

Security Issues in Next Generation Mobile Networks: LTE and Femtocells

Igor Bilogrevic, Murtuza Jadliwala and Jean-Pierre Hubaux

Laboratory for computer Communications and Applications (LCA1), EPFL, Lausanne, Switzerland
{firstname.lastname}@epfl.ch

Abstract—Cellular mobile networks are used by more than 4 billion users worldwide. One effective way to meet the increasing demand for data rates is to deploy femtocells, which are low-power base stations that connect to the mobile operator through the subscriber’s residential Internet access. Yet, security and privacy issues in femtocell-enabled cellular networks, such as UMTS and LTE, still need to be fully addressed by the standardization bodies. In this paper, we review significant threats to the security and privacy of femtocell-enabled cellular networks. We also propose novel solution directions in order to tackle some of these threats by drawing inspiration from solutions to similar challenges in wireless data networks such as WLANs and mobile ad hoc networks (MANETs).

I. INTRODUCTION

The use of mobile devices has changed since the advent of digital technologies such as GSM. What started as a voice only service, has been upgraded to support data traffic as well. With modern smartphones, users are able to browse the Internet and obtain services such as ebanking, navigation, social networking and recommendations based on the subscriber’s location. Femtocells, which are low-power and low-range base stations for cellular networks installed by users at their own premises, are believed to meet the surge in data rates that these multimedia and interactive services require. They offload the macrocell network and provide backhaul connections to the cellular operators’ networks through the users’ residential broadband accesses [7].

Long Term Evolution (LTE) is the mobile network technology for the next generation mobile communications, as defined by the 3rd Generation Partnership Project (3GPP) [1]. In addition to features such as increased data-rates, lower latencies and better spectral efficiency, one of the most interesting aspects is the radically novel all-IP core network architecture, known as Evolved Packet Core (EPC). LTE is expected to make extensive use of user-installed femtocells, in order to achieve its goals of spectral efficiency and high-speed for a greater number of users. It is clear that the sensitivity and confidentiality of users and data transiting in such digital cellular networks is paramount both to businesses and private users.

Security and privacy in such networks is achieved at several levels in their architectures, such as the air interface, the operator’s internal network and the inter-operator links. The main assumption underlying the security of legacy mobile networks, such as GSM and UMTS, is the trust that each operator has in its own infrastructure and in other operators

with whom it has a roaming agreement. Clearly, the evolution to LTE and its flat all-IP core network emphasizes the urgency for a revision of trust relationships among operators and their network components, as both their exposure and vulnerability to external threats are greatly affected. For instance, it has become easier for a malicious user to tamper with the femtocell in order to access confidential data, as it resides directly at the user’s premises, or to disrupt the legitimate communications both at the femtocell and at the core network level, due to the openness of the IP networks.

Our goal in this paper is to raise awareness about security and privacy issues in femtocell-enabled cellular networks, such as LTE, by reviewing some significant security threats and countermeasures. Our solutions are inspired from similar research efforts in the WLAN and mobile ad hoc network (MANET) research community.

The rest of this paper is organized as follows. In Section II we review present security and privacy threats in femtocell-enabled networks, with a focus on user data privacy and robustness of the core network. In Section III we discuss possible solution directions and their challenges. We conclude the paper in Section IV.

II. SECURITY AND PRIVACY CHALLENGES

Figure 1 shows the threat model for a femtocell-enabled mobile network. The three vulnerable elements are indicated by arrows: (i) the air interface between the mobile device (User Equipment) and the femtocell (Home(e)NodeB), (ii) the femtocell itself and (iii) the public link between the femtocell and the security gateway (SecGW). Our intent is to focus on certain attacks on the aforementioned elements, which are achievable without breaking the cryptosystems or the protocols. A more exhaustive list of all possible attacks and countermeasures can be found in [2].

A. Attacks on the Air Interface

The attacks on the air interface can be either passive (the attacker only passively listens to the communications between the mobile device and the base station) or active (in addition to listening, the attacker injects or modifies the data). Although prerogatives for active attacks have been mitigated by cryptographically protecting the messages sent over the air, passive attacks, such as traffic analysis and user tracking, are still possible.

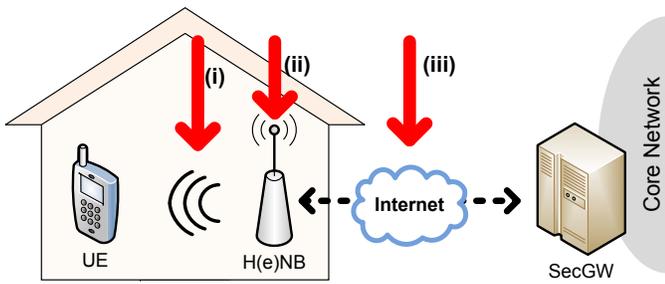


Figure 1. Three different targets for malicious attacks on femtocell-enabled mobile networks: (i) the air interface between the mobile device (User Equipment) and the femtocell (Home(e)NodeB), (ii) the femtocell itself and (iii) the public link between the femtocell and the security gateway.

The issue of user identity protection was already raised in the early GSM networks, and the solution that has been adopted ever since has never been substantially revisited. With the ongoing migration towards all-IP and femtocell-enabled cellular networks, the legacy solution might not be appropriately suited anymore. In fact, GSM, UMTS and LTE standards mandate the use of unlinkable temporary identifiers (TMSIs [3] and GUTIs [4]) to protect the identity of mobile devices at the air interface, but the capillary deployment of femtocells might render this insufficient to guarantee a satisfactory level of protection for the users. TMSIs (or GUTIs) are usually unchanged in a given location (or tracking) area, which is composed by up to a hundred adjacent cells, and femtocells could make it possible for malicious users not only to track the movements of mobile subscribers, but due to the low range, to have an unprecedented accuracy as well. For instance, such tracking attacks could be perpetrated by curious employers, in order to monitor whether an employee is visiting a competitor, or by governmental agencies, in order to illegitimately track people's locations.

Subscriber identity and tracking are the emerging threats at the air interface in femtocell-enabled mobile networks. Solutions that are suited for such networks can be inspired from the experience gained by the research community in MANETs. In particular, studies such as [5], [8] suggest directions for a more dynamic and context-aware location privacy protection mechanisms. We discuss the most relevant aspects in Section III.

B. Attacks on the Femtocell

From the perspective of a mobile device, being connected to a regular base station, i.e., (*e*)NodeB, or a femtocell is equivalent, because the protocols and security standards used at the air interface are exactly the same. From a malicious user's point of view, it makes a substantial difference because it is much easier for a malicious user to tamper with a small and inexpensive (£120 [15]) femtocell than it could be with a large and complicated device located on a rooftop. The physical size, material quality, lower cost components and the IP interface of the femtocell make it more suited for reverse engineering and tampering than a traditional, more expensive and business-grade (*e*)NodeB base station.

As the over-the-air user data encryption is terminated at the femtocell, hardware tampering with the device could expose the private information of the unsuspecting user. For instance, if an adversarial user is able to set the femtocell to accept all external users without having to register them first, as opposed to having a Closed Subscriber Group (CSG), he would be able to analyze their communications. Moreover, attacks such as device impersonation, Internet protocol attacks on the network services, false location reporting or simply unauthorized reconfiguration of the onboard radio equipment could hinder the network operator from controlling interference and power management features. This could have severe consequences on the quality of service. To this end, femtocells should be equipped with trusted execution environments (TrE) [2] that render malicious manipulation of the onboard software and the on-the-wire sniffing very hard to achieve. However, as femtocells are authorized to operate only on specific geographic areas, false location reporting issues could still arise if IP-only geo-localization techniques are deployed. This is because, in order to manipulate the source IP address of the femtocell, there would be no need to physically tamper with it.

C. Attacks on the Core Network

The large scale deployment of comparatively less expensive femtocells is a good alternative for mobile operators as it avoids expensive upgrades to the backbone connections. However, the exposure of the core network's point of entrance to the public Internet has a severe drawback: it renders most Internet-based attacks, such as Denial of Service (DoS, discussed in Section III) or impersonation attacks, feasible against the mobile network operators. Let us focus on the implications of the exposure of public IP addresses of security gateways to the Internet, which are required by a large number of femtocells in order for the whole system to function properly.

DoS attacks (as well as Distributed DoS, DDoS) are a well known occurrence in large companies (such as eBay, Amazon or Yahoo [10]) that host a multitude of web-based services. In order to deal with such attacks in a systematic way, Mirkovic [11] proposes a general classification of attacks and defense mechanisms such that system developers and researchers can better observe and react to the inherently different attacks by exploiting their common traits. If the detection of ongoing DDoS attacks is best performed at the victim site, many researchers ([14], [6], [12], [13]) agree that a distributed solution is better suited against large-scale DDoS attacks than a solution localized only at the final link with the target. The reason is that the suppression mechanisms are most effective near the sources of the attack, as it is possible to filter the malicious traffic from the genuine connections and to avoid that it even reaches and saturates the final link with the target. But the requirement for these solutions to succeed is that different ISPs are able and willing to cooperate to provide protection. Failure to reach an agreement could jeopardize the effectiveness of their solutions.

For a mobile network operator, this means that an effective protection against DDoS attacks needs to encompass not only

the ISP that is providing Internet access but also the neighboring ISPs. Together, they could both limit the femtocell service disruption at the security gateways and ensure the service delivery to the femtocell subscribers. However, cooperation among ISPs is best achieved when all concerned parties have incentives to jointly protect the mobile operators' gateways. We further discuss this issue in the following section.

III. DISCUSSION

In this section, we present solution directions to the two most relevant issues discussed in Section II, i.e., identity and location tracking at the air interface and distributed DDoS defense for the core network.

A solution to the issue of identity and location tracking consists of an adaptive scheme to assign and change identifiers based on context. This would require the mobile devices to dynamically decide when to change identifiers, based on their own observation of the surroundings and thus move away from the network controlled strategy to a user-triggered ID change strategy. For instance, when planning a cellular network, mobile operators have to decide where and how many base stations to install, in order to provide an optimal trade-off between service quality, availability and cost. A densely populated area will usually have many more cells than a rural area with a lower population density. As each cell has a unique cell ID, a mobile device is able to assess whether the current location has a high cell density or not by reading the cell broadcast messages. Moreover, the majority of recent feature-phones and smartphones are equipped with Bluetooth radio technology for low-range ad hoc connectivity. Combined with the cell ID broadcast messages, Bluetooth can be used to define more precisely the number of neighboring devices and to trigger the coordinated temporary ID (or pseudonym) change. Network and device parameters such as neighborhood density, device speed, mobility patterns and neighborhood dynamics affect the effectiveness of the ID change and, as also shown in [8], they should be used when making ID change decisions.

The second challenge for mobile networks with publicly accessible IP interfaces concerns the vulnerability to Internet-based DDoS attacks. Several well-known solutions for thwarting such threats and attacks exist, such as network analysis [13], [12] and client puzzles [16]. But, as the effectiveness of these solutions relies on several participating entities (ISPs), incentives for the cooperation among them need to be studied. One framework that has been extensively applied to security studies for cooperation among self-interested parties is *Game Theory* [9]. A game-theoretic framework will allow us to study the incentives, predict the outcomes and distribute individual profits that are optimal, with respect to a given criteria, and commensurate to the role of each individual ISP in the protection of the security gateways. By using information such as the ISP's national Internet traffic share, femtocell penetration and subscriber base, the model could determine the best strategies for each ISP, which would guarantee the highest profit in any given situation.

IV. CONCLUSION

The control over security and privacy in the next generation of mobile networks, such as LTE, is held solely by the core network. On one hand, this is beneficial as it ensures the trust relationship between subscriber and home network. On the other hand, it impedes dynamic and mobile device controlled actions that could guarantee a better protection.

In this paper, we have reviewed some significant threats to security and privacy in femtocell-enabled mobile networks and have presented solution directions to mitigate two among the most relevant and immediate ones. First, we discussed the issue related to the identity and location tracking with femtocell technology. We have shown that by using contextual information such as node density, device speed and mobility pattern, the mobile device-triggered ID change can reduce the risk of being tracked. Second, we suggested a novel approach towards the protection of the mobile network against Internet-based DDoS attacks. Successful incentive strategies, stimulating cooperation among local ISPs, could ensure an efficient protection and, at the same time, enable a transparent service for legitimate users.

REFERENCES

- [1] 3GPP LTE. <http://www.3gpp.org/LTE>. Visited on 04.05.2010.
- [2] 3GPP TR 33.820 v8.3.0. Technical Specification Group Service and System Aspects; Security of H(e)NB. http://www.3gpp.org/ftp/Specs/archive/33_series/33.820/33820-830.zip. Visited on 04.05.2010.
- [3] 3GPP TS 23.003 v4.9.0. Numbering, addressing and identification. Visited on 05.05.2010.
- [4] 3GPP TS 23.003 v8.6.0. Numbering, addressing and identification. Visited on 05.05.2010.
- [5] A.R. Beresford and F. Stajano. Location privacy in pervasive computing. *IEEE Pervasive Computing*, pages 46–55, 2003.
- [6] S. Chen and Q. Song. Perimeter-based defense against high bandwidth DDoS attacks. *IEEE Transactions on Parallel and Distributed Systems*, 16(6):526–537, 2005.
- [7] Femto Forum. <http://www.femtoforum.org/femto/aboutfemtocells.php>. Visited on 04.05.2010.
- [8] J. Freudiger, R. Shokri, and J.-P. Hubaux. On the optimal placement of mix zones. In *The 9th Privacy Enhancing Technologies Symposium*. Springer, 2009.
- [9] D. Fudenberg and J. Tirole. *Game theory*. MIT Press, 1991.
- [10] L. Garber. Denial-of-service attacks rip the Internet. *Computer*, 33(4):12–17, 2000.
- [11] J. Mirkovic. A taxonomy of DDoS attack and DDoS defense mechanisms. *ACM SIGCOMM Computer Communication Review*, 34(2):39–53, 2004.
- [12] J. Mirkovic, M. Robinson, P. Reiher, and G. Oikonomou. Distributed Defense Against DDOS Attacks. *University of Delaware CIS Department Technical Report CIS-TR-2005, 2*, 2005.
- [13] C. Papadopoulos, R. Lindell, J. Mehringer, A. Hussain, and R. Govindan. Cossack: Coordinated suppression of simultaneous attacks. In *Proceedings of DISCEX III*, pages 2–13. Citeseer, 2003.
- [14] T. Peng, C. Leckie, and K. Ramamohanarao. Survey of network-based defense mechanisms countering the DoS and DDoS problems. *ACM Computing Surveys (CSUR)*, 39(1):3, 2007.
- [15] Vodafone Sure Signal. <http://shop.vodafone.co.uk/shop/mobile-accessories/vodafone-sure-signal>. Visited on 04.05.2010.
- [16] B. Waters, A. Juels, J.A. Halderman, and E.W. Felten. New client puzzle outsourcing techniques for DoS resistance. In *Proceedings of the 11th ACM conference on Computer and communications security*, pages 246–256. ACM, 2004.