>22</td>
<td>Masquerade as a valid H(e)NB</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Provide radio access service over a CSG</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Fraudulent software update / configuration changes</td>
<td>extremely</td>
</tr>
<tr>
<td></td>
<td></td>
<td>changes</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>Misconfiguration of H(e)NB</td>
<td>irritating to harmful</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>Mis-configuration of access control list (ACL) or compromise of the</td>
<td>irritating to harmful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access control list</td>
<td></td>
</tr>
</tbody>
</table>

### Attacks on the core network, including H(e)NB location-based attacks

<table>
<thead>
<tr>
<th>Group</th>
<th>#</th>
<th>Threat</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>11</td>
<td>Changing of the H(e)NB location without reporting</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>12</td>
<td>Software simulation of H(e)NB</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>13</td>
<td>Traffic tunnelling between H(e)NB</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>14</td>
<td>Misconfiguration of the firewall in the modem/router</td>
<td>annoying</td>
</tr>
<tr>
<td></td>
<td>16</td>
<td>Denial of service attacks against core network</td>
<td>annoying</td>
</tr>
<tr>
<td></td>
<td>24</td>
<td>H(e)NB announcing incorrect location to the network</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>9</td>
<td>Eavesdropping of the other user’s UTRAN or E-UTRAN user data</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>10</td>
<td>Masquerade as other users</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>18</td>
<td>User’s network ID revealed to Home (e)NodeB owner</td>
<td>breaking</td>
</tr>
<tr>
<td></td>
<td></td>
<td>users privacy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>22</td>
<td>Masquerade as a valid H(e)NB</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>23</td>
<td>Provide radio access service over a CSG</td>
<td>very harmful</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>Fraudulent software update / configuration changes</td>
<td>extremely</td>
</tr>
<tr>
<td></td>
<td></td>
<td>changes</td>
<td>harmful</td>
</tr>
<tr>
<td></td>
<td>19</td>
<td>Misconfiguration of H(e)NB</td>
<td>irritating to harmful</td>
</tr>
<tr>
<td></td>
<td>20</td>
<td>Mis-configuration of access control list (ACL) or compromise of the</td>
<td>irritating to harmful</td>
</tr>
<tr>
<td></td>
<td></td>
<td>access control list</td>
<td></td>
</tr>
</tbody>
</table>
1. the 3GPP and operators are aware of the threats generated by femtocells
2. the threats are briefly described, with their effects and mechanism to prevent them
3. it is not a howto for attacks though (too vague), but a general overview of dangers
SFR femtocell

- sold by SFR (2nd biggest operator in France)
- cost: 99€ + mobile phone subscription
- hardware: ARM9 + FPGA for signal processing
- OS: embedded Linux kernel + proprietary services
- built by external vendors (in our case Ubiquisys), configured by operator
1. a brief description of our femtocell
2. all attacks have been performed with this model from SFR
3. however, the attack concepts apply to all femtocells, only the implementation varies
4. as hardware + software comes from the vendor and configuration is done by the operator, all fuckups are shared among them ;)

SFR femtocell
- sold by SFR (2nd biggest operator in France)
- cost: 99€ + mobile phone subscription
- hardware: ARM9 + FPGA for signal processing
- OS: embedded Linux kernel + proprietary services
- built by external vendors (in our case Ubiquisys), configured by operator

Rogue femtocell
- Femtocells provide a recovery procedure similar to a factory reset.
- New firmware is flashed, and settings are cleared.
- Used to "repair" the device without any manual intervention.

Diagram:
- Femtocell
- OAM
- Getting parameter and firmware list:
  - HTTPS (client certificate)
- Clear text over HTTPS
- Getting new firmware (if different):
  - HTTP
  - Firmware encrypted and signed
Femtocells provide a recovery procedure similar to a factory reset. New firmware is flashed, and settings are cleared. It is used to "repair" the device without any manual intervention.

1. Remember: keep it cheap
2. Operators do not want to send a technical team to repair the femtocell
3. Users are responsible for the femtocell
4. The diagram shows a simplified procedure. The complete procedure has already been presented in other confs.
- Firmware server is not authenticated

- Public key is in parameter and firmware list, which is not signed

---

recovery to fail
1. the recovery procedure has a security flaw: it does not authenticate the image server
2. attacker can push his own configuration and firmwares
3. the images are signed, but the public key can be provided in the configuration file (which is not signed)
4. devices can be cloned (except for the SIM)
5. we were able to analyze the procedure because an unencrypted recovery image could be retrieved. this has been fixed, but we now have the tools to decrypt them
6. however, there are still other ways to get unencrypted images ;)

mobile telecommunication
rogue femtocell
recovery to fail
debug traces

- based on local_trace_config.txt
- heavy use of dbg_trace (libosal.so)
- LD_PRELOAD db_trace to export traces
- still not very verbose (see next slide)
disabling limited trace

- all trace levels set to 1
- limited trace option compiled in libosal.so (needs patching)
Understanding the box: final traces

Reply: 60 00 11 00 00 00 00 54 6F 40 04 00 11 00 44 01 02 01 1C 90 00 05
Command: 60 00 05 00 A0 B2 01 04 1C 6E
Reply: 60 00 1E 00 4D 6E 62 0E 8F 20 53 52 52 FF FF FF FF FF FF FF FF FF FF
usim_send_sc_id_response: IMSI: 0000000000000000
usim_send_sc_id_response: MSISDN
CPU Load Total=0%
SC_Main: message received, id = 0x10, if = 0x10e
Mem (KB): 62808 tot, 40432 used, 22376 free, 8244 buff, 17856 cache
CPU Load Total=0%
gac_tu3903_callback called
gac_thread_proc, Message received in state 1, Interface ID 24095, Message ID 34,
gac_thread_proc: Message received in state 1, Interface ID 24095, Message ID 34,
gac_idle called
Message 34 on IF_ID_SELF interface, state GAC_IDLE
TU3903 message received,
gac_request_ipsec called
Performing DNS lookup of qdn uncl-ch1.fr.sfr.com
gac_dns_lookup called
Calling gethostbyname with qdn uncl-ch1.fr.sfr.com,
gac_tu3903_callback exiting
Retrieved IPV4 address
Calling gac_ipsec_build_send_tunnel_req with IP address 0x0 for qdn uncl-ch1.fr.sfr.com
gac_ipsec_build_send_tunnel_req called
Sending tunnel_req with qdn uncl-ch1.fr.sfr.com
Sending tunnel_req with IP
gac_ipsec_build_send_tunnel_req: starting timer with value 120
gac_ipsec_build_send_tunnel_req exiting
gac_request_ipsec exiting
Changing state to GAC_CONNECTING_IPSEC_INITIAL
gac_idle exiting returning 2
SC_Main: message received, id = 0x215, if = 0x5e1f
SC -> SC: SC_HLR_PERIODIC_METRIC_TIMER_EXPIRED
ScHlr::handlePeriodicMetricTimerExpire;
u32 ScHlr::getUEsCampedOn() const: 0 UEs camped-on
SC -> APM: APM_PERFORMANCE_IND[52]= 0, avg= 1
ScMsgManager::getPrMqHandle: state error interface 0x115
build_and_send_apm_performance_ind; getPrMqHandle() returned null pointer
SC_Main: message received, id = 0x210, if = 0x5e1f

© mobile telecommunication
✗ end-user attacks
✗ network attacks

SecT / TU-Berlin
any attacks hmm?

WHAT NOW?
requirements

- classical approach in GSM: IMSI-Catcher
  - fake operator BTS (MCC/MNC)
  - acts as MitM between operator and victim
  - phone usually can't detect
  - usually used to track and intercept communication

- UMTS standard requires mutual authentication
  ⇒ GSM approach not working \(^1\)

- no devices acting as UMTS base station + code is available

\(^{1}\)some attacks by using protocol downgrades are known
end-user attacks

- intercepting communication

requirements

2. no openBTS or openBSC project for UMTS exists
3. USRP is capable of doing it, but no implementation exists

---

1. classical approach in GSM: IMSI-Catcher
   - fake operator BTS (MCC/MNC)
   - acts as MitM between operator and victim
   - phone usually can't detect
   - usually used to track and intercept communication
2. UMTS standard requires mutual authentication
   - GSM approach not working
3. no devices acting as UMTS base station + code is available

---

1. some attacks by using protocol downgrades are known
in case of femtocell: mutual authentication also provided
⇒ but it's useless 😊

- mutual authentication is done with the **home operator**
- NOT with the actual cell
⇒ the femtocell forwards the authentication tokens
⇒ mutual authentication is performed even with a rogue device
How to build a 3G IMSI-Catcher:

- Cell configuration is kindly provided as a feature of femtocells
- Local cell settings stored in a proprietary database format
- Some comfort provided → web interface

- We can catch any phone user of any operator into using our box
- Roaming subscribers are allowed by SFR

⇒ the femtocell is turned into a full 3G IMSI-Catcher
end-user attacks
intercepting communication
getting the fish into the octopus' tentacles

1. there is an operator web interface (main) and a vendor web interface (hidden)
2. they are password protected, but easily accessible (just get a valid cookie to override the auth)
3. roaming might be allowed because the HNB-GW is only forwarding the traffic, without filtering
4. users are handled the same way as in a real operator network
5. collecting IMSI (even without call interception) is already a privacy threat
6. roaming notification can be dropped on the way (shown later)
 Intercepting traffic

- proprietary IPsec client + kernel module (xpressVPN)
- multiple ways to decrypt IPsec traffic: NETLINK, ip xfrm state (not available on SFR box)
- we decided to hijack/parse ISAKMP messages passed via sendto(2) glibc wrapper
- voice data encapsulated in unencrypted RTP stream (AMR codec, stream format)
1. there are several ways to get decrypted traffic. the easiest is probably netlink
2. we don't need the decrypted traffic on the box, so we just extract the keys before they are passed to the PF_KEY2 kernel interface and decrypt traffic on our gateway
3. details of GAN will be presented later
extracting voice

- LD_PRELOAD ipsec user-space program to hijack sendto() and extract keys
- pass key material to host running tcpdump
- decrypt ESP packets
- extract RTP stream (rtpbreak)
- opencore-based (nb) utility to extract AMR and dump to WAV
DEMONSTRATION

interception
but what about over-the-air encryption?

- only the phone ↔ femtocell OTA traffic is encrypted
  ⇒ encryption/decryption happens on the box

- femtocell acts as a combination of RNC and Node-B: receives cipher key and integrity key from the operator for OTA encryption

<table>
<thead>
<tr>
<th>Protocol</th>
<th>info</th>
</tr>
</thead>
<tbody>
<tr>
<td>UMA</td>
<td>GA-C SR UPLINK DIRECT TRANSFER (DTAP) (MM) Authentication Resp</td>
</tr>
<tr>
<td>UMA</td>
<td>Unknown URR (144)</td>
</tr>
</tbody>
</table>

- reversing tells us: message is **SECURITY MODE COMMAND** (unspecified RANAP derivate), which includes the keys
1. OTA encryption only is by design: there is no end-to-end encryption in telco network. Every element performs a task. The communication is unencrypted in the AN/CN.
2. The operator network is usually closed and trusted.
3. We didn't find any standard, but seems to be a 3xTLV: (algorithm, integrity key), (key status), (algorithm list, encryption key).
derived from RANAP, but spec unknown
end-user attacks
intercepting communication
SECURITY MODE COMMAND

1. thanks Dieter Spaar for help on this one!
femtocell operator communication: the GAN protocol

- device is communicating with operator via GAN protocol (UMA)
  - TCP/IP mapped radio signaling
  - encapsulates radio Layer3 messages (MM/CC) in GAN protocol
  - one TCP connection per subscriber
  - radio signaling maps to GAN messages are sent over this connection

- GAN usage is transparent for the phone
1. GAN is not the only I_u_h solution. I_u_b and IMS are the other alternatives
2. GAN is the standardized term for UMA
3. GAN is defined in 3GPP TS43.318 and TS44.318
4. GAN was designed to be used between MS and GANC over WLAN
**GAN proxy/client**

- proxies all GAN connections/messages
- reconfigure femtocell to connect to our proxy instead of real GANC
- proxy differs between GAN message types
- attack client controls GAN proxy over extended GAN protocol
SMS message filtered by GAN proxy
modified by client
transfered to real GANC

Unlicensed Mobile Access
Length Indicator: 38
0000 .... = Skip Indicator: 0
.... 0001 = Protocol Discriminator: URR (1)
URR Message Type: GA-CSR UPLINK DIRECT TRANSFER (112)

L3 Message
URR Information Element: L3 Message (26)
URR Information Element length: 34
.... 1001 = Protocol discriminator: SMS messages (9)
L3 message contents: 39011f00010007913306091093f013151c0f810094712627...

GSM A-I/F DTAP - CP-DATA
GSM A-I/F RP - RP-DATA (MS to Network)
GSM SMS TPDU (GSM 03.40) SMS-SUBMIT

0... .... = TP-RP: TP Reply Path parameter is not set in this SMS SUBMIT/DELIVER
.0... .... = TP-UDHI: The TP UD field contains only the short message
..0. .... = TP-SRR: A status report is not requested
.... 1 0... = TP-VPF: TP-VP field present - relative format (2)
..... .1.. = TP-RD: Instruct SC to reject duplicates
.... ..01 = TP-MTI: SMS-SUBMIT (1)
TP-MR: 28

TP-Destination-Address - (0049176272385)

TP-PID: 0
TP-DCS: 0
TP-Validity-Period: 63 week(s)
TP-User-Data-Length: (3) depends on Data-Coding-Scheme

TP-User-Data
SMS text: Tdd
1. client indicates it is waiting for a SMS
2. proxy identifies uplink direct transfer, L3 body + type SMS
3. forwards message to attacking client
4. client decodes TPDU and destination number
5. adjusts according to our needs and re-injects into the proxy
6. proxy transfers it to the GANC
DEMONSTRATION

SMS modification
how about impersonating subscribers?

- lets use services for free, billed to a victim
- client requires subscriber information
- proxy additionally caches subscriber info (TMSI/IMSI) for each MS-GANC connection
- phone needed for authentication
- applies to any traffic (SMS, voice, data)
- victim is impersonated
1. client requests subscriber information from the proxy (IMSI/TMSI)
2. issues a service request (call, data, sms, ...) with subscriber information
3. network asks for authentication
4. attack client can't answer this because the secret stored on the victims USIM is required to compute response
5. proxy pages victim and forwards the AUTH request
6. victim assumes a service is coming in, answers AUTH request
7. proxy relays response to the operator and notifies client about the new state
8. client continues injecting messages on behalf of the victim, free for the attacker, billed to the user
9. injection can also work the other way round, to attack phones
DEMOnSTRATION

SMS injection
IMSIs'ing non-local subscribers

return of the IMSI detach

- IMSI detach DoS discovered by Sylvaint Munaut in 2010 \(^2\)
  - results in discontinued delivery of MT services (call, sms,...)
  - network assumes subscriber went offline
- detach message is unauthenticated
- however, this is limited to a geographical area (served by a specific VLR)
- user can not receive calls

\(^2\)http://security.osmocom.org/trac/ticket/2
an attacker can send an IMSI detach message to cause an interruption of mobile terminated services

2. MSC forwards detach message to VLR and marks the subscriber as detached

3. VLR notifies HLR of the detach via Location Cancel Request

4. as a result the network assumes the subscriber is not available anymore

5. this is limited to a geographical area

6. if you fake an IMSI detach with subscriber information unknown to your current VLR, the message will be ignored

7. so the attack works only against victims in the same VLR
proximity constraint not existent in femtocell network

devices reside in various geographical areas

but all subscribers meet in one back-end system → and they are all handled by one femtocell VLR (at least for SFR) 😊

we can send IMSI detach payloads via L3 msg in GAN

⇒ we can detach any femtocell subscriber, no proximity needed!
DEMONSTRATION

IMSI detach

[Image of two people with pitchforks in a field]
attacking other femtocells

- attack surface limited:
  - network protocols: NTP, DNS spoofing (not tested)
  - services: webserver, TR-069 provisioning (feasible)

- both HTTP. TR-069 is additionally powered by SOAP and XML

- lots of potential parsing fail

- all services run as root
network attacks

1. the attack surface of the femtocell from a network attackers perspective is rather limited
2. all devices make heavy used of NTP and DNS, besides IPsec
3. NTP functionality is based on ntpdate. used as a reliable clock source for frequency stability
4. DNS is done by libc functionality. used to identify operator services
5. both based on UDP, thus spoof'able (NTP also not using authentication headers
6. mentioned web services are accessible from within the network
7. and TR-069 is open so that the femtocell operator can push updates
8. way more potential to find bugs by reversing the software
we went for the web service (wsal)

based on shttpd \(^3\)/mongoose \(^4\)/yassl embedded webserver

we found a stack-based buffer overflow in the processing of HTTP PUT requests

direct communication between femtocells is not filtered by SFR

exploit allows us to root *any* femtocell within the network

www.sec.t-labs.tu-berlin.de/~nico/wsal_root.py

\(^3\)http://docs.huihoo.com/shttpd/
\(^4\)http://code.google.com/p/mongoose/
1. we decided to audit the web service in more detail, both because of the good knowledge about involved protocols and as we later found out the service is based on an open source project
2. we discovered a buffer overflow in the PUT processing
3. PUT itself is not much of value because the web server directory is read-only and directly traversal is handled by the web service
4. however the buffer overflow itself allows us to reliably root other devices
5. this is extremely serious because most of the previous threat now leverage from a local problem to a global problem
DEMONSTRATION

remote root
collecting subscribers

- other femtocell are accessible within the network
- website is also accessible
- leaks **phone number** and IMSI of registered subscriber
- **wink** IMSI detach $\Rightarrow$ detach whole network

![Status page with IMSI and MSISDN information]
network attacks

god mode

- collecting subscribers

1. scraping can easily be done
2. there is a lot more info: access mode, software version,
   ...
3. the scraped IMSIs can be abused to build a database and detach all subscribers at once
4. would block incoming services for the whole network
locating subscribers

- Location verification performed by OAM
- Femtocell scan for neighbour cells
1. Location verification is a security aspect defined by the specification.
2. Used to enforce femtocell location, avoid roaming evasion, respect radio licenses, ...
3. Other methods are: geoIP and GPS (if available on the board).
global control

- web-site/database is not read-only
- OAMP, image and GAN server can also be set
- or using root exploit
- traffic can be redirected to our femtocell (either settings or iptables)

⇒ any femtocell can be flashed
⇒ any femtocell subscriber communication can be intercepted, modified and impersonated
HNS servers run typical Open Source software, not especially secured, e.g:

- MySQL, SSH, NFS, Apache (with directory indexing), ... available
- FTP used to submit performance measurement reports, including femtocell identity and activity
- all devices share the same FTP account
- vsftpd users are system users, SSH is open :D
advanced access

- SeGW is required to access the network
- authentication is performed via the SIM (removable)
- how about configuring an IPsec client with this SIM?
  - no hardware and software limitation
  - no femtocell required anymore
  - femtocells don't act as a great wall to protect the operator network anymore :D
attacks on operator network

signaling attacks (not blocked)

free HLR queries

leveraging access to:

- other Access Networks
- Core Network

...
other femtocell research

- THC vodafone [http://wiki.thc.org/vodafone](http://wiki.thc.org/vodafone), rooted in 2009, unfortunately bug fixed since 2 years
- Samsung femtocell
- Clearly shows that this is no single operator problem and might cause some pain
- Femtocell architecture is defective by design, security wise
1. operator infrastructure is trusted, weakly secured
2. femtocells are physically accessible by attackers
3. compromised devices endangers the mobile telecommunication network infrastructure
thanks (in no particular order)

- Jean-Pierre Seifert
- Collin Mulliner
- Benjamin Michélé
- Dieter Spaar
- K2
network attacks
god mode

thanks (in no particular order)

1. hay collecting pictures: Basil & Tracy,
   http://www.flickr.com/photos/basilb/
2. hole in haystack pictures: funkypancake,
   http://www.flickr.com/photos/funkypancake/
3. hay eater: Seattle Roll,
   http://www.flickr.com/photos/seattle_roll/
thank you for your attention

questions?
Nico Golde <nico@sec.t-labs.tu-berlin.de>
@iamnion

Kévin Redon <kredon@sec.t-labs.tu-berlin.de>

Ravi Borgaonkar <ravii@sec.t-labs.tu-berlin.de>
@raviborgaonkar

or just femtocell@sec.t-labs.tu-berlin.de

all material from this talk (including tools) will be available one week after Black Hat at:
http://tinyurl.com/sectfemtocellhacks
extended coverage

- femtocells have a small coverage (by definition, 25-50m)
- signal range can be increased using amplifier and external antenna
network attacks
  god mode
  extended coverage

1. the board has an antenna connector
2. used to test the device while/after manufacturing, without emitting into the air