Experimental Analysis of the Femtocell Location Verification Techniques

Ravishankar Borgaonkar, Kevin Redon, and Jean-Pierre Seifert

Security in Telecommunications
Technische Universität Berlin and Deutsche Telekom Laboratories
10587, Berlin, Germany
{ravii,kredon,jpseifert}@sec.t-labs.tu-berlin.de

Abstract. Mobile network operators are adapting femtocells in order to simplify their network architecture for increased performance and greater revenue opportunities. While emerging as a new low-cost technology which assures best connectivity, it has also introduced a range of new potential risks for the mobile network operators. Here we study the risks associated with the location verification techniques of femtocells. First we state the goals of location verification and describe techniques implemented in the existing femtocells. We demonstrate how location locking techniques can be defeated by using modern attack vectors against the location verification methods. Our experimental result suggest that location security methods are insufficient to avoid femtocell's misuse. An attacker can operates the femtocell from an unregistered location, thereby creating problems for various important services such as for assisting emergency call services, for following licensed spectrum rules, for Lawful interception services, and for the commercial purposes.

Keywords: Femtocell, HNB, Security, Location.

1 Introduction

Femtocell is a emerging technology which enhances third generation (3G) coverage and provides assurance of best connectivity in the 3G telecommunication networks. It acts as an access point that securely connect standard mobile stations to the mobile network operator's core network using an existing wired broadband connection. For mobile service operators key benefits are increase in network capacity, lowers capital cost and expands revenue opportunities. For users it assures increase in indoor coverage, higher rate of data transfer, high quality voice and higher multimedia experience. A femtocell can be deployed in a licensed spectrum owned by a mobile network operator and in the users premises, for example home, office and enterprise.

The femtocell security is divided into two parts: the device authentication and the encryption of the calls and control information transferred across the untrusted backhaul connection between the femtocell and the femtocell gateway. Even though the femtocell supports the necessary security features that a base

T. Aura, K. Järvinen, and K. Nyberg (Eds.): NordSec 2010, LNCS 7127, pp. 49–54, 2012.

station provides; in particular which are mutual authentication, encryption and integrity over the wireless link, there are still two issues. First is use of 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. Secondly, 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.

Main aim of our study is to analyze the risk associated with the femtocell security. Our study finds that the femtocells, which are currently deployed in the market, are insecure and do not follow the security requirements mentioned by the 3GPP standard. In this paper, we experimentally evaluate various security aspects, in particular, the location verification techniques used in the device. We examine and show that the location verification techniques are inadequate to block the use of femtocell, if it is operating at an unregistered location and at unlicensed frequency spectrum.

The rest of the paper is organized as follows. Section 2 describes security architecture of femtocell. Section 3 explains goals of location locking methods of the femtocell. Femtocell location tracking methods and various attacking vectors are presented in Section 4. Conclusions and discussions are presented in Section 5. Note that the Home NodeB (HNB) is the 3GPP standard name of the femtocell and we will use the HNB in the following sections.

2 HNB Security Architecture

The HNB is installed in the users' premises and its traffic is tunneled via public Internet (wired broadband) connection. Hence for the mobile network operator, it is important to ensure that HNB protects the communication over the insecure public Internet, and over the air-link between itself and the mobile device. Main components of the HNB security architecture and their roles are described as follows [3,1]:

HNB Device- The main function of the HNB is to act as a small base station. The HNB connects the UE via its radio interface to the mobile service operator's core network. It transmits the UE data by establishing a secure IPsec [4] ESP tunnel with the SeGW over an insecure backhaul link (broadband Internet connection).

SeGW - The SeGW acts as a border gateway of the operator's core network. First, it mutually authenticates and registers the HNB to establish a secure IPsec tunnel, and then forwards all the signaling and the user data to the operator's core network. Mutual authentication can be performed using certificates. The interface between the SeGW and the operator's core network is considered to be secured.

HNB Management System (HMS) - The HNB Management System is a management server, and responsible for the configuration and the provisioning of the user data according to the operator's policy. It can be functioned to provide the required software updates on the HNB and can be located inside the operator's core network.

AAA Server and HSS - The subscription data and authentication information is stored in the HSS. The AAA server authenticates the hosting party (the HNB) by accessing the authentication information from the HSS. Both the AAA server and the HSS are deployed in the operator's core network.

HNB GW - The HNB gateway performs the access control for the non-CSG (Closed Subscriber Group) capable UE attempting to access a HNB. The SeGW can be integrated with a HNB-GW, and if not integrated then, the interface between SeGW and HNB-GW may be protected using NDS/IP (Network Domain Security/IP network layer security) [5] .

UE- The UE is a standard user equipment that supports the 3G (UMTS) communication. It connects to the HNB over-the-air using a 3G AKA (Authentication and Key Agreement) procedure.

3 Goals of the Location Locking Methods

It is important for the operator to ensure that the HNB operates at the given location and satisfy various requirements such as security, regulatory, and operational requirements [2]. The HNB can only provide reliable and accurate home address information if the users keep them in their assigned and registered location. However, it is possible for users to move the HNB when traveling, intending to continue using free roaming service anywhere they go. This could led to a verity of problems for the operator. Hence the operator has to lock the HNB to a specific location for the following reasons: a) to provide the users location for emergency calls, b) to ensure that the HNB is operating in a country in which it has a network operation, c) to provide real-time lawful interception data to the government agencies.

4 Location Locking Methods and Attacks

In this section, we describe location locking techniques implemented in the HNBs. Then we present various attack vectors to beat these location locking methods. Note that without opening the HNB box and with no physical tampering, we were able to bypass the location locking methods. We performed experimental analysis of the location locking techniques in a Faraday Cage. Different attacks on the location based techniques were performed in the cage only. Though the attacks we described below are performed on the two HNB, it may affect other HNBs which are deployed currently.

The HMS registers and verifies location information of the HNB. First the operator registers and fix the HNB location information in the server called Access point Home Register (AHR). After the initial registration process, the operator obtains the location information of the HNB and compares it with the corresponding information stored in the AHR. The main parameters used for identifying the HNB location information are a) IP address of the broadband access device, b) information of the surrounding macro-cells ,and c) information

received from the GPS device attached to the HNB or the UE. In this section, we explain these location locking mechanisms deployed in the HNB system architecture [3]. They are as follows:

4.1 IP Address of the Broadband Access Device

The HNB gets an IP address when connected to the devices which provides the broadband access such as a DSL modem or a home router. The operator can locate the HNB by its assigned IP address and by the location information related to IP address which is stored in the server (AHR). When the HNB is placed behind NAT (Network Address Translator), STUN protocol is used to determine its IP address. The HNB operator can request the geographic location information based on the IP address to the interface defined by the NASS (Network Attachment Subsystem) standard [6].

Attack Vectors

The virtual private network (VPN) can be used to impersonate the IP address of the legitimate HNB. A VPN emulates a private IP network over the public Internet infrastructure [7]. The VPN technology can be used to connect remotely to the a LAN (Local Area Network) (where the HNB in installed and registered) and thus the HNB can obtain a local IP address. Thus VPN can be used to impersonate the IP address of the legitimate HNB and the use of IP address for location authentication is not considered reliable.

There may be a situation in which the 3G or 2G signals are not be available in the home In addition, not all the HNB devices are equipped with the GPS receivers. In these circumstances, the operator has two parameters to authenticate the HNB location: IP address and the information received from the UE. However it is obvious that if there are no 2G or 3G signals in the area, the HNB can not receive any information from the UE. For the attack, we use a VPN to replay the HNB's IP address. We placed the HNB to an unregistered location and established a VPN tunnel to the LAN at the HNB's registered location. We were able connect the HNB to the SeGW with the registered IP address. We were able to operate the HNB in a normal mode from an unregistered location.

4.2 Information of Neighboring Macro-cells

The HNB can receive neighboring macro-cells information such as PLMN ID (Public Land Mobile Network Identity), LAI (Location Area Identity) or Cell ID. It contains a hardware chip to scan PLMN ID and cell ID. In this method, first ,the HNB scans the neighboring macro-cells information in a receiver mode when it powered on and sends this scanned information to the AHR (Home Register of HNB). The AHR role is to store this information along with the registration message requests to the appropriate HNB profiles. Most of the electronic devices including the HNB use a 2G receiver hardware to scan the neighboring macro-cell information because 3G signals are weak inside the house.

Attack Vectors

In this scenario, the operator can fetch and use neighboring micro-cell information to perform location authentication of the HNB device. As discussed earlier in Section 4.1, the adversary can use a VPN connection to emulate the IP address. However, in order to operate the HNB with the given regulations, the attacker still needs to block or simulate neighboring micro-cell information. This can be done in two ways. An attacker can use a 2G signal jammer device. The 2G jammer devices blocks any nearby 2G network signals without interrupting other electronic devices. We analyzed a few HNB devices and found that most of the devices use a 2G receiver hardware to record neighboring micro-cell information. Hence it is possible to block nearby 2G network signals using such jammers without interrupting the 3G network signals of the HNB.

In other way, the attacker can use a nanoBTS [9] and openBSC package to replay the neighboring micro-cell information. The nanoBTS picocells are small 2G (GSM) base-stations that use the A-bis interface. They can be connected to the openBSC with A-bis over IP interface [10]. The adversary can configure the nanoBTS to transmit the recorded (registered) micro-cell information. In this way, the attacker can show that the HNB is operating at the given and registered location by providing the legitimate micro-cell information. We examined this attack using a nanoBTS and were able to provide required information to the HNB for location authentication.

4.3 UE Information

The UE position can be useful to verify the HNB location, provided that it is equipped with the GPS (Global Positioning System) feature. In addition, the UE can send its location information using available micro-cells or GPS data to the AHR via the HNB.

4.4 GPS Information

The location information can be obtained using an A-GPS receiver unit built inside the HNB. A-GPS (Assisted GPS) is a system used to improve the start-up performance of a GPS satellite-based positioning system [8]. The HNB can receive the location information from the A-GPS unit and deliver it to the home registration server for the verification. However, it is important to install the HNB in a location where it can receive the GNSS (Global Navigation Satellite Systems) satellites signals.

Attack Vectors

Use of GPS as a geolocation technology is ineffective since the HNBs are installed in the home and GNSS signals are weak inside the house. However some mobile network operators suggest to use an additional antenna to improve the signal strength. The attacking vectors against this mechanism includes jammers, an

attenuation methods, and GPS generators devices. An attacker can use of GPS jammers. These low cost jammers are commercially available in the market and could be positioned in the vicinity of HNB antenna. This attack could be arguable due to legal issues in using the jammer. In an attenuation method, the attacker can wrap the HNB in layers of aluminum foil to create a Faraday cage like environment and blocks the GPS signals. The GPS generators are the devices used by GPS manufactures for the research and development. It can transmit the recorded timing signals and orbital data. The attacker can use such devices to spoof the HNB. The method in which the HNB receive location information from the UE is not reliable, since in the UE may not have inbuilt GPS feature and not receive 3G or 2G signals.

5 Discussion and Conclusion

In this paper, we practically analyzed and showed that the location verification techniques used in the femtocells that are built and deployed today are insufficient to avoid its misuse. Our results reveals that the femtocell location can be spoofed by an adversary which could have impact on the emergency services, on the lawful interception procedure, and on the operators regulations. An adversary may move femtocells for avoiding expensive roaming calls while traveling and for hiding his location from government agencies. Our study suggest that most of the femtocells deployed today are vulnerable against the modern location attack vectors. Hence new additional location locking mechanisms are needed to improve the overall femtocell security architecture.

References

1. 3GPP, Security of Home Node B (HNB) / Home evolved Node B (HeNB), TS 33.320, V9.1.0 (April 2010), http://www.3gpp.org
2. 3GPP Technical Specification Group Service and System Aspect, Security of H(e)NB, TR 33.820, V8.3.0 (December 2009)
3. 3GPP TR 33.820 V8.3.0: Technical Specification Group Service and System Aspects; Security of H(e)NB; (Release 8)
4. Kent, S., Atkinson, R.: [RFC 2406]: IP Encapsulating Security Payload (ESP), http://www.ietf.org/rfc/rfc2406.txt
5. 3GPP TS 33.210: Network Domain Security (NDS); IP network layer security (IP)
6. ETSI ES 282 004 V1.1.1 Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); NGN functional architecture; Network Attachment Sub-System(NASS) (2006)
7. Gleeson, A., Lin, A., Heinanen, J., Armitage, G., Malis, A.: [RFC 2685]: A framework for IP Based Virtual Private Networks
8. Djuknic, G.M., Richton, R.E.: Geolocation and Assisted GPS. IEEE Computer 34, 123–125 (2001)
9. The nanoBTS: small GSM base stations, http://www.ipaccess.com
10. OpenBSC, http://openbsc.gnumonks.org/trac/wiki/nanoBTS