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

Ravishankar Borgaonkar, Nico Golde and Kevin Redon
Security in Telecommunications
Technische Universität Berlin and Deutsche Telekom Laboratories
{ravii,nico,kredon}@sec.t-labs.tu-berlin.de

Abstract

Femtocells are an emerging technology deployed by operators around the world to enhance 3G connectivity and offload increasing data traffic. These secured devices are installed in the customers home and connect the mobile phone to the mobile network operator's network using an existing broadband connection.

Various researchers (including us) have shown in the past that these devices are not secure and it is possible to compromise these devices. However, nobody has actually published further attacks that utilized the device. We will give a short introduction to femtocell technology and show different attacks based on a rogue femtocell. These attacks can target end-users being logged into a femtocell, femtocell owners, as well as network operators.

1 Introduction

As a consequence of the rise of smartphones and inexpensive data flatrates, the load on UMTS networks has significantly increased. Network operators try to solve this problem, by offloading traffic to other technology such as Wi-Fi or femtocells. Femtocells as well as wireless access points are used a substitute for the traditional Base Transceiver Station (BTS) or the 3G equivalent Node B. In 2010, roughly 31% of the global smartphone traffic has been offloaded to fixed-line networks [5]. This includes femtocells.

A femtocell is a small, inexpensive 3G base station that a customer buys (sometimes it is even for free) from the operator. It is installed in his home or business environment and connected to the operator network via the existing broadband connection of the customer (usually DSL). By doing so, operators solve the problem of offloading there traffic and at the same time provide the customer with perfect 3G coverage at his home. Contrary to using Wi-Fi for offloading purposes, femtocells have the advantage for a customer, that the mobile phone does not need to implement a second stack besides the normal mobile telephony stack. The usage of a femtocell device is completely transparent for the mobile phone, as it will not notice any difference between the normal operator and the femtocell access point.

However this seemingly great and cheap solution also involves risks. As this is the first time that operators deploy to the users a piece of hardware and software that is traditionally deployed at locations where an attacker can not get physical access to the device, these devices have to be secure. Gaining control over such a device opens up the operator network, as well as a number of attacks utilizing this device.

The femtocell security is divided into two parts. On the one hand, the device has to be properly authenticated to the operator network. On the other hand, it is very important that all data traffic across the untrusted backhaul connection between femtocell and operator backend is actually secure. Femtocells support the necessary security features that a base station provides; in particular mutual authentication, encryption and integrity over the wireless link. However there are two issues. One is, using an existing wired broadband connection as backhaul is a

challenge, as the provider of the backhaul is not necessarily the same as the provider of femtocell. The second is, security of the femtocell device is vital and different from the standard base station. Adversaries can get the physical access to a device due to its low cost and easy availability in the market. These two issues suggest that the femtocells may become an attractive target for the attackers. Despite the importance of security, various groups have demonstrated how to get root access to these devices.

The paper is organized as follows. Section 2.2 describes femtocell architecture and its components. In Section 3 we present various attacks and their impact on mobile communication. In Section 5 we briefly conclude.

2 Femtocell Architecture

In this section, we describe UMTS architecture in general, femtocell architecture and their different components. The idea is to give an idea about how these two architectural components are interconnected with each other and their important functions respectively.

2.1 UMTS Infrastructure

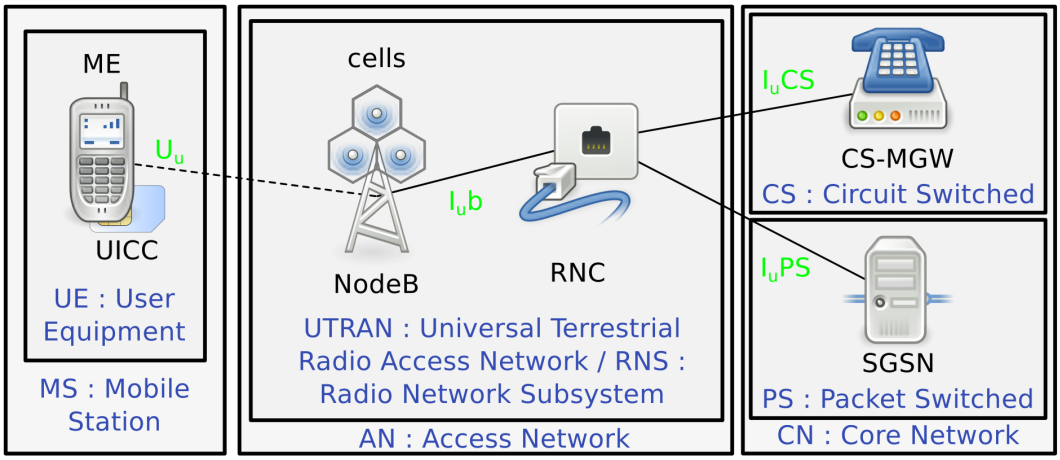

Figure 1. UMTS Infrastructure

The Third Generation (3G) Universal Mobile Telecommunications System (UMTS) infrastructure, as illustrated in Figure 2.1 is similar to GSM. But the some names have been changed. The network is divided in three parts:

- The Mobile Station (MS) includes the end user device, mainly the mobile phone, called Mobile Equipment (ME). But it can be any other User Equipment (UE) which uses a Universal Subscriber Identity Module (USIM) for telecommunication.
- The Access Network (AN) enables the connection between the AN and Core Network (CN). It includes the antennas (e.g. transceivers) called Node B (NB) and the Radio Network Controller (RNC) controlling the NB. The combination of NBs and RNC forms the Radio Network System (RNS).
- The CN it responsible for routing the telecommunication traffic: voice, SMS, data. It is further divided in two parts, the Circuit Switched (CS) and the Packet Switched (PS). The CS is equivalent to the landline phone network. It routes the voice and SMS traffic. The PS network routes the data traffic (Internet). Numerous elements are located in the CN, each with a dedicated task. But for authentication and accounting the

access the common Home Location Register (HLR), responsible for the user identity. The Visitor Location Registers (VLRs) holds the user currently registered to a specific location.

2.2 Femtocell Infrastructure

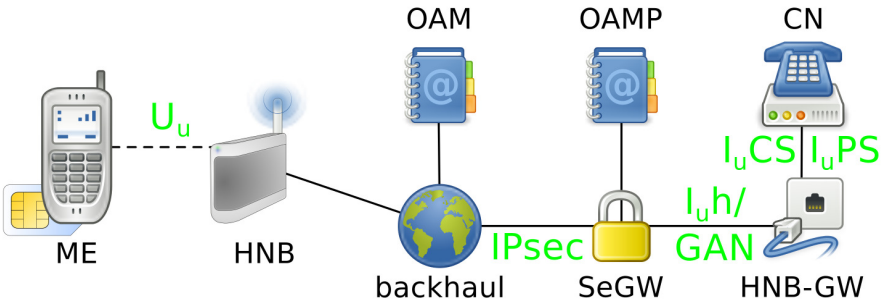

Figure 2. Femtocell Infrastructure (HNS)

The main elements of femtocell infrastructure [3] and their roles are described as follows:

HNB Femtocells are deployed in closed environments, e.g. home environments, the base station is not called NB but Home Node B (HNB) instead. The HNB is a small access point that connects MS (Mobile Stations) to the operator's core network through radio interface. It provides almost all functionalities of the base station such as GPP signaling, Radio Resource Management, IP (Inter- net Protocol) transport functions, QoS (Quality of Service) management functions, TR-069 Management functions, NAT (Network Address Translator), security functions, and auto configuration functions.

SeGW The IPsec encrypted HNB traffic enters into the core network via the SeGW (Security Gateway). Accordingly, it mutually authenticates the HNB first and establish further security tunnels. Then it forwards all the singling and call related data to the core network. The interface between the SeGW and core network is considered to be secure.

HNB-GW The Home Node B Subsystem (HNS) makes up the RNS equivalent in a femtocell AN. As femtocells are deployed in closed environments, e.g. home environments, the base station is not called NB but Home Node B (HNB) instead. While in a typical UMTS network, a set of NBs is controlled by an RNC, the so-called HNB GateWay (HNG-GW) is controlling a set of HNBs. The HNG-GW is the main communication endpoint for mobile signaling originating from the HNB (including mobile phone traffic). In our case the HNB is communicating with the HNG-GW by using the Generic Access Network (GAN) protocol [2]. It maps the 3GPP Layer 3 (L3) messages used by MS and the CN to a TCP/IP connection. Additionally GAN is also used for signaling, the system used to control the telecommunication circuit and to manage the network. It provides following additional functionalities: 3GPP RANAP (Radio Access Network Application Part), Network timing delivery and synchronization, IP security functions, HNB traffic aggregation, and routing and auto configuration functions.

HMS The HNS also includes the HNB Management System (HMS) to manage the femtocell. The Operation, Administration and Maintenance (OAM) forms the services needed to perform an initial configuration and possible firmware recovery procedure. It also consists of services monitoring the devices for various alarm conditions and location verification. This is needed so that the HNB can connect to the SeGW and contact the Operation, Administration, Maintenance and Provisioning (OAMP). The OAMP is performing the required provisioning and

configuration of the HNB. To do so femtocells make use of the standardized TR-069 [9] protocol. This includes services needed by the SeGW for authentication, accounting, and authorization.

3 Femtocell Threats

In this section, we describe various attacks that in a real operator network. The discussion of how to root a femtocell is out of scope for this paper. However, previous research [7, 4, 6, 8] exhibits interesting directions in this regard.

During our security assessment, we performed a wide range of attacking vectors. The 3rd Generation Partnership Project (3GPP) lists a number of threats [1] involved in the femtocell deployment process and ecosystem. Different threats, their impact on the operator and on the users, and related solution are described in this document. These attacks and their impacts are presented in table 3.

The attacks can be categorized as following:

- Root and flashing the femtocell: First of all, we required a rogue femtocell. We will briefly show how to take control of such a device [8].
- Remote root access: The methods to control our own device can not be applied to remote devices of other customers. However, we found another way to get control over any femtocell connected to the operator network (remote root exploit).
- Information Collecting: Because the other femtocells are accessible on the network, either by using the web interface or the remote root, it is possible to collect the device settings. This includes the telephone number of the subscribers and the location of the device.
- Security Gateway access: The requirement of a controlled network environment to use the rogue femtocell for testing purposes is a serious limitation. Previously we used the femtocell to access the operator network. Trial and error lead to a proper IPsec configuration (client and server). We can now connect to the operator using an IPsec client running on an external machine rather than using the femtocell. Therefore, the femtocell is not required anymore for studying the operator network. Additionally the normal computer broadens the possibilities, as it has more powerful hardware and software.
- Subscriber DoS: It has been demonstrated that it is possible to perform DoS attacks against subscribers in GSM. We will show that it is possible to apply this to a femtocell network in order to disconnect all femtocell subscribers.
- Owner DoS: Using the remote access, we can also brick any femtocell by changing crucial configuration settings. The operator would then need to handle the influx of broken devices and replace them.
- Operator DoS: Using the Security Gateway access, we can use common penetration testing techniques to tools to attack the operator. Furthermore, using the remote access to other devices, it becomes possible to perform certain attacks against operator equipment.
- IMSI-Catching: This small device can be turned into a inexpensive UMTS IMSI-Catcher by reconfiguring it. Even the mutual authentication can be performed, by design.
- Interception: By having root access, it is possible to intercept all the communication to and from the phone. Additionally, a configuration tweak allows us to reroute all communication from the other femtocell to ours.
- Modification: Using a rogue device it is not only possible to eavesdrop on user data but also to modify data. As a demo, we will show how to change the text in an SMS message, or it's destination number.

HNB threats (TR 33.820)				
group	**#**	**threat**	**impact**	**status**
Compromise of H(e)NB Credentials	1	Compromise of H(e)NB authentication token by a brute force attack via a weak authentication algorithm	harmful	untested
	2	Compromise of H(e)NB authentication token by local physical intrusion	harmful	performed
	4	User cloning the H(e)NB authentication Token. User cloning the H(e)NB authentication Token	very harmful	performed
Physical attacks on a H(e)NB	3	Inserting valid authentication token into a manipulated H(e)NB	harmful	performed
	6	Booting H(e)NB with fraudulent software (“re-flashing”)	up to disastrous	performed
	8	Physical tampering with H(e)NB	harmful	performed
	26	Environmental/side channel attacks against H(e)NB	harmful	performed
Configuration attacks on a H(e)NB	7	Fraudulent software update / configuration changes	extremely harmful	performed
	19	Mis-configuration of H(e)NBMis-configuration of H(e)NB	irritating to harmful	performed
	20	Mis-configuration of access control list (ACL) or compromise of the access control list	irritating to harmful	performed
Protocol attacks on a H(e)NB	5	Man-in-the-middle attacks on H(e)NB first network access	very harmful	performed
	15	Denial of service attacks against H(e)NB	annoying	performed
	17	Compromise of an H(e)NB by exploiting weaknesses of active network services	extremely harmful	performed
	25	Manipulation of external time source	harmful	untested
	27	Attack on OAM and its traffic	very harmful	possible
	28	Threat of H(e)NB network access	harmful	performed
Attacks on the core network, including H(e)NB location-based attacks	11	Changing of the H(e)NB location without reporting	harmful	performed
	12	Software simulation of H(e)NB	very harmful	performed
	13	Traffic tunnelling between H(e)NBs	very harmful	untested
	14	Misconfiguration of the firewall in the modem/router	annoying	nonexistent
	16	Denial of service attacks against core network	annoying	possible
	24	H(e)NB announcing incorrect location to the network	harmful	performed
User Data and identity privacy attacks	9	Eavesdropping of the other user’s UTRAN or E-UTRAN user data	very harmful	performed
	10	Masquerade as other users	very harmful	performed
	18	User’s network ID revealed to Home (e)NodeB owner	breaking users privacy	performed
	22	Masquerade as a valid H(e)NB	very harmful	performed
	23	Provide radio access service over a CSG	very harmful	performed
Attacks on Radio resources and management	21	Radio resource management tampering	harmful	performed

Figure 3. femtocell threats listed by 3GPP TR 33.820

- Injection: A similar approach as for modifying content also enables us to inject data into the network. This allows us to produce data traffic on behalf of a victim. E.g. this has the potential to be abused for impersonation, free phone calls, fraud and the-like.
- Signaling Attacks: Finally, thanks to these device we now have access to the telecommunication operator network. The network is used differently, but signaling is still it's fundamental idea and signaling traffic can be generated by the device.

4. Recommendations

Based on our research analysis and results, we propose a few recommendations for mobile operators, femtocell manufacturers, and for the end-users.

Mobile Operator The mobile operator considers femtocell technology as a cost-effective solution to satisfy higher mobile data demands from the customers. Accordingly they seek low cost but efficient femtocell devices from a vendor. Considering security risks involved in these low cost embedded devices, operators have to enforce strict security policies in their infrastructure. We believe current security mechanism implemented by the operator fail to detect our attacks coming from a rogue femtocell. Hence, there should be some additional protection techniques to filter out such attacks. In particular, there should be additional protection mechanisms at the interface point where femtocell architecture integrates into the core network. Our attacks assist in identifying these security risks and provide few pointers in creating such security policies.

Femtocell Vendor Hardware security is a key challenge for femtocell vendors in balancing the low cost per device. Our results reveal that the femtocell hardware lacks basic security techniques in various essential requirements such as handling of firmware binaries (update process), secret data storage and management, and boot sequence. They should make use of USIM/TPM (Trusted Platform Module) based techniques to ensure the integrity of the device and involved communication. Note that not all femtocell devices deployed commercially are protected using an Operating System in combination with a TPM solution. They do not follow 3GPP standard and guidelines strictly. Though femtocell vendors are improving hardware security of the device recently, in addition they should force the mobile operator to use stronger protection techniques despite of their low cost per device requirement.

End User For end users, it is difficult to detect that they are being attacked through a rogue femtocell. The only recommendation is to check their mobile bills regularly to ensure no frauds affecting their mobile subscription. In other attacks such as voice/SMS interception, there is nothing an end-user can do besides blaming the operator.

5 Conclusion

We practically analyzed and demonstrate several attack vectors from a rogue femtocell against various parties in a femtocell ecosystem. Our result suggests that due to the trade off between security and inexpensiveness of femtocells, mobile operators are risking security of their infrastructure and end users as well. Therefore, new additional security mechanisms are needed to improve the overall femtocell security architecture. We believe that current femtocell technology is in an immature state. Especially attacks targeting end-users are almost impossible to prevent because all communication happens outside the scope of the operator.

References

[1] 3GPP. Security of H(e)NB. Technical Report TR 33.820 v8.3.0, 3G Partnership Project, Dec 2009.

[2] 3GPP. 3GPP TS 43.318 - Generic Access Network (GAN). http://www.3gpp.org/ftp/Specs/html-info/43318.htm, April 2011.

[3] 3GPP. Security of Home Node B (HNB) / Home evolved Node B (HeNB). Technical Specification TS 33.302 v11.2.0, 3G Partnership Project, Jun 2011.

[4] R. Allen. Verizon / Samsung 3G SCS-2U01. http://rsaxvc.net/cgi-bin/mt/mt-search.cgi?blog_id=3&tag=Samsung&limit=20, February 2011.

[5] Cisco. Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2010-2015. http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html, Jan 2011.

[6] T. Group. Vodafone Access Gateway. http://wiki.thc.org/vodafone, June 2011.

[7] Lokkju. Samsung-Femtocell. http://code.google.com/p/samsung-femtocell/, March 2011.

[8] Ravishankar Borgaonkar, Kevin Redon and Nico Golde. Femtocell Security Project. http://www.isti.tu-berlin.de/security_in_telecommunications/menue/research/projects/femtocell_security/.

[9] The Broadband Forum TR-069. CPE WAN Management Protocol . http://www.broadband-forum.org/technical/download/TR-069_Amendment-3.pdf, November 2010.