Cellpot: A Concept for Next Generation Cellular Network Honeypots

Steffen Liebergeld
Telekom Innovation Laboratories
& TU Berlin
steffen@sec.t-labs.tu-berlin.de

Matthias Lange
Telekom Innovation Laboratories
& TU Berlin
mlange@sec.t-labs.tu-berlin.de

Ravishankar Borgaonkar
Telekom Innovation Laboratories
& TU Berlin
ravii@sec.t-labs.tu-berlin.de

***Abstract*—Smartphones have been shown to be vulnerable. Similarly, cellular networks have been shown to be vulnerable to denial of service attacks through signaling. Attackers can use compromised smartphones to remotely attack the cellular network. Therefore the mobile network operator requires measures to detect and mitigate attacks as they emerge. In the past honeypots proved to be a valuable tool to detect ongoing attacks. Several designs for honeypots on smartphones have been proposed. However, their utility is hampered as they are unlikely to achieve a sufficient coverage.**

In this paper we introduce Cellpot as a novel honeypot concept for threat detection and defence directly inside the cellular network. Cellpot comprises an army of honeypots that are deployed on small cell base stations and is under full control of the operator. We show that Cellpot provides a cost-effective and scalable way for operators to detect and mitigate threats to their core network by reducing signaling overhead. We also present selected applications such as prevention of SMS spam, mobile theft and mobile malware.

I. Introduction

Over the last few years we have seen a sharply increasing number of mobile threats. With their multitude of vulnerabilities, Smartphones became an attractive target for malware. Apart from causing distress and monetary loss for the user, they can also use signaling to attack the cellular network itself. Traynor et al. showed that a relatively small number of devices is sufficient for distributed denial of service (DDoS) attacks against the cellular network core [22]. Further recent jamming attacks on LTE networks [6], [3] and various DoS attacks on 2G [19] and 3G [16], [12] networks indicate that there is a need to monitor cellular networks for signaling DoS attacks to protect the core network.

With their core infrastructure at risk, it is of the mobile network operator's (MNO) interest to be able to detect and mitigate these threats. We think that being able to offer protection and to have the ability to warn users is a valuable market asset for MNOs. Moreover, cellular networks are critical infrastructure that is used for communication and coordination of police, disaster control and medical aid. Ensuring its safety against DoS attacks is a matter of national security. A prerequisite is the ability to detect threats as they emerge, as well as measures to stop attacks before they reach the cellular core network.

Naturally the best place to perform detection is the cellular network perimeter because it is the central switch between mobile devices and the cellular core network. Traditional base stations are very expensive and every software upgrade requires extensive certification and validation. This makes every extension or modification of the network perimeter costly and time consuming, which is prohibitive for threat detection and mitigation methods.

As a mechanism to meet growing coverage and capacity demands the Small Cell forum [17] defined *small cells* as wireless infrastructure that operates in licensed bands. They are deployed at the customer's site and connect to the core network via the customer's landline Internet connection. Small cells are, contrary to traditional base stations, cheap and quick to deploy. A recent Goldman Sachs study forecasts that by 2016 18% of radio access network (RAN) investments will be invested into small cells which by then will handle as much as 80% of all wireless traffic [10]. Each cell handles a small number of mobile devices only.

With their cheap hardware, easy and quick deployment, small cells are a scalable place for threat detection, intelligence collection and mitigation. The key insight is, that small cells act like honeypots, because due to their stronger signal they lure the attacker's mobile device into connecting to the small cell instead of the traditional base station. Thus, small cells that are placed in malls, train stations or airports are likely to catch many attacks.

Honeypots are a well established tool for collecting intelligence about threats in IP networks. For small cells, a new form of honeypot is needed. To that end we introduce *Cellpot*, a novel honeypot concept to detect, collect intelligence and mitigate threats against the cellular network directly on the base station. Our concept largely avoids the costs involved with certification and validation with respect to the radio network. Recent work of Golde et al. [7] shows that the current femtocell hardware can be turned into a monitoring node within the cellular network. We present a practical software design that ensures security of the core network and the honeypot.

The contributions of this paper are:

- We present Cellpot, a novel concept that puts a hon-

SENT '14, 23 February 2014, San Diego, CA, USA
Copyright 2014 Internet Society, ISBN 1-891562-36-3
http://dx.doi.org/10.14722/sent.2014.23005

eypot inside the cellular network that can collect information on mobile threats and implement measures to thwart them. We show how Cellpot can be put to use by describing a set of possible applications.

- We introduce a practical software architecture for small cell hardware that can protect the core network and securely host Cellpot.

The rest of the paper is structured as follows. In Section II we present related work and give an introduction to the femtocell network architecture. In Section III we introduce our threat model. We introduce the Cellpot concept in Section IV, and outline its applications in Section V. In Section VI we introduce a software design that has the potential to significantly increase small cell security. We conclude in Section VII.

II. Related Work and background

Borgaonkar et al. performed a thorough security analysis of a femtocell [4]. They found several security flaws which allow an attacker to compromise the femtocell's firmware. They demonstrate how the location verification techniques can be circumvented and how an attacker can use a femtocell from an unregistered location to e.g. avoid roaming charges [5]. Golde et al. show that currently deployed femtocells can be easily turned into monitoring nodes [7]. A commercially available femtocell can be modified to be used to track phones, intercept communication and even modify and impersonate traffic.

Song et al. [18] proposed a honeypot system to detect infected mobile devices. Their system analyses and monitors the communication behavior of the mobile devices. The honeypot is not designed to detect or analyse attacks against the mobile network.

Liebergeld et al. [14] proposed *nomadic honeypots* to collect threat intelligence directly on smartphones. Their solution allows to contain attacks even in the event of a complete compromise of the smartphone operating system. It requires modifications of the smartphone firmware.

Mulliner et al. [15] introduce a software architecture for smartphones that can mitigate threats against the cellular network even in the event of a full compromise of the smartphone operating system.

Client-side solutions that require custom firmwares are unlikely to find much adoption because of costs for certification needed for admission to cellular networks, which have to be done again for every new type of device.

A. Small Cells in Cellular Networks

Today MNOs are facing growing coverage and capacity demands. One mechanism to meet these demands are *small cells* as defined by the Small Cell forum [17]. According to a survey 98% of the MNOs consider small cells to be essential for the future of their networks.

Small cells are designed to reduce the load on the mobile network by offloading data to a landline broadband connection. Small cells are low powered radio access nodes which operate in a defined spectrum. They cover a range between 10 meters of up to 1 km. Small cells can be categorised into femto-, pico, micro and macro cells and are distinguished by the area they can cover and the number of users they can handle.

In this paper we focus on the femtocell architecture. However, the Cellpot concept can be applied to the other small cell categories as well.

A femtocell is a plug and play, self-provisioning, low-cost small base station that serves existing mobile devices to provide improved indoor coverage with maximum user data rates. Figure 1 depicts architectural components of femtocell networks and shows how femtocells are integrated into existing operator networks. Femtocell devices communicate with the MNO network via the Femtocell Gateway (Femtocell-GW). The femtocell handles radio management functions and the Femtocell-GW acts as an interface to provide core network connectivity.

The femtocell devices are deployed in an environment that is not under the operator's control. They connect to the MNO core network over public Internet. Hence new network components were added to enforce security requirements such as the Security Gateway (SeGW), the Femtocell-GW, and the HNB Management System (HMS).

The SeGW acts as a border gateway of the MNOs network and mutually authenticates femtocells before they establish a secure tunnel over an untrusted broadband connection to prevent eavesdropping or modification of traffic. After successful mutual authentication of femtocell devices, the SeGW forwards all the signaling and user data to the MNO's network. Femtocell devices connect to the Femtocell-GW in order to interact with core network entities over an IPSec Virtual Private Network (VPN). It performs access control and provides various functionality for seamless mobile communication. The HMS is a management system, responsible for the configuration and provisioning of femtocells remotely. Operators are able to remotely control femtocells over the untrusted broadband connection via the IPSec VPN through the SeGW. They use TR-069 [20], the industry preferred protocol used for remote management of femtocells. More detailed information about the femtocell security architecture can be found in [1]. As shown in figure 1, information about core network elements such as SGSN, MSC, VLR, and HSS is out of scope for this paper.

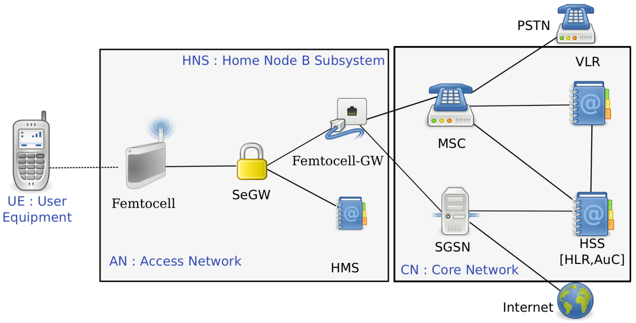

Fig. 1. Overview of the femtocell security architecture. A femtocell communicates through the security gateway with the core network.

III. Threat Model

For this paper we assume an attacker who has physical access to a femto- or small cell base station. The base station uses a landline broadband connection to connect with the mobile operator's core network. This communication channel is encrypted (e.g. using IPSec) and we assume the attacker is not able to wiretap, intercept or modify the communication.

The attackers possess one or more mobile devices which enables them to connect to the base station and create signaling traffic such as changing call forwarding settings or sending SMS.

Attacks on the cellular infrastructure can be categorised by three properties. First, attacks on quality-of-service (QoS), for example by using excessive signaling to hit the network performance. Second, attacks on the availability by e.g. jamming the frequencies. Third, attacks on the security and privacy of users. In this paper we focus on the first and second case exclusively.

For the Cellpot concept, we do not cover attacks on the base station firmware itself, including hardware based attacks (e.g. JTAG) and software based attacks. However, we agree that security of the firmware is of paramount importance, and current firmware does not offer enough protection. Therefore we will address concerns with firmware security in Section VI

IV. Cellpot - A new Concept for Cellular Honeypots

Cellpot is a novel concept for honeypots inside the core cellular network. Cellpot's purpose is threefold: First, it is a key tool for the cellular operator to gather intelligence on mobile threats. Second, it acts as a means to protect the core cellular network, and finally, it protects the mobile user.

As previously discussed, small cells act like honeypots because their stronger signal makes the attacker's mobile device connect to the small cell instead of the base station. To that end, we place Cellpot on small cells, directly at the perimeter of the core network, between the mobile users and the network.

The Cellpot concept consists of three components:

Cellpot A Cellpot comprises the original small cell hardware and a custom firmware. Its primary duties are to monitor the signaling traffic and to do anomaly detection. It can also be equipped with means to counter attacks, such as software to rate limit signaling commands, or filters for expensive premium SMS/MMS. In our concept as many Cellpots as possible are deployed in order to gain a large coverage and thus increase the chances to catch attacks. The custom firmware has to be certified only once for each type of small cell hardware. Because there are much less types of small cells than there are mobile devices, the costs involved with certification are much smaller for small cell hardware than they are for mobile devices.

Peer to peer network Cellpots are interconnected with each other in a P2P network. This network is used to share information between Cellpots and to distribute command and control information. The P2P network elects *master nodes* based on the throughput of their landline Internet connection.

Honeypot Gateway Server The HGS is the central unit of control of all deployed Cellpots. It is used by the MNO to centrally collect threat information from the Cellpots as well as to issue commands for countermeasures.

To gather intelligence, Cellpots interpose between the customer and the core network to detect anomalies in signaling traffic. Cellpots are interconnected with each other in a P2P network. The P2P network has the following duties:

Detect DDoS attacks: Signalling attacks as shown by Traynor et al. [22] are executed using a large mobile botnet, whose bots do not necessarily share the same location. Because these bots connect to the core network with different base stations, an ongoing attack might seem to be legitimate to a single Cellpot. To detect such attacks, Cellpots are interconnected with each other with a P2P network and share their information on signaling traffic. If this distributed knowledge indicates an attack, the master nodes will inform the MNO using the HGS.

Command and Control: Based on the information received from the Cellpot network, the MNO can instruct Cellpots to execute countermeasures, e.g. to rate limit or disable certain commands. These commands are sent directly to the master nodes, which distribute them into the P2P network.

We opted to use a P2P network because it significantly increases the scalability of our Cellpot infrastructure. This architecture reduces load on the centralized HGS. With this solution, the HGS needs to be connected to a small set of master nodes only. Figure 2 illustrates the Cellpot architecture.

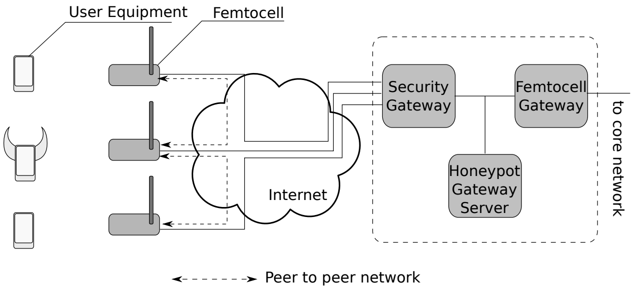

Fig. 2. Cellpot consists of three components: The Cellpot that consists of custom firmware on femtocell hardware, a peer to peer network that connects all Cellpots, and the Honeypot Gateway Server, which is connected to a number of Cellpots that have been elected as master nodes. The Cellpots do anomaly detection on data incoming from mobile devices. The Honeypot Gateway Server is the command and control interface for the whole Cellpot infrastructure.

A. Sensors and Filters for Data Capture

In this section we discuss how Cellpot collects data for the purpose of anomaly detection.

Cellpot uses *sensors* to record events that could be of interest to collect threat intelligence. A sensor wiretaps the traffic from a communication device and records events of interest. In the case of femtocells there are only two communication interfaces: the radio link and the Ethernet interface.

When a sensor detects a suspicious event it can start to increase the rate with which data is collected. This avoids recording lots of uninteresting events while in the attack case missing important events.

In the case of Cellpot sensors are also used for threat mitigation. In that case the sensor is acting as a *filter*. For Cellpot we envision filters for premium SMS, abnormal signaling traffic and a stolen-devices list.

V. Applications of Cellpot

In this section we discuss how Cellpot can be used by the different stakeholders of the mobile security community. The different stakeholders are mobile network operators, device manufacturers, Computer Emergency Response Team (CERT) organizations, mobile antivirus companies, and academic researchers.

Honeypots can be categorised by their goals into four types [23]. Honeypots can be used for *detection* of attacks through e.g. anomaly detection. A *prevention* honeypot is able to dwarf attacks. Honeypots are used for *research* to discover patterns and learn about new attacks. To mitigate attacks the intelligence collected by a honeypot can be used to *react* in a precautionary manner. We believe that Cellpot can be categorised in the above four types by interested stakeholders depending on their security requirements.

Since the Cellpot system is easy for MNOs to integrate into their next generation networks, we discuss new applications. The main advantage for operators to deploy the following applications on the Cellpot is to minimize signaling overhead by detecting and preventing various attacks on the small cell itself before it can reach into their core network.

A. SMS Spam Prevention

SMS spam is any unwanted text message delivered to mobile users via SMS. This spamming issue continues to grow and constitutes 20-30% of all SMS traffic in Asian markets such as China and India due to the introduction of unlimited text plans [8]. As a consequence of SMS spamming attacks, mobile operators are seeing financial loss due to higher infrastructure and operational costs, poor customer experience, and regulation threats. Typically MNOs deploy various additional solutions within their Signalling System No. 7 (SS7) core network to prevent SMS spam attacks. However such type of solutions introduce additional cost and signaling overhead into the core network.

Our Cellpot architecture provides a new way for operators to prevent SMS spam. The prevention techniques can be applied directly on small cells and the Cellpot gateway. Potential advantage of this method is that operators can detect and block spam messages before they can be sent to the Short Message Service Centre (SMSC), minimizing malicious SMS related signaling traffic in the core network. The Cellpot can be equipped with different filter techniques to block malicious premium rate SMS numbers, mobile malware spreading via SMS messages, and phishing.

B. Mobile Theft Prevention

Mobile theft is a rising issue and law enforcement authorities are pushing mobile network operators to tackle it effectively [21]. MNOs deploy Equipment Identity Register (EIR) [9] in their networks and store the identity of stolen or lost phones, typically the International Mobile Equipment Identity (IMEI) number of phones. Operator's EIR are automatically connected with other operators to share IMEI database. However deploying additional EIR system introduces additional cost and signaling. Also the system is not effective since attackers usually change the IMEI of the device illegally.

The Cellpot architecture provides a way to detect stolen mobile phones by uploading IMEI database directly on to the Cellpot gateway and small cells. Further mobile data collected in our honeypot system could assist in finding new ways to detect stolen phones despite their IMEI change. This approach does not add SS7 signaling overhead into the core network.

C. Malware and Phishing Prevention

The Cellpot architecture provides a unique way to monitor mobile data which includes the websites users are trying to connect to. A new anti-phishing framework can be developed using the Cellpot architecture similar to Li and Schmitz work in [13]. The Cellpot can detect known malicious websites serving malware using services such as *MalwareBlacklist.com* and inform the operator.

Discussion: Legal Issues

Our Cellpot architecture provides a platform for monitoring mobile traffic including calls, SMS, and data. Depending on its application, the data collected by Cellpot can contain user's private information such as International Mobile Subscriber Identity (IMSI) number, call history, and even the browsing history etc. A subset of that data is transferred from small cells to the MNO.

The private nature of this data could raise privacy concerns in some countries. However, we want to stress that the Cellpot architecture does not require the MNO to store user's call or SMS data. It is necessary to use certified anonymizing algorithms in the Cellpot. Considering that fact that MNOs already provide lawful interception interfaces to government agencies [2], and that they store user's data according to their local laws, we believe that in practice our Cellpot will not create legal issues for MNOs during deployment.

VI. Making Cellpot Resilient Against Firmware Attacks

A well known problem with femtocells is their system design, which is tailored for minimal costs instead of security. Previous work showed how femtocells can be rooted and how that poses huge risks for both the operators and their customers [7]. This is a concern for our Cellpot as well, especially if it is equipped with active anti-attack measures. Because in the event of a rooted femtocell these measures could be targeted at other subscribers, e.g. to block them from the network or mark their phones as stolen. Even more concerning is that a single malicious Cellpot could poison the whole Cellpot P2P network, which could then no longer be trusted. We believe that future small cell hardware will suffer from the same security weaknesses because they–too–will be tailored for small cost.

An analysis of femtocell vulnerabilities shows that they are caused by a combination of three factors: First, the femtocell firmware is built using outdated versions of open source software. Second, it employs a web-based configuration environment, which requires a webserver to run on the femtocell. Webservers have a bad security track record and present a broad user-accessible attack vector. Third, the components running on the femtocell are insufficiently isolated from one another; If an attacker succeeds in executing custom code (e.g. through a vulnerability in the webserver), she can easily obtain root permissions (*rooting*).

To that end we propose to harden femtocells against rooting by logically partitioning them into two isolated environments. Both environments have separate distinct duties and access distinct pieces of hardware. We call one *firmware environment* (FE), and the second one *infrastructure environment* (IE). This setup is illustrated in Figure 3.

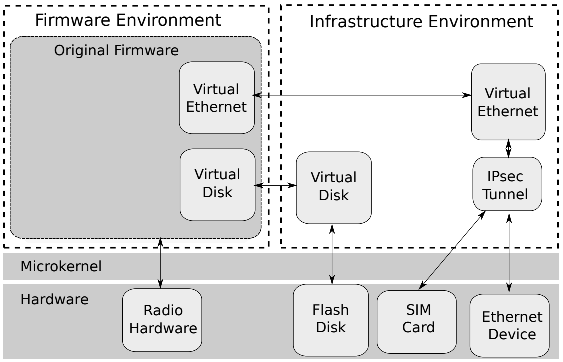

Fig. 3. The software architecture of a single Cellpot consists of two environments; The firmware environment and an infrastructure environment. Only the infrastructure environment is allowed access to cryptographic keys and the Ethernet port. A modern microkernel ensures isolation between the two environments, which are implemented with virtual machines.

The FE has access to the radio hardware and is equipped with a virtual network device. It does not have access to the Ethernet device. We move the entire original firmware into the FE. The firmware takes care of software defined radio and voice encoding. It uses the virtual network device to communicate with the core cellular network. The FE also hosts the configuration interface. It boots and operates from a virtual disk.

The IE in turn has access to the Ethernet port and the flash disk. In particular, its duties are:

- Establishing the link to the core network, using IPSec or similar technology. The key material needed for the link is either hosted directly inside the IE, or in a smart card (e.g. SIM card) that is accessible to the IE exclusively.
- Establishment of a virtual network link to the FE.
- Hosting of the Cellpot infrastructure, including its control link and P2P network.
- Establish a virtual disk to host the FE.
- Reset, update, start and stop the FE.

We require the IE to be booted using secure boot.

By isolating both environments we assure that rooted firmware can be controlled, e.g. by taking the whole femtocell offline or by resetting the firmware environment. Furthermore the attacker cannot access cryptographic keys or tamper with the Cellpot infrastructure. It also solves the problem of costly and time consuming software updates: Certification and validation of the radio stack has to be done only on new firmware versions. Without the costs involved with radio certification and validation, updating and extending the honeypot software can be done frequently.

Contemporary femtocells contain cheap system-on-chip (SoC) components that typically consist of a low power ARM9 core clocked at about 160Mhz and about 64 to 128MB RAM. Currently, these SoCs do not have TrustZone capabilities. Lange et al. showed that virtualization of complex systems like Android is possible on similar embedded systems with the help of a microkernel [11].

Consequently we suggest an implementation using a modern microkernel such as Fiasco.OC as basis, with the partitions being established by virtual machines, similar to the design by Liebergeld et al. [14].

ARM9 and the small amount of memory of current femtocells do not lend themselves to such a system. A system with a Cortex-A9 CPU and about 256MB of RAM enables a performant platform for our software. We argue that the little increase in the total bill of materials is well worth the increase in security.

VII. Conclusion

In this work we introduce Cellpot, a novel mechanism that enables threat intelligence directly inside the cellular network. It consists of customized small cells, that are interconnected with a P2P network, and that are under control of the cellular operator with a secure backchannel. Cellpot has the ability to deploy countermeasures against detected threats, and enables a multitude of applications. Further it provides a platform for mobile network operators to deploy and run additional applications to reduce signaling.

The security of small cell firmware has been shown to be deficient. To ensure Cellpot security, we present a software architecture that is applicable to future small cell hardware and that succeeds in securing the core cellular network even if the firmware has been compromised. Our modular architecture restricts certification and validation to the firmware and allows for frequent updates to the honeypot software.

References

[1] 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.

[2] 3GPP. Universal Mobile Telecommunications System (UMTS); LTE; Lawful interception requirements. Technical report, 3rd Generation Partnership Project, 2011. 3GPP TS 33.106 version 10.0.0 Release 10.

[3] R. Bassil, A. Chehab, I. Elhajj, and A. Kayssi. Signaling oriented denial of service on lte networks. In *Proceedings of the 10th ACM international symposium on Mobility management and wireless access*, MobiWac '12, pages 153–158, New York, NY, USA, 2012. ACM.

[4] R. Borgaonkar, K. Redon, and J. Seifert. Security analysis of a femtocell device. In *Proceedings of the 4th international conference on Security of information and networks*, SIN '11, pages 95–102. ACM, 2011.

[5] R. Borgaonkar, K. Redon, and J.-P. Seifert. Experimental analysis of the femtocell location verification techniques. In *Proceedings of the 15th Nordic conference on Information Security Technology for Applications*, NordSec'10, pages 49–54, Berlin, Heidelberg, 2012. Springer-Verlag.

[6] Cnet-News. LTE networks vulnerable to inexpensive jamming technique. Online http://news.cnet.com/8301-1035_3-57550805-94/lte-networks-vulnerable-to-inexpensive-jamming-technique/, 2012.

[7] N. Golde, K. Redon, and R. Borgaonkar. Weaponizing Femtocells: The Effect of Rogue Devices on Mobile Telecommunications. In *Proceedings of the 19th Annual Network and Distributed System Security Symposium (NDSS)*, February 2012.

[8] GSMA. SMS Spam and Mobile Messaging Attacks Introduction, Trends and Examples. Online http://www.gsma.com/technicalprojects/wp-content/uploads/2012/04/srssmsspamandmobilemessagingattacksthreatsandtrendswp.pdf, Jauary 2011.

[9] GSMA. Handset theft. Online http://www.gsma.com/publicpolicy/handset-theft, 2012.

[10] R. Haraldsvik. 2013 Predictions: Small cell networks and services for a 2020 mobile world. Online http://www.rcrwireless.com/article/20130114/wireless/2013-predictions-mobility2020-small-cell-networks-services-2020-mobile-world/, 2013.

[11] M. Lange, S. Liebergeld, A. Lackorzynski, A. Warg, and M. Peter. L4Android: A Generic Operating System Framework for Secure Smartphones. In *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*, SPSM '11, 2011.

[12] P. P. C. Lee, T. Bu, and T. Woo. On the detection of signaling DoS attacks on 3G/WiMax wireless networks. *Comput. Netw.*, 53(15):2601–2616, Oct. 2009.

[13] S. Li and R. Schmitz. A novel anti-phishing framework based on honeypots. In *Proceedings of 4th Annual APWG eCrime Researchers Summit (eCRS'2009)*. IEEE, 2009.

[14] S. Liebergeld, M. Lange, and C. Mulliner. Nomadic Honeypots: A Novel Concept for Smartphone Honeypots. In *Proceedings of the Workshop on Mobile Security Technologies 2013*, Most 2013, 2013.

[15] C. Mulliner, S. Liebergeld, M. Lange, and J.-P. Seifert. Taming Mr Hayes: Mitigating Signaling Based Attacks on Smartphones. In *Proceedings of the IEEE/IFIP 41st International Conference on Dependable Systems Networks (DSN)*, Boston, MA, June 2012.

[16] 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.

[17] Small-Cell-Forum. 2013 predictions: Small cell networks and services for a 2020 mobile world, February 2013.

[18] Y. Song, X. Zhu, Y. Hong, H. Zhang, and H. Tan. A mobile communication honeypot observing system. In *Proceedings of the fourth international conference on Multimedia Information Networking and Security (MINES)*. IEEE, 2012.

[19] D. Spaar. A Practical DoS Attack against the GSM Network.

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

[21] N. Times. Cellphone Thefts Grow, but the Industry Looks the Other Way. Online http://www.nytimes.com/2013/05/02/technology/cellphone-thefts-grow-but-the-industry-looks-the-other-way.html?pagewanted=all&_r=0, 2013.

[22] 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 *Proceedings of the 16th ACM conference on Computer and communications security*, pages 223–234. ACM, 2009.

[23] F. Zhang, S. Zhou, Z. Qin, and J. Liu. Honeypot: a supplemented active defense system for network security. In *Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003.*, pages 231–235, 2003.