Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunication

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

Abstract

Mobile phones and carriers trust the traditional base stations which serve as the interface between the mobile devices and the fixed-line communication network. Femtocells, miniature cellular base stations installed in homes and businesses, are equally trusted yet are placed in possibly untrustworthy hands. By making several modifications to a commercially available femtocell, we evaluate the impact of attacks originating from a compromised device. We show that such a rogue device can violate all the important aspects of security for mobile subscribers, including tracking phones, intercepting communication and even modifying and impersonating traffic. The specification also enables femtocells to directly communicate with other femtocells over a VPN and the carrier we examined had no filtering on such communication, enabling a single rogue femtocell to directly communicate with (and thus potentially attack) all other femtocells within the carrier's network.

1 Introduction

During the last years, there has been significant growth in Fixed Mobile Convergence (FMC), mostly due to the popularity of Wi-Fi networks, inexpensive mobile data rates, and the increasing usage of smartphones. At the end of 2010, one fifth of more than five billion mobile subscriptions globally had access to mobile broadband [15]. Subsequently, mobile generated data traffic is rapidly increasing and has been predicted [18] to reach a compound annual growth rate (CAGR) of 92% between 2010 and 2015. Therefore, Mobile Network Operators (MNOs) are exploring different solutions to offload the increasing data traffic and bandwidth requirements towards networks such as Wi-Fi and femtocells, instead of expanding their existing expensive Third Generation (3G) networks. One estimate suggests [19] that 31% of the global smartphone traffic in 2010 was offloaded to fixed-line networks through dual-stack handsets (radio communication over Wi-Fi) or femtocells.

A femtocell is a small cellular base station that is typically deployed in home or business environments. It is connected to the operator's network via a broadband connection such as DSL. By deploying these inexpensive devices, carriers are offloading mobile data and voice traffic from their infrastructure to a fixed broadband line provided by the customer. Furthermore, the customer takes care of the device installation and maintenance by simply attaching it to a local network. This enables operators to both reduce their costs and solve targeted reception problems in indoor environments. Unlike techniques where the phone directly offloads the connection through a Wi-Fi network, femtocells do not require handsets to operate in a dual-stack mode, as the femtocell is acting as a normal base station, offering improved radio coverage, high mobile data rates, and high voice quality to subscribers.

As of the first quarter of 2011, 19 operators have adopted femtocell technology in 13 countries around the world and many others are running field trials [25]. This number has increased to 31 operators in 20 countries during the second quarter of 2011 [26], including high profile operators such as Vodafone, Movistar, AT&T, SFR, China Unicom, and NTT DoCoMo. Informa estimated that carriers have deployed 2.3 million femtocell access points at the end of 2010 and forecasts it to reach 49 million in 2014 [26]. Thus there are now large fractions of operator infrastructure which communicate over the Internet and which are deployed at locations where users and adversaries have physical access to the equipment. Due to this situation, these devices may become an appealing target to perform attacks on mobile communication, or use them as a stepping-stone for attacks targeting the operator's network. Therefore, security is one of the top priorities for operators during the deployment process of these devices.

We believe that it is a fundamental flaw of the 3G specifications to treat base stations as trusted devices. This becomes even more important in the context of femto-

cells. Femtocells involve different aspects of security including integrity of the device, access control mechanisms, and protection of the software update process. Among the top threats [4] identified by the industry are: booting the device with modified firmware; software and configuration changes; eavesdropping on user data; masquerading as other users; traffic tunneling between femtocells; Denial of Service attacks against femtocells and core network parts. While these threats are defined abstractly, their practical impact on mobile communication is rather unclear. We aim to measure the scale of such impact in a real operator network, conducting a practical security analysis of a femtocell device available to the public.

Despite the importance of femtocell security, it is well known [29, 17, 16, 46] that it is possible to get root level access to these devices. However, the negative consequences of rogue devices on mobile communication have not been thoroughly analyzed yet. In this paper, we show that rogue devices pose a serious threat to mobile communication by evaluating the security impact of femtocell-originated attacks. We begin with an experimental analysis of security threats affecting end-users; both end-users deliberately using such a device as well as those who are not intentionally booked into the cell (e.g. by means of a 3G IMSI-Catcher). Furthermore, we evaluate the risk of femtocell-based attacks against the mobile communication infrastructure. This includes operator components and femtocells owned by other subscribers. We investigate how these components can be accessed and what type of network-based attacks are possible against them. Moreover, we argue how femtocell features in combination with common software vulnerabilities can provide a suitable environment to perform signaling attacks or allow to turn the femtocell network into a global interception and attacking network.

While these devices run flavors of the Linux operating system, large parts of the functionality are provided by undocumented, proprietary binaries. Therefore, we conducted a vulnerability analysis of the femtocell and network architecture using a mixture of reverse engineering and experimental testing. In our work, we concentrate on a device deployed by the operator Société Française du Radiotéléphone (SFR): the SFR Home 3G [41] femtocell. SFR is the second largest mobile phone operator in France and has been among the early adopters of this technology [42]. However, due to the design of the femtocell architecture, most of the attacks presented in this work are not limited to this specific operator or device. During our analysis, we have found several security critical attack vectors that can be leveraged to the previously mentioned threats defined by the industry. We will outline the risks of the femtocell technology that are caused due to a combination of operator specific configuration mistakes and problems inherent in the design of the femtocell architecture.

The key contributions of this paper are:

- **End-User Risk Assessment**: We demonstrate that attacks based on a rogue femtocell can easily compromise all important security aspects for mobile phone users, namely integrity, authenticity, confidentiality, and availability. Such attacks include intercepting, modifying or impersonating user-generated mobile communication traffic. These attacks are inherent in the basic architecture of current femtocells and are carrier independent.
- **Femtocell/Infrastructure Weakness Analysis**: We characterize network based attacks originating from a rogue femtocell device. Moreover, we highlight the design concerns of the femtocell security architecture in the procedure of attack exploration and experimentation. We exhibit how these issues conflict with some of the basic 3G security principles and requirements.
- **Implementation and Evaluation**: We developed a set of attack-software to both implement attacks and enable interactions with critical components of the operator infrastructure. Furthermore, we evaluated the presented attacks based on a commercially deployed femtocell in a real operator network, highlighting the problems inherent with this new technology.

Both the operator as well as the vendor have been notified of our research results. The implementation specific flaws have been addressed by the femtocell vendor in firmware version V2.0.24.1.

The remainder of the paper is organized as follows. In Section 2 we provide a brief overview of the femtocell infrastructure and involved network components as well as describing how they are cooperating with each other. In Section 3 we demonstrate attacks based on a rogue femtocell against end-users and their impact on mobile communication. Section 4 describes experimental attacks targeting the femtocell infrastructure. In Section 5, we present vulnerabilities in the femtocell security architecture and discuss the overall effect on the 3G security principles. Section 6 discusses related work and how our research extends previous work in this area. Finally, we briefly conclude our research in Section 7.

2 Background and Overview of the 3G System Architecture

This section briefly describes the 3G infrastructure and exhibits how the architecture integrates femtocells. Additionally we discuss how femtocells can be compromised by an attacker and turned into rogue devices. The technical term for a femtocell in a 3G network is Home Node B

(HNB) [14]. We will attempt to use common terms rather than industry specific terms throughout this work, but sometimes using industry acronyms is unavoidable, thus a complete list of abbreviations can be found in the appendices.

2.1 3G Architecture

In the following paragraph, we give an overview of the 3G architecture as defined by 3rd Generation Partnership Project (3GPP) [9] and as illustrated in a simplified version in Figure 1.

A classical 3G network is divided into three main parts. Firstly, the subscriber part consists of Mobile Stations (MSs), most notably mobile phones, smartphones, and 3G modems. Secondly, the Access Network (AN) is responsible for connecting the wireless devices to the operator back-end network, which is known as the Core Network (CN).

The AN usually consists of multiple Radio Network Subsystems (RNSs). An RNS accommodates base stations called Node Bs (NBs) and a Radio Network Controller (RNC) managing them. The RNC acts as the gateway towards the CN and forwards all traffic originating from MSs that passes through the NBs. Both the original GSM and current 3G architectures trust the base stations: although the phones use link-encryption to communicate with the base station and the base stations could use link-encryption to communicate with the operator's back-end network, there is *no* end-to-end confidentiality or integrity between the user's phone and the carrier's network.

The third part is the CN that further contains two subsystems. The Mobile Switching Center (MSC) residing in the Circuit Switched (CS) subsystem is mainly responsible for call routing related tasks and maintains the circuit-switched model of conventional telephony (the Public Switched Telephone Network (PSTN)). Conversely, the Packet Switched (PS) network subsystem primarily comprises a Serving GPRS Support Node (SGSN) to route data traffic and resembles a conventional packet-switched network.

The CS and PS subsystems both share a number of common infrastructural components such as the Visitor Location Register (VLR) and the Home Subscriber Server (HSS) which are critical components of access control and billing. A VLR acts as a database for temporary subscriber information belonging to subscribers within a dedicated geographical area served by this register. The HSS incorporates the Home Location Register (HLR) and the Authentication Center (AuC) required to manage and authenticate subscriber information. An HLR acts as a central database storing all data associated with each registered subscriber of the operator. The AuC assists other components within the network by providing authentication and cipher key material needed to establish communications.

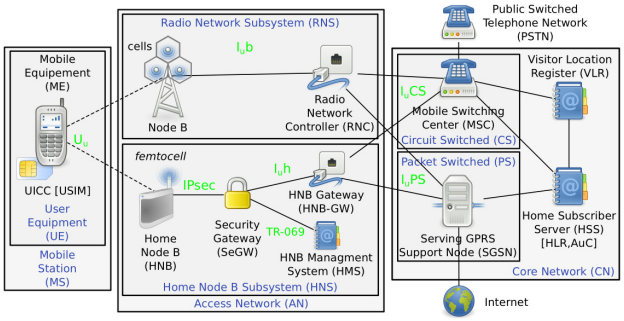

Figure 1. Femtocells and their place in the 3G network architecture.

2.2 Femtocell Infrastructure

In order to integrate femtocells (in technical parlance, Home Node Bs (HNBs)) into existing operator networks, a new subsystem has been added, namely the Home Node B Subsystem (HNS). This subsystem shares most major functionality present in the RNS of a conventional 3G network and connects to the same carrier back-end network. The femtocells act as a small cellular base station. Each femtocell communicates to the carrier network via the HNB GateWay (HNB-GW), which has similar functionality to the RNC component of a conventional 3G network. In particular, the HNB handles radio management functions whereas the HNB-GW acts as an interface to provide core network connectivity. As we explain in Section 3.1, the deployed HNB actually is a combination between the NB and the RNC.

Unlike the traditional telecommunication equipment, carriers deploy femtocells in environments that are not under their control. Thus the standard introduced new network services in order to enforce security requirements and to allow operators to remotely control these devices. The Security GateWay (SeGW) component enables the femtocell to communicate with the carrier network in a secure way over an untrusted, shared broadband connection using a separate link-encryption layer to prevent eavesdropping or modification of traffic.

In order to allow the operator to remotely control the femtocell, the standard introduced the Operation, Administration, Maintenance, and Provisioning (OAMP) [8] server as a part of the HNB Management System (HMS) [3]. It acts as the central management entity within the network. While the main components and interfaces of the HNS are defined by the 3GPP, the implementation details are left to vendors and may differ among the various operator networks.

Just like a normal base station, the femtocell is effectively trusted: although there is link-layer encryption between the mobile devices and the femtocell, and between

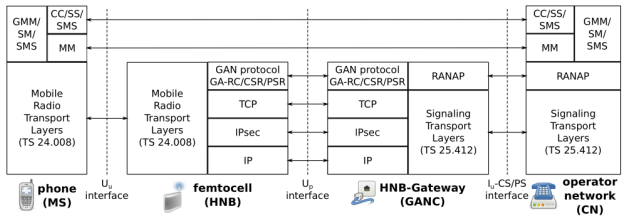

Figure 2. The GAN protocol stack.

the femtocell and the carrier's network, there is no end-to-end integrity or confidentiality between the phone and the carrier.

2.3 Core Network Communication: Generic Access Network Protocol

Integration of femtocells into the existing telecommunication network over the public Internet is a challenge for operators and vendors. The 3GPP defines the following three approaches to connect these devices to the core network over the so-called I_uh interface: I_ub over IP, SIP/IMS, and Radio Access Network (RAN) gateway based [30]. While these protocols differ in details, the architecture and supported features are all similar. We concentrate on the third approach based on a RAN gateway as our device uses this protocol. This technique utilizes the 3GPP Generic Access Network (GAN) protocol as the interface between the femtocell and the gateway [6].

The GAN protocol, formerly known as Unlicensed Mobile Access (UMA), was originally designed to allow mobile communication over Wi-Fi access points, enabling the phone to connect to the operator network over an IP network. This protocol was first standardized by MNOs in 2004 [31] and lead to the GAN specification [5, 6] in 2005. The protocol transparently encapsulates all traffic generated by the phone and forwards it to the HNB-GW. This gateway is referred to as GAN Controller (GANC). Similar to the RNC in traditional 3G networks, it is linked to the operator's CN using the I_uCS/I_uPS interface. For compatibility with the HNB architecture, the GAN protocol has been slightly extended (see Section 3.1).

The HNB acts as a gateway between the MS and the GANC as depicted in Figure 2. As in a classical 3G network, mobile phones connect to cells (in this case the HNB) via the U_u interface. Therefore, the presence of GAN is transparent to the subscriber's phone. Our femtocell device supports this protocol to enable mobile telecommunication via the customer's broadband connection. The GAN protocol implementation running on the HNB maps all 3GPP Layer 3 (L3) radio signaling to TCP/IP based GAN messages and passes them to the GANC. This enables the HNB to perform signaling tasks by sending encapsulated L3 messages to the GANC.

Details of these GAN messages are as follows. To map radio signaling from a specific subscriber to GAN messages, the femtocell maintains a TCP connection with the GANC for each individual subscriber. The connection management is based on Generic Access Resource Control (**`GA-RC`**) messages. The CS traffic is encapsulated in Generic Access Circuit Switched Resource (**`GA-CSR`**) messages, while PS traffic is covered by Generic Access Paket Switched Resource (**`GA-PSR`**) messages. We discuss the specific roles of these messages in Section 3.2. Additionally, GAN supports MAP based signaling to control the telecommunication circuit and to manage the network [11]. This provides the necessary protocol functions for all Mobile Terminated (MT) as well as Mobile Originated (MO) services and thus supports full 3G functionality.

2.4 Compromising Femtocells

In order to operate the femtocell as a rogue base station and perform the attacks presented in Section 3 and 4, an attacker must acquire full control over the femtocell. Since femtocells are connected to the carrier's network, they must be secured to protect this critical infrastructure.

This securing should include such functionality as mutual authentication between the device and the serving network, secure storage, secure network access, and secure communication [12]. However, due to the mass deployment of femtocells, carriers rely on a low cost per unit. Hence, femtocell manufacturers face a trade-off between secure hardware, software security, and low production costs. Consequently, the implementation often includes flaws that can be used to gain control over the device.

Common methods for initial debugging of embedded devices are test-pin probing, packet sniffing, network scanning, and reverse engineering. Attackers use test-pin probing to detect UART or JTAG ports, or other techniques which researchers have used to gain root access on various commercially deployed devices [24, 29, 17, 16, 46].

Alternatively, as these techniques did not reveal obvious flaws in the device we studied, we examined the recovery procedure in order to compromise our device. If, for any reason, the femtocell is unable to connect to the carrier's network, the recovery mechanism enables the device to repair itself. The recovery procedure fetches and installs the latest working firmware images and configuration settings from the Operation, Administration, and Maintenance (OAM) server. We discovered two critical flaws in the implementation of the recovery mechanism on our device. Firstly, there is no mutual authentication between the OAM server and the femtocell. While the OAM server authenticates the femtocell, there is no authentication of the OAM server. Thus, we were able to setup our own OAM service and modify its address by spoofing DNS replies.

Figure 3. Our setup: A computer to monitor traffic and perform attacks, a victim phone and an SFR femtocell.

Secondly, the firmware images provided by the OAM server were signed and encrypted. However, the implementation of this security mechanism included a trivial vulnerability: the OAM server provides the keys used to decrypt and verify the files in the configuration that is fetched by the femtocell. As a result, we were able to use existing images provided by the operator, add additional software and adjust configurations according to our needs, and deploy these modified images via the firmware recovery procedure. Using this method, we gained full control over the HNB [17] and were able to utilize it to perform the attacks presented in the next sections. Our experimental setup, as depicted in Figure 3, essentially consists of a victim phone, a rogue femtocell, and a computer utilized to monitor the network traffic, flash the device, and perform the presented attacks. [1]

3 End-User Threats

A great advantage for end-users of a femtocell is the increased local 3G coverage, and thus higher mobile data bandwidth in their home environment. However, as we demonstrate in the following sections, end-users using such a device are subject to several attacks when connected to a rogue femtocell. End-users include subscribers who are knowingly using this cell (e.g by using a femtocell installed in their home environment), as well as those who may not be aware of this because the attacker has installed his rogue femtocell in an unexpected location.

In both cases, the femtocell architecture has to ensure the confidentiality, integrity, and authenticity of mobile communication as well as the availability of mobile services to the registered subscribers. We show how all these protections can be bypassed by a rogue femtocell. It is important to note that although the experimented attacks targeted a specific vendor and a specific protocol (GAN), these attacks rely on the trusted nature of femtocells in the cellular network architecture and thus are adaptable to different vendors, carriers, and devices.

[1] Although we and others have exploited specific flaws in individual femtocells, due to the absence of substantial and expensive tamper resistance, we must assume that an attacker can always gain root access on any femtocell in their extended physical possession.

3.1 IMSI-Catching and Call Interception (Confidentiality)

The confidentiality of the subscriber data is a very important security aspect in mobile communication networks. It is well known [38, 48] that it is easy to build an *IMSI-Catcher* device for GSM networks by using radio equipment and Open Source software. An IMSI-Catcher is a combination of hardware and software that pretends to be a legit operator's base station and is usually used to intercept a victim's communication and determine their IMSI (International Mobile Subscriber Identity), which enables the identification and tracking of individual phones. At the same time, it acts as a proxy between the victim's phone and the carrier, which prevents this monitoring from being detected. This attack leverages the fact that the network is not authenticated by the phone in GSM.

The 3G network was not supposed to be vulnerable to IMSI-Catchers, as the phone authenticates the carrier network. Yet a rogue femtocell can be used to create a 3G IMSI-Catcher as follows.

Mutual Authentication/Over-the-Air Encryption In contrast to GSM, the 3GPP defines [13] mutual authentication between the mobile phone and the carrier's network for 3G using a challenge response procedure assisted by the subscriber's Universal Subscriber Identity Module (USIM). If the carrier is not properly authenticating itself, the phone would not attempt to register with the network. Yet since a femtocell is an authorized and authenticated base station with an operator back-end connection, we can use a rogue femtocell as a cheap 3G IMSI-Catcher, circumventing the problem of mutual authentication without relying on protocol downgrading attacks. Thus, posing a serious threat to the data confidentiality of subscribers being booked into an HNB.

In order to provide mutual authentication, encryption and integrity protection, the femtocell acts as a combination of RNC and NB known from classic 3G networks. To understand call interception, we briefly describe the encryption and authentication procedure. The full details of this procedure are defined in [1, 13].

To guarantee the aforementioned security protections to subscribers, the femtocell receives an Authentication Token

(AUTN), an Expected Response (XRES), a random challenge RAND, an Integrity Key (IK), and a Cipher Key (CK) from the carrier's AuC server. The RAND and AUTN values are forwarded to the phone. This AUTN is required by the phone to verify the authenticity of the network. By using a shared secret key K in combination with the random challenge RAND, the subscriber's USIM computes an Authentication Response (RES), IK, and CK. The resulting RES is required to authenticate the phone to the carrier's network and must be compared with XRES by the femtocell.

The IK and CK keys generated by the CN and transferred to the femtocell are not forwarded to the phone, but kept locally. This IK key is required by both parties to provide integrity protection for authentication and cipher algorithm selection between the femtocell and the phone. In contrast, CK is used as a key to encrypt Over-the-Air (OTA) communication between the phone and the femtocell. The femtocell decrypts, encapsulates, and relays the *decrypted* data of mobile subscribers to the operator network. In the case of our device, the signaling traffic is transferred to the HNB-GW via the GAN protocol and the voice call data is encapsulated in an unencrypted RTP stream.

Thus the femtocell has established encrypted connections in two directions based on entirely unrelated cryptographic material. While the connection between the femtocell and the SeGW is encrypted using IPsec, the communication with the phone is encrypted using standard algorithms such as A5/3, with all communication transferred from from one encryption scheme into the other on the femtocell.

As OTA encryption support is mandatory and 3G protocols do not provide the necessary functionality for end-to-end encryption, the femtocell has to receive IK and CK from the core network. This in turn means that an attacker in control of the femtocell can sniff and manipulate traffic on the device. In the case of our device, the GAN protocol has been slightly extended for the use with femtocells to provide a **`Security Mode Command`** message that allows the operator network to transfer key material to the device for OTA encryption support [49].

Access Modes/HNB Configuration A femtocell usually provides three types of access modes [22]: *open* access, *hybrid* (semi-open), and *closed* access mode. Most femtocells, including our device, default to closed access mode for residential deployments. The device receives a Closed Subscriber Group (CSG) list during the initial provisioning phase of the femtocell. The femtocell applies this list to enforce an access control policy that only allows registered subscribers to connect to it. However, we were able to change this access mode to open access via a hidden operator web interface that contains basic security flaws. While there is a login page, the configuration pages can be accessed directly and thus bypass the authentication mechanism. The exact location of the specific pages can be determined by analyzing the firmware images. Since the access policy is a software feature, not a hardware restriction, and is enforced on the femtocell, a compromised femtocell can always bypass this control and change modes.

Changing this access mode to hybrid enables the device to allow any subscribers of a specific operator to connect to it, while open access allows any subscriber of *any* operator to access the network through the femtocell. The femtocell firmware usually supports the functionality to enable open-access mode for its use in business environments or public areas. Thus carriers supporting open access mode also very likely support roaming between different operators via the femtocells (in particular via the GANC). Moreover, it is possible to change the Mobile Country Code (MCC) and the Mobile Network Code (MNC) of the femtocell to trick a victim subscriber into believing it is connected to the home operator. As roaming is allowed and the subscriber's home operator will provide valid AUTN tokens, mutual authentication is still performed successfully. Additional techniques on how to lure phones into using the IMSI-Catcher have been presented by Dennis Wehrle [48].

Circumventing IPsec The femtocells connect to the back-end network via the SeGW, protected using IPsec or similar VPN technology. This means that even though it is possible to use the device as an IMSI-Catcher, it is not possible to directly eavesdrop on the subscriber traffic. However, there are multiple ways of sniffing this data as an attacker with root access to the femtocell. In our case, a user-space program is in charge of establishing the IPsec connection while a proprietary kernel module encapsulates the network traffic by means of Encapsulating Security Payload (ESP).

To allow the kernel to handle encryption of this tunnel, the user-space program has to pass the cipher material (HMAC, Cipher keys, Security Parameter Index) to the kernel (PF_KEYv2 interface). On our test device, this is performed using the sendto(2) syscall. By hijacking the libc provided wrapper function of this syscall and parsing the message, we were able to grab the key material for exfiltration.

Monitoring Voice Calls With a successfully exfiltrated session key, we now can construct a sniffer to capture data in the IPSec stream. We built a small helper program which uses the key material to decrypt the captured traffic. In combination with rtpbreak [21], it reconstructs the unencrypted RTP stream from the packets. The same helper program is also capable of extracting short messages and other user-generated critical data. The voice data is encoded in the RTP stream using the 3GPP AMR [10] speech codec in

stream format. We also constructed a small utility based on OpenCORE [44] which can transcode the captured data streams into playable audio waveforms.

This allows an attacker to impersonate any operator by utilizing a rogue femtocell as an inexpensive 3G IMSI-Catcher and wiretap device. Consequently, adversaries can intercept mobile communication by installing the device in the radio range of a victim.

This threat is a design problem in the current femtocell architecture since the communication is in-the-clear within the femtocell and a compromised femtocell can always exfiltrate key material. It is not possible with the current femtocell architecture to support end-to-end encryption of critical mobile subscriber data. Moreover, mutual authentication is always properly performed, as the device is forwarding authentication tokens received from the corresponding CN of the victim's operator.

3.2 Modifying Traffic (Integrity)

Data integrity, not just confidentiality, is also critical. Yet we show that a rogue femtocell can also be used to compromise data integrity. We demonstrate such a type of attack by modifying outgoing Short Message Service (SMS) traffic for a phone which is communicating through our rogue femtocell. However, the same approach can be applied to any traffic generated by the phone as well as traffic directed to the phone.

As depicted in Figure 2, all traffic generated by the phone is passed to the GANC using the GAN protocol. Nevertheless, the phone is not aware of this protocol being used for the communication. The GAN protocol maps the Connection Management (CM) and Mobility Management (MM) layer messages of the 3G standard to a TCP/IP based network protocol. As soon as the IPsec tunnel is established and the device receives provision data, the femtocell attempts to build a permanent connection to the GANC. This procedure is based on GAN Generic Access Resource Control (**GA-RC**) messages. Additionally, the GAN protocol provides a Generic Access Circuit Switched Resource (**GA-CSR**) layer which is the equivalent to the GSM Radio Resource (**GA-RR**) layer. This layer is in charge of setting up a bearer between the mobile phone and the GANC. To successfully modify the mobile generated traffic, an attacker has to perform a Man-in-the-Middle (MitM) attack on the GAN traffic. Therefore, our attacks on such network-based signaling consist of the following two parts.

GAN Proxy The first part comprises a GAN protocol proxy that forwards all signaling traffic between the femtocell and the GANC. In addition to this transparent proxying, it enables us to differentiate between GAN messages exchanged via this connection. Consequently, the proxy is able to detect incoming and outgoing GAN messages and in our example, track those that carry SMS data. Since the femtocell is under our control, we can reconfigure the device to communicate with our GAN proxy instead of the real GANC. This provides a simple method to force the HNB to communicate through our MitM proxy.

Attack Client The second part consists of an attack client program that communicates with the GAN proxy over a slightly extended version of the GAN protocol. This client is able to inject or modify messages exchanged between the femtocell and GANC (thus not requiring OTA key material). To modify outgoing or incoming text messages, our client registers itself with the proxy to indicate that it is waiting for a text message. In the event of an outgoing message by a victim's phone, the proxy forwards its SMS to the registered attack client. Since all authentication is already complete, there is no additional authentication or encryption required. Our attack program is able to decode the forwarded **SMS SUBMIT** message and allows to change either the message content or the destination number. Finally, it re-injects the modified message to the proxy which subsequently forwards it to the GANC as if it was originating from the victim phone.

There is no way for the victim phone or the HNB-GW to detect that the message arriving at the operator network is not the same as the one that was originally sent. This demonstrates that, in the current femtocell architecture, it is impossible to ensure the integrity of subscriber data given an HNB is under control of an attacker.

3.3 Injecting Traffic/Impersonating Subscribers (Authenticity)

An even higher risk subscribers have to face is the complete impersonation of their subscriber identity. This means that an attacker is able to establish phone calls, send text messages or other data to the network while using a victim's subscriber information, without modifying any phone-generated traffic, allowing the attacker to bill the victim for attacker generated traffic. Reasonable threats include the abuse for social engineering, premium-rate service fraud, or simply the ability to make free phone calls. In this section, we describe how to perform such an attack, abusing subscriber information of a victim booked into a rogue femtocell. For the sake of simplicity, we demonstrate this by injecting an SMS on behalf of a victim using an attacker controlled femtocell.

In general, a phone attempting to use a service needs to issue a service request over a radio channel. To issue such a request on behalf of a victim, the victim's subscriber identity (namely the International Mobile Subscriber Identity (IMSI) or Temporary International Mobile Subscriber

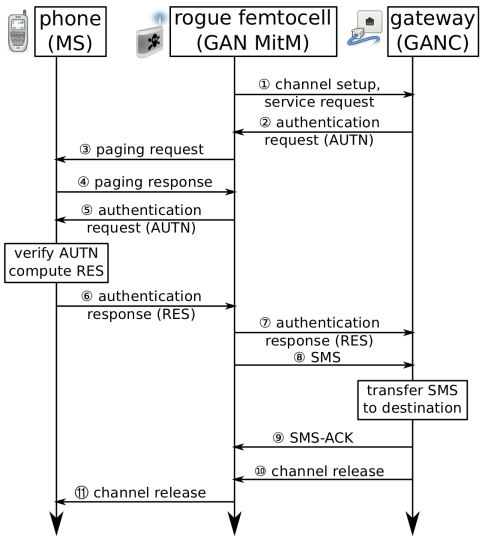

Figure 4. GAN MitM: SMS Injection.

Identity (TMSI)) needs to be known to the attacker. For this reason, the developed GAN proxy additionally caches every subscriber information exchanged between phones and operator network. In order to impersonate a subscriber, the attack client registers itself to the GAN proxy and requests a fresh subscriber identity. The proxy returns the identity (depending on the availability either IMSI or TMSI) to the client. Afterwards, the proxy is able to map GAN messages received from the attacking client to the existing TCP connection of the specific subscriber. As service requests are always authenticated in 3G, the attack client and proxy have to additionally circumvent this authentication. The actual attack, as illustrated in Figure 4, is performed as follows:

1. To send a text message, the attacker needs to setup a virtual radio channel over the existing TCP connection between the femtocell and GANC that belongs to the victim's phone. This is performed by sending a **`GA-CSR REQUEST`** message including an establishment cause indicating the reason for the resource allocation. After receiving, the GANC either accepts or denies this request.
   In case of an accept, the previously gathered subscriber identity is used by the attacking client to transfer a **`GA-CSR UPLINK DIRECT TRANSFER`** message to the GANC. This message carries the victim's subscriber identity and an L3 message indicating that the client is performing a service request and intends to send an SMS.
2. Since it is not possible to send text messages without being authenticated, the network replies with a **`GA-CSR DOWNLINK DIRECT TRANSFER`** message encapsulating an authentication request. The attack client can not properly answer this request as the secret key K that is required to compute the expected response (RES) is unknown (stored on the USIM).
3. The proxy solves this problem by paging the victim subscriber. This paging process is a normal procedure to make a phone aware of an incoming service. The victim phone user does not notice the paging request as it is sent before an actual incoming service is displayed on the device.
4. When the phone replies to the paging request, the proxy forwards the authentication request to the victim phone.
5. Next, the victim phone answers the authentication request. There is no way for the victim to detect that this event has been caused by an outgoing service request from the attacker.
6. The proxy forwards the authentication response to the GANC and stops further communication with the victim device.
7. After this step succeeded, the attacking client continues the process of injecting a fake **`SMS SUBMIT`** message of our choice to the operator network.
8. The carrier acknowledges the successful SMS transmission and allocated channels are released (10).

As mentioned before, the victim phone as well as the GANC are unable to detect this as long as the victim's phone is currently associated with the rogue femtocell. There is no way for the operator network to identify this message as being spoofed. The impact of this attack is serious as the resulting billing for the service is based on the victim's subscriber identity. We verified this in a real operator network using prepaid SIM cards. Therefore, this attack clearly violates the principle of message authenticity. Furthermore, this injection attack illustrates that the HNB specification violates one of the basic 3G security objectives (Clause 5, item a) described in [2]. We have to stress that this attack vector is not limited to text messages, but can be applied to phone calls or data connections in a similar way. While it is already possible to spoof caller-IDs and short messages (e.g., via external SMS gateway providers offering this as a service), the effect from an attacker's point of view is slightly different. Unlike when using spoofing services, the victim is billed for the usage of the service. Additionally, it is hard if not impossible to track the source of the spoofed message as no external gateway is used and the traffic is originating from within the operator network.

3.4 Denial of Service (Availability)

Another threat are Denial of Service (DoS) attacks against subscribers using a rogue femtocell. It was previously discovered [37] that the **`IMSI DETACH MM`** message is not authenticated in GSM and 3G networks. This

type of message is usually sent to the network when a mobile phone powers off. In particular, it represents the signal for the network indicating that the subscriber is no longer using the network and should not be paged for services. Because this message is not authenticated and no confirmation is delivered to the phone, an attacker can fake such **IMSI DETACH** messages to the network. As a result of this, the network assumes that the subscriber is disconnected from the network and thereby mobile-terminated services (incoming calls, text messages, etc.) are not delivered to the phone anymore. Therefore, the phone continues to assume that it is still connected and listens for paging requests.

Consequently, **IMSI DETACH** messages can be abused for DoS attacks against femtocell subscribers. However, since this message is delivered to the VLR which is usually responsible for a certain geographical area, the attack can not be performed from arbitrary locations. Because **DETACH** messages carry the subscriber identity of the phone to be detached, an attacker additionally has to know the identity (IMSI or TMSI) that currently maps to the victim within the operator network.

While in a typical network this attack is limited due to geographical constraints, it is possible to abuse this behavior in a more serious way in the case of a network of compromised femtocells. Operators usually deploy a dedicated VLR that is used for all femtocell subscribers in the network even though the customer devices are from widely scattered geographical locations. In practice this means that it allows us to detach the complete subscriber base of a femtocell network given the knowledge of the mobile identities. The process of gathering these required mobile identities from femtocell subscribers is described in Section 4.1. The injection of **IMSI DETACH** messages is based on the capability to send arbitrary L3 messages by utilizing the GAN protocol. In order to attack other subscribers, we have written a program that initiates a new connection to the GANC by sending a **GA-CSR REQUEST**. As soon as this "channel" is established, the program continues by sending a **GA-CSR UPLINK DIRECT TRANSFER** message carrying the required L3 message for the detach process. This L3 message consists of a detach indication and the victim's IMSI, because unlike the TMSI, the IMSI is not random.

There may be situations in which the detach would not work, since the subscriber is currently identified within the network using the TMSI rather than the IMSI. However, in practice it is easy to bypass this nuisance by submitting an unknown TMSI to the network. If the network is unable to resolve the TMSI to a subscriber, it requests the client to identify itself using the IMSI. We developed a program to automate this process by looping over a set of mobile identities and sending the required network packets to the GANC. Due to the nature of using a separate channel for each subscriber, this approach can further be optimized by parallelizing this process.

Hence, this Denial of Service (DoS) attack has a global impact on the availability of subscribers within the femtocell infrastructure. Our results show that it is possible to perform a large scale DoS attack from a rogue femtocell against all subscribers currently using the femtocell infrastructure.

4 Infrastructure Threats

Rogue femtocells do not only represent a serious threat to subscribers but also to network operators. Considering that these devices expose a certain part of the operator network to the device owner, it is important that infrastructural components are secured against attacks originating from within the network. Since femtocells are a part of the infrastructure as well, we also focus on their remote attack surface. Femtocells reside in the AN and not in the CN. Thus, not all components of the operator infrastructure are exposed to an attacker. However, several critical infrastructure elements exist within the AN. Additionally, it is possible to access some of the components in the CN by exploiting existing functionality of the femtocell. We conducted an analysis of the network entities exposed to a rogue femtocell in a real operator network and their potential for abuse.

This section is divided into three parts. The first part focuses on the possibility to collect information about other subscribers within the femtocell network. The second part analyses the attack surface of femtocells that may lead to a compromise of a remote device or the disruption of its services. The last part discusses how a combination of our findings can have a critical impact on the operator network as well as on the femtocell infrastructure.

4.1 Data Mining Subscriber Information

Given that an attacker can easily gain access to a single femtocell, it is interesting to know what parts of the network are exposed and what kind of information can be gathered. In the following paragraphs, we focus on which kind of information can be collected about mobile phone users via other femtocells within the femtocell's ecosystem.

Scraping The aforementioned hidden web interface on our device is not only accessible to the device owner or operator, but also from other femtocells within the carrier's network! Thus, anyone connected to the SeGW is able to collect the information provided by the web interface. This interface includes several interesting bits of subscriber information that an attacker can possibly collect. This information includes:

- The International Mobile Equipment Identity (IMEI) and IMSI of the femtocell: This can be used to spoof the identity of HNBs as presented in Section 5.
- The IMSI and telephone number (MSISDN) of every user registered in the CSGs: Along with this information, it additionally indicates if a subscriber is connected or performing a call. Collecting this data from all femtocell subscribers is clearly a privacy issue. Furthermore, the IMSI can also be utilized to perform IMSI-detach attacks as discussed in Section 3.4.
- The neighbor macrocell list: The femtocell needs to perform a scan for neighbor macrocells to determine which radio frequency can be used by the device. Additionally, the list is used by the OAMP to perform location verification as required by the 3GPP specification [14]. By using this list, attackers are able to geolocate the device with high precision. This reveals the exact location of the device, and due to the limited coverage, also the location of the subscribers using it.

Even if a femtocell does not offer a web interface, the configuration parameters need to be stored on the device. An attacker successfully getting root access to other devices, as shown in 4.2, will be able to collect this information as well.

Performance Measurement Server As required by the standard [7, 8], the femtocell monitors the overall cell activity and submits this data in the form of reports to the PM server. In our case, the device uploads a report every hour using FTP.

The operator we examined used a common FTP account for all femtocells, with no additional file system based security constraints. This enables our rogue femtocell to read all such reports, including those submitted by other femtocells. Due to this flaw, it is possible to collect all measurement reports from all femtocells in the carrier's network. In particular, the reports contain the following information: the IMEI and IMSI of the HNB; the measurement date; the cell ID, broadcasted Over-the-Air by the HNB; and the type, duration, and quantity of data transmitted (voice, video, or data traffic).

This enables detailed profiling of femtocells and connected subscribers in the network. While this issue may be an operator specific configuration error, the femtocell specifications require [8] carriers to support this feature. We believe that such information should be well protected and, if saved at all, in an encrypted form. Leakage of the IMEI and IMSI of each HNB exposes serious security threats since this data is used for enforcing access control policies (for example in provisioning process) within the network. In addition, it certainly endangers the privacy of the HNB subscribers by disclosing their activity.

4.2 Gaining Remote Root Access on Femtocells

If an attacker manages to gain root access on other devices within the carrier's network, all of the end-user attacks described in Section 3 become even more serious threats.

Therefore, we conducted a security analysis of the attack surface that our test device exposes to a remote attacker. This includes running services on the device and protocols used to communicate within the network. We identified the NTP and DNS networking protocols as well as a web server and a TR-069 provisioning service as attack vectors.

Besides NTP and DNS, the femtocell is not making use of any particularly exploitable network protocols. DNS is used to resolve NTP, SeGW, and OAM server names. NTP is often used by femtocells to provide frequency stability on the air interface [4]. Both of these protocols are implemented using standard Open Source software such as ntpdate and glibc functions. It is important to note that these protocols may be subject to spoofing attacks due to their UDP-based nature. Spoofing DNS to provide a firmware recovery server specified by an attacker seemed interesting. Nevertheless, it is not possible for a remote attacker, as this address is not resolved through the IPsec tunnel, but through the LAN interface, thus such an attack would require compromising ISP resolvers. Additionally, our test device is not making use of NTP authentication headers [36] which allows an attacker to spoof NTP server replies. This may impact the availability of the HNB by disrupting frequency adaption. However, none of the network protocols seemed to provide a practical way to gain root access to the device.

Instead, we focused more on the software services provided by the device. The configuration deployment is based on TR-069 [45] which has been adopted by the industry as the de-facto standard for remote provisioning. Both the OAMP services as well as the femtocell run a software stack implementing TR-069 which is based on the Simple Object Access Protocol (SOAP) over HTTP/S. SOAP itself is based on XML. The service providing this functionality is a proprietary daemon running on the femtocell. The provisioning port is also accessible from within the network, enabling the operator to proactively push configuration updates to the femtocell at any time. Additionally, our test device provides access to a web server which is also accessible within the femtocell network. The interface provided by the web server is used by the operator in order to debug customer problems and perform advanced configuration tasks.

Both of these services involve several protocols that are non-trivial to implement (given the history of bugs in web servers and XML parsers). We believe that these services are the most interesting attack vector. They will likely contain software vulnerabilities and poorly reviewed code (compared to the Open Source solutions used by the device). As often on embedded Linux systems, there is no

user management on the system and all services run with root privileges. This makes the system services and protocols used by the device an attractive target to attackers.

In order to backup this claim, we conducted an analysis of the web server software by means of reverse engineering the proprietary binaries. As a result, we discovered a buffer overflow in the processing of one of the web server's supported HTTP methods. We were able to successfully exploit this vulnerability and acquire root access to the device. This attack vector enables us to gain control over the femtocells of other customers as the carrier we examined enables any given femtocell to communicate with all other femtocells over the VPN. Thus, it leverages the previously described end-user threats in Section 3 to other femtocells in the network that are not under our physical control. The vulnerability is registered as CVE-2011-2900.

4.3 Leveraging Attacks Against Infrastructure Components

In this section, we describe how it is possible to further leverage the existing flaws to attack the operator infrastructure. We focus on attacks that do not target mobile phone users directly, but the availability and confidentiality of the network.

Signaling Attacks It is well known that attacks based on signaling pose noteworthy threats to the availability of cellular network systems [23, 40, 47]. Femtocells support radio signaling and communication with back-end networks by design. The femtocell exchanges signaling messages with architectural components such as VLR, HLR, AuC, and SGSN via the HNB-GW to offer mobile services to subscribers. Therefore they also provide potential for abusing this functionality to perform signaling attacks. As described in 3.3, it is possible to send malicious traffic to the HNB-GW from the femtocell, using our attack client and the GAN proxy. This indicates that if such a device is compromised and configured maliciously by an attacker, it can be used to carry out signaling attacks against classical CN components. While the gateway might apply rate filtering rules, the femtocell is intended to be used by multiple subscribers and thus provides an advantage compared to using a malicious mobile phone for such attacks. Furthermore, the femtocell is communicating via a broadband connection with the back-end and is not subject to additional constraints caused by radio communication (e.g. frequency stability and synchronization). Therefore, it can be used to inject signaling traffic into a network protocol basis at a comparably high rate. A reasonable threat is to use the presented GAN protocol to flood the network with *Location Update Requests* that include different IMSI numbers for each request [47]. As a result, it might be possible to considerably increase the load of the network because it has to generate and store authentication tokens as well as keeping state of these requests. Sending these requests can be performed without any mobile phone and can be automated using the aforementioned attack client to generate the corresponding L3 messages.

Femtocell Botnets Naturally the impact of DoS attacks originating from a single femtocell is limited. Therefore, performing signaling attacks in a distributed manner seems far more practical. A remote root access vulnerability, such as discussed in Section 4.2, contributes to this by providing a possibility to build a femtocell botnet. A number of characteristics that add to this are:

- Communication between femtocells is not filtered. It is important to note that the 3GPP standard explicitly allows communication between two femtocells [14].
- These devices are identical, making it a homogeneous network. Therefore a vulnerability discovered on one of these devices can be applied to all other femtocells within the network.
- Operators are actively deploying femtocells all over the country to extend 3G coverage, thus their number is growing rapidly. We identified around 5000 devices connected to the network in our target operator. The exact number of the deployed femtocells devices is not disclosed publicly by the operator yet.
- Due to the fact that it is a small device not intended for direct user interaction, it is hard for users to notice behavioral changes of them.
- Finally, femtocells are supposed to be always reachable and connected to the carrier's network.

Therefore, elevating a remote software vulnerability into a channel to control other femtocells to carry out distributed signaling attacks seems feasible. Moreover, abusing a large number of femtocells allows to send signaling traffic at a low-rate in low-volume and thus evade known detection mechanisms [32].

Global Interception Since direct communication between femtocells is permitted, it is possible to retrieve information from other devices, as demonstrated in Section 4.1. Besides gathering information, it also allows to change the configuration of other femtocells. The easiest way to achieve this is by using the web interface provided by the vendor. Another possibility to taint the femtocell configuration is to utilize a software vulnerability such as the root exploit mentioned in Section 4.2 and alter the settings in the device's database.

A crucial point of the femtocell communication is the selected HNB-GW address. By changing this address to an attacker-controlled IP address, it is possible to further extend the local user threats presented in Section 3 to a global threat affecting all femtocell-connected subscribers. Consequently, it allows an attacker to redirect signaling traffic of a victim's femtocell to an attacker supplied address. This could be running the previously mentioned GAN proxy. Therefore, attacks such as interception, modification or injection of arbitrary traffic can be leveraged to remote femtocells within the network.

Another important setting is the address of the SeGW. In particular, altering this address allows an adversary to force a remote femtocell to connect to an attacker-controlled SeGW. This can even be a machine outside the femtocell network running an IPsec server implementation. Even though the SeGW is authenticating itself based on a certificate stored on the femtocell, it can be simply replaced utilizing the root access. As explained in the next section, an attacker can connect to the SeGW without a femtocell in order to forward and intercept the traffic. Additionally, it is possible to reconfigure a victim's femtocell to act as an IMSI-Catcher and to operate in open access mode as explained in Section 3.1. As a result, not only registered subscribers but also mobile phones that are in the radio range of a remote device can be intercepted. Being able to route traffic among femtocells, combined with the ability to reconfigure the devices, enables an attacker to turn the femtocell infrastructure into a global interception network.

We believe that this indicates the inherent need for secure storage in femtocell devices to deploy certificate or other information required for authentication with the SeGW.

4.4 Opening Up the Access Network

Traditionally, carrier networks used to be completely separated from other public networks and inaccessible for adversaries. This changes with the integration of femtocells into the mobile telecommunication infrastructure. As explained before, the SeGW has been introduced to provide secure communication between the femtocells and operator's network and restrict access to the AN. It defends against network based attacks such as eavesdropping, injection, or altering of traffic. Additionally, it ensures authenticity of femtocells connecting to the network. Consequently, femtocell devices can securely communicate with the operator network via a public broadband connection and at the same time a separation between the Internet and the private operator network is maintained.

Due to this inherent requirement of network separation, the integrity of the femtocell is of high relevance. An attacker in full control of the femtocell can overcome this protection mechanism by tunneling traffic through the device. This can be easily achieved by installing, e.g., a SOCKS [33] proxy on the device or by using standard Linux network utilities such as iptables to transform the femtocell into a NAT router. Nevertheless, the necessity of utilizing such a device as a gateway to the operator network poses a serious limitation to attackers. Therefore, direct access to the SeGW would bypass this limitation. We show that it is possible to open up the access to the MNO network without a femtocell and thus increase the possibility to perform network based attacks against operator infrastructure.

The femtocell is communicating to the SeGW by an IPSec tunnel. The authentication procedure is based on EAP-SIM [28], utilizing the Subscriber Identity Module (SIM) placed inside the femtocell. Since the IPsec software on the device is based on a proprietary kernel module and user-space utility, it is difficult to figure out exact configuration details. However, by doing trial and error testing, it was possible to determine them.

Afterwards we applied these details to the configuration of a strongSwan [43] IPsec client running on a computer. Because it is possible to remove the SIM from the femtocell device, we were able to insert it into a smart card reader connected to this computer. As strongSwan directly supports EAP-SIM based authentication, this provides full connectivity to the carrier's network from a normal computer or any device capable of connecting a smart card reader.

Moreover, during our experiments it became clear that the setup does not even require a SIM that is provided within a femtocell (and obviously can be removed)! Any valid SIM card from the operator was able to connect to the SeGW. Therefore, our experimental setup overcomes the natural limitations and requirement of utilizing a femtocell device to attack the network, enabling connectivity to the carrier network from any computer using a prepaid SIM card.

5 Femtocell Security Architecture Vulnerabilities and Analysis

In this section, we discuss the current femtocell security architecture and determine its effect on the existing 3G security principles. We present weaknesses in the authentication process of femtocells that we discovered during our experimental analysis. Additionally, we argue how 3G security concepts contrast with the design of the femtocell security architecture.

Impersonating Femtocells According to 3GPP requirements [12], the femtocell has to register with the HNB-GW. This is achieved by sending **`GA-RC REGISTER REQUESTs`** that are based on the subscriber identity (IMSI). However, no additional security measures are applied to this message and the existence of the IPsec tunnel

is independent from this procedure. Therefore, it is possible to exploit this functionality to register femtocells using spoofed identities. In our case, this registration process is based on the IMSI stored in the femtocell's SIM, but can be altered either by modifying the system software or by using the presented GAN proxy. In practice this means that by spoofing this message, an attacker can impersonate any HNB that is known to the network. Subsequently, the femtocell security architecture fails to provide adequate authenticity protection during the registration phase of the device. Possible implications of this attack may be the bypass of existing access control policies implemented at the HNB-GW. Furthermore, it may be possible to eavesdrop on communication by subscribers registered at the spoofed HNB.

Key Material/AUTN Handling The lack of end-to-end confidentiality and integrity protection of the communication between the operator network and the phone is an another inherent design problem of the femtocell-enabled security architecture.

To provide OTA encryption, the carrier's network transfers the relevant data to the femtocell including the AUTN, RAND, XRES, CK, and IK values [49, 1, 13]. These enable confidentiality and integrity of signaling and user-generated data between the MS and the HNB. The communication is decrypted on the device and forwarded unencrypted to the HNB-GW. However, as discussed earlier in Section 2.4, local as well as remote attackers can compromise femtocells in various ways. As a result, total control over the HNB always implies the possibility to violate the confidentiality of subscriber-generated data once the IPsec connection is bypassed. Moreover, authentication tokens are sent to the device during subscriber registration attempts. Because the device supports roaming subscribers, the GAN protocol provides a trivial way to request AUTN tokens from the network for any subscriber by any operator. As demonstrated before, those can be reused (for a certain time) in other attack scenarios [35].

Even though it is required to transfer such authentication information to the femtocell, we believe that this contradicts with the current 3G security architecture, as it affects the principles of integrity and confidentiality. While similar procedures apply to traditional 3G networks, it is important to note that those are not generally accessible by adversaries, physically or by means of network attacks. Given the history of vulnerabilities in various embedded network devices [20], it may be difficult to ensure the physical security of femtocells while at the same time maintaining low production costs. Solely relying on the device to ensure security of subscriber communication seems unpractical.

6 Related Work

It is necessary to not only secure the femtocell subscribers and the device itself, but also the carrier's infrastructure against potential threats. While designing the femtocell security architecture and standards, the GSM Association and 3GPP have addressed such threats. In particular, they discuss security issues and potential attacking vectors experienced during the life-cycle of femtocell deployments [12, 34]. However, this specification frames various security aspects very abstractly and does not address some of the new threats that we have presented. In the academic context, a few security groups have analyzed the femtocell security challenges and requirements [39] and proposed new protection mechanisms [27]. Our research contributes to this, providing extensive experimental results by evaluating a commercially deployed femtocell.

Despite the security requirements, a few researchers have demonstrated weaknesses in such systems to gain root access [29, 17, 16, 46]. Therefore, it shows that such threat is real and these crucial security issues are not only present in a single device or operator network. However, most of this research has solely targeted the femtocell's security shortcomings and does not address practical attacks and their impact against the carrier infrastructure and end-users. Our work differs from these groups by measuring the impact of integrating compromised femtocells into the mobile network infrastructure, which deals with security and privacy issues affecting both the end-users and mobile operators.

Additionally, our work describes how an HNB can be abused to build a 3G IMSI-Catcher. These devices tend to be very expensive on the market. Wehrle and Paget recently demonstrated [38, 48] that they can be built using low cost hardware and Open Source software. However, their research exploits well known vulnerabilities of the GSM authentication protocol required to build such a device. Meyer and Wetzel demonstrated that under some circumstances it is possible to perform a UMTS MitM attack by downgrading a victim phone to use GSM [35]. Instead of exploiting GSM weaknesses, we bypassed the problem of mutual authentication provided by 3G in order to turn an HNB into a low cost 3G IMSI-Catcher device.

7 Conclusion

Deployed 3G femtocells already outnumber traditional 3G base stations globally, and their deployment is increasing rapidly. However, the security of these low-cost devices and the overall architecture seems poorly implemented in practice. They are inherently trusted, able to monitor and modify all communication passing through them, and with an ability to contact other femtocells through the VPN net-

work. Yet when placed in untrustworthy hands, this assumption of trust proves dangerous.

In this paper, we evaluated and demonstrated attacks originating from a rogue femtocell and their impact on end-users and mobile operators. It is not only possible to intercept and modify mobile communication but also completely impersonate subscribers. Additionally, using the provided access to the operator network, we could leverage these attacks to a global scale, affect the network availability, and take control of a part of the femtocell infrastructure.

Telecommunication network security is traditionally based on secrets, trust relationships and the fact that it is hard for adversaries to tamper operation equipment. It has become evident in the past (e.g. due to external gateway providers, massive fraud problems, 3G to GSM downgrade attacks) that it is problematic to rely on this trust. Still the femtocell technology relies on a single point of failure, the device itself.

As our experimental results demonstrate, this has a considerable impact on mobile telecommunication. We believe that attacks specifically targeting end-users are a major problem and almost impossible to mitigate by operators due to the nature of the current femtocell architecture. The only solution towards attacks against end-users would be to not treat the femtocell as a trusted device and rely on end-to-end encryption between the phone and the operator network. However, due to the nature of the 3G architecture and protocols and the large amount of required changes, it is probably not a practical solution.

Finally, the authors would like to question whether or not the practical advantages of femtocell technology outweigh their potential for critical attacks.

Acknowledgements

We would like to thank Nicholas Weaver for his many insightful comments on this paper and guidance throughout the process of creating the camera-ready version. Additionally, we would like to thank Ramtin Amin for providing us with a copy of his libuma code which we used as the basis for our attack toolkit. Furthermore, we thank Dmitry Nedospasov for his help in reviewing this paper.

References

[1] 3GPP. Universal Mobile Telecommunications System (UMTS); 3G Security; Integration Guidelines. Technical Specification TS 33.103 v4.2.0, 3G Partnership Project, September 2001.

[2] 3GPP. Universal Mobile Telecommunications System (UMTS); LTE; 3G Security; Security Principles and Objectives. Technical Specification TS 33.120 v4.0.0, 3G Partnership Project, March 2001.

[3] 3GPP. Service requirements for Home Node B (HNB) and Home eNode B (HeNB). Technical Specification TS 22.220 v11.2.0, 3G Partnership Project, June 2005.

[4] 3GPP. Security of H(e)NB. Technical Report TR 33.820 v8.3.0, 3G Partnership Project, December 2009.

[5] 3GPP. Generic Access Network (GAN); Mobile GAN interface layer 3 specification. Technical Specification TS 44.318 v9.2.0, 3G Partnership Project, March 2010.

[6] 3GPP. Generic Access Network (GAN); Stage 2. Technical Specification TS 43.318 v9.0.0, 3G Partnership Project, February 2010.

[7] 3GPP. Telecommunication management; Performance Management (PM); Concept and requirements. Technical Specification TS 32.401 v9.1.0, 3G Partnership Project, October 2010.

[8] 3GPP. Telecommunications management; Home Node B (HNB) Operations, Administration, Maintenance and Provisioning (OAM&P); Concepts and requirements for Type 1 interface HNB to HNB Management System (HMS). Technical Specification TS 32.581 v9.2.0, 3G Partnership Project, April 2010.

[9] 3GPP. Universal Mobile Telecommunications System (UMTS); LTE; Network architecture. Technical Specification TS 23.002 v9.2.0, 3G Partnership Project, January 2010.

[10] 3GPP. Mandatory Speech Codec speech processing functions; Adaptive Multi-Rate (AMR) speech codec; Transcoding functions. Technical Specification TS 29.090 v10.0.0, 3G Partnership Project, April 2011.

[11] 3GPP. Mobile Application Part (MAP) specification. Technical Specification TS 29.002 v10.3, 3G Partnership Project, January 2011.

[12] 3GPP. Security of Home Node B (HNB) / Home evolved Node B (HeNB). Technical Specification TS 33.302 v11.2.0, 3G Partnership Project, June 2011.

[13] 3GPP. Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Security architecture. Technical Specification TS 33.102 v9.4.0, 3G Partnership Project, January 2011.

[14] 3GPP. UTRAN architecture for 3G Home Node B (HNB); Stage 2. Technical Specification TS 25.467 v10.2.0, 3G Partnership Project, June 2011.

[15] ABI Research. One Billion Mobile Broadband Subscriptions in 2011: a Rosy Picture Ahead for Mobile Network Operators. http://www.abiresearch.com/press/3607-One+Billion+Mobile+Broadband+Subscriptions+in+20113A+a+Rosy+Picture+Ahead+for+Mobile+Network+Operators, February 2011.

[16] R. Allen, R. Allen, and D. Kelly. Gaining root on Samsung Femtocells. http://rsaxvc.net/blog/2011/07/gaining-root-on-samsung-femtocells.html, July 2011.

[17] R. Borgaonkar, K. Redon, and J.-P. Seifert. Security Analysis of a Femtocell device. In *Proceedings of the 4th International Conference on Security of Information and Networks*, SINCONF. ACM, November 2011.

[18] Cisco. Cisco Visual Networking Index: Forecast and Methodology, 2010-2015, February 2011.

[19] 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, January 2011.

[20] A. Cui, Y. Song, P. V. Prabhu, and S. J. Stolfo. Brave New World: Pervasive Insecurity of Embedded Network Devices. In *12th Annual International Symposium on Advances in Intrusion Detection*, RAID '09, pages 378–380, Berlin, Heidelberg, September 2009. Springer-Verlag.

[21] M. Dallachiesa. rtpbreak. http://dallachiesa.com/code/rtpbreak/.

[22] G. de la Roche, A. Valcarce, D. López-Pérez, and J. Zhang. Access control mechanisms for femtocells. *Communications Magazine, IEEE*, 48:33–39, January 2010.

[23] W. Enck, P. Traynor, P. McDaniel, and T. La Porta. Exploiting Open Functionality in SMS-Capable Cellular Networks. In *Proceedings of the 12th ACM conference on Computer and communications security*, CCS '05, pages 393–404, New York, NY, USA, 2005. ACM.

[24] Z. Fasel and M. Jakubowski. Infrastructure Weaknesses in Distributed Wireless Communication Services. http://www.shmoocon.org/, February 2010.

[25] Femto Forum. Femtocell Market Status. http://www.femtoforum.org/femto/pdfs01.php, February 2011.

[26] Femto Forum. Femtocell Market Status. http://www.femtoforum.org/femto/pdfs01.php, June 2011.

[27] C.-K. Han, H.-K. Choi, and I.-H. Kim. Building Femtocell More Secure with Improved Proxy Signature. In *Global Telecommunications Conference, 2009. GLOBECOM 2009. IEEE*, pages 1–6, Honolulu, HI, November 2009.

[28] H. Haverinen and J. Salowey. Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM). RFC 4186, 3G Partnership Project, January 2006.

[29] N. Jacobsen. Samsung-Femtocell. http://code.google.com/p/samsung-femtocell/, March 2011.

[30] Kineto Wireless. UMA: The 3GPP Standard for Femtocell-to-Core Network Connectivity. http://www.kineto.com/products/downloads/wp_UMA_Femto_3GPP_2007.pdf, 2007.

[31] Kineto Wireless Inc. official Unlicensed Mobile Access presentation webiste. http://www.smart-wi-fi.com/, June 2010.

[32] P. P. C. Lee, T. Bu, and T. Woo. On the Detection of Signaling DoS Attacks on 3G Wireless Networks. In *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 1289–1297, Anchorage, AK, May 2007.

[33] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L. Jones. SOCKS Protocol Version 5. RFC 1928, March 1996.

[34] R. Mangtani. Security Issues in Femtocell Deployment. Technical Report 1.0, GSM Association, July 2008.

[35] U. Meyer and S. Wetzel. A Man-in-the-Middle Attack on UMTS. In *Workshop on Wireless Security*, pages 90–97, 2004.

[36] D. L. Mills. Network Time Protocol (Version 3) - Specification, Implementation and Analysis. RFC 1305, March 1992.

[37] S. Munaut. IMSI Detach DoS. http://security.osmocom.org/trac/ticket/2, May 2010.

[38] C. Paget. Practical Cellphone Spying. https://www.defcon.org/html/defcon-18/dc-18-speakers.html#Paget, August 2010.

[39] R. Rajavelsamy, J. Lee, and S. Choi. Towards security architecture for Home (evolved) NodeB: challenges, requirements, and solutions. *Security and Communication Networks*, 4(4):471–481, April 2011.

[40] J. Serror, H. Zang, and J. C. Bolot. Impact of Paging Channel Overloads or Attacks on a Cellular Network. In *Proceedings of the 5th ACM workshop on Wireless security*, WiSe '06, pages 75–84, New York, NY, USA, 2006. ACM.

[41] SFR. SFR Home 3G : pour une couverture 3G optimale à domicile. http://www.sfr.fr/vos-services/equipements/innovations/sfr-home-3g/.

[42] SFR press release. SFR lance le service Femtocell, SFR Home 3G, pour offrir la meilleure couverture 3G au domicile de ses clients. http://www.sfr.com/presse/communiques-de-presse/sfr-lance-le-service-femtocell-sfr-home-3g-pour-offrir-la-meilleure, November 2009.

[43] A. Steffen, M. Willi, and T. Brunner. strongSwan IPsec solution. http://www.strongswan.org/, June 2011.

[44] M. Storsjo. OpenCORE. http://sourceforge.net/projects/opencore-amr/.

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

[46] The Hacker's Choice. Vodafone Access Gateway. http://wiki.thc.org/vodafone, June 2011.

[47] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. Mcdaniel, and T. La Porta. On Cellular Botnets: Measuring the Impact of Malicious Devices on a Cellular Network Core. In *Computer and Communications Security*, pages 223–234, 2009.

[48] D. Wehrle. Open Source IMSI-Catcher für GSM. http://www.ks.uni-freiburg.de/php_arbeitdet.php?id=166, October 2009.

[49] J. Zhang and G. de la Roche. *Femtocells: Technologies and Deployment*. John Wiley & Sons, Ltd, March 2010.

APPENDIX

Acronyms

3G	Third Generation. 1, 2, 4–7
3GPP	3rd Generation Partnership Project. 3–5
AN	Access Network. 3, 9, 12
AuC	Authentication Center. 3, 6, 11
AUTN	Authentication Token. 5, 6
CK	Cipher Key. 6, 13
CM	Connection Management. 7
CN	Core Network. 3, 4, 6, 7, 9, 11
CS	Circuit Switched. 3, 4
CSG	Closed Subscriber Group. 6, 10
DoS	Denial of Service. 9
ESP	Encapsulating Security Payload. 6
FMC	Fixed Mobile Convergence. 1
GAN	Generic Access Network. 4, 6–9, 11–13
GANC	GAN Controller. 4, 6–9
HLR	Home Location Register. 3, 11
HMS	HNB Management System. 3
HNB	Home Node B. 2–5, 7, 8, 10, 13
HNB-GW	HNB GateWay. 3, 4, 6, 7, 11–13
HNS	Home Node B Subsystem. 3
HSS	Home Subscriber Server. 3
IK	Integrity Key. 6, 13
IMEI	International Mobile Equipment Identity. 10
IMSI	International Mobile Subscriber Identity. 7, 9–13
L3	3GPP Layer 3. 4, 8, 9, 11
MCC	Mobile Country Code. 6
MitM	Man-in-the-Middle. 7
MM	Mobility Management. 7
MNC	Mobile Network Code. 6
MNO	Mobile Network Operator. 1, 4, 12
MS	Mobile Station. 3, 4, 13
MSC	Mobile Switching Center. 3
NB	Node B. 3, 5
OAM	Operation, Administration, and Maintenance. 4, 5, 10
OAMP	Operation, Administration, Maintenance, and Provisioning. 3, 10
OTA	Over-the-Air. 6, 7, 13
PS	Packet Switched. 3, 4
PSTN	Public Switched Telephone Network. 3
RES	Authentication Response. 6
RNC	Radio Network Controller. 3–5
RNS	Radio Network Subsystem. 3
SeGW	Security GateWay. 3, 6, 9, 10, 12
SFR	Société Française du Radiotéléphone. 2
SGSN	Serving GPRS Support Node. 3, 11
SIM	Subscriber Identity Module. 12, 13
SMS	Short Message Service. 7, 8
SOAP	Simple Object Access Protocol. 10
TMSI	Temporary International Mobile Subscriber Identity. 7, 9
UMA	Unlicensed Mobile Access. 4
USIM	Universal Subscriber Identity Module. 5, 6
VLR	Visitor Location Register. 3, 9, 11
XRES	Expected Response. 6