

Security for Smart Mobile Networks: The NEMESYS Approach

Erol Gelenbe*, Gokce Gorbil*, Dimitrios Tzovaras†, Steffen Liebergeld‡,
David Garcia§, Madalina Baltatu¶ and George Lyberopoulos||

*Imperial College London, Dept. of Electrical and Electronic Engineering,
SW7 2AZ London, United Kingdom

Email: {e.gelenbe, g.gorbil}@imperial.ac.uk

†Centre for Research and Technology Hellas, Information Technologies Institute,
57001 Thessaloniki, Greece

‡Technical University of Berlin, 10587 Berlin, Germany

§Hispacec Sistemas S.L., 29590 Campanillas (Malaga), Spain

¶Telecom Italia IT, 20123 Milan, Italy

||COSMOTE - Mobile Telecommunications S.A., 15124 Maroussi, Greece

Abstract—The growing popularity of smart mobile devices such as smartphones and tablets has made them an attractive target for cyber-criminals, resulting in a rapidly growing and evolving mobile threat as attackers experiment with new business models by targeting mobile users. With the emergence of the first large-scale mobile botnets, the core network has also become vulnerable to distributed denial-of-service attacks such as the signaling attack. Furthermore, complementary access methods such as Wi-Fi and femtocells introduce additional vulnerabilities for the mobile users as well as the core network. In this paper, we present the NEMESYS approach to smart mobile network security, to develop novel security technologies for seamless service provisioning in the smart mobile ecosystem, and to improve mobile network security through a better understanding of the threat landscape.

Index Terms—Mobile network security, femtocell security, anomaly detection, visual analytics, virtual mobile client honeypot.

I. INTRODUCTION

Smartphones, tablets, and similar smart mobile devices are taking over the mobile device market, and this trend is not expected to slow down in the near future. Table I gives the number of mobile devices shipped worldwide in 2012 based on data from Canalys [1]. The data shows that smartphones and tablets represented 42% of all mobile devices shipped in 2012, and their combined market share is expected to grow to 66% by 2016. The significance of these numbers is highlighted by the fact that among all consumer devices, only the television has had such a fast market penetration rate in the USA [2]. Furthermore, while smartphones represented only 18% of total global mobile phones in use in 2012, they were responsible for 92% of total global mobile phone traffic [3].

Smart devices increasingly store and provide access to a range of personal, corporate, financial and security-related data. While the availability and ease of access to such data via different types of network connections (e.g. Wi-Fi, cellular), the ability to download, install and use mobile applications, and the practicality of using networked services while on the

TABLE I
THE NUMBER OF MOBILE DEVICES SHIPPED WORLDWIDE IN 2012 AND FORECAST FOR 2016, IN MILLIONS OF UNITS, ACCORDING TO CANALYS (FEB. 2013) [1].

Device type	2012 shipments	2016 shipments	2012–2016 CAGR
Basic phone	122.0	58.0	−17.0%
Feature phone	770.8	660.9	−3.8%
Smartphone	694.8	1,342.5	17.9%
Tablet	114.6	383.5	35.3%
Notebook	215.7	169.1	−5.9%
Netbook	18.3	0.3	−64.2%
Total	1,936.2	2,614.2	7.8%

go make the smart mobile device an inseparable companion to the modern man, they also provide the perfect breeding ground for malicious software. Cyber-criminals have not had continuous access to such varied sources of personal and financial data before the advent of the smartphone. Increasing use of mobile payments presents a new area to exploit, and attackers have already devised covert ways to make direct financial gain from the mobile users, e.g. via premium calls and SMS [4]. Furthermore, the use of multiple communication technologies in smart devices allows attackers to cross service boundaries. For example, an attack carried out over Wi-Fi would allow the attacker to launch attacks over the mobile phone network. In addition to exposing the mobile user to heterogeneous attack vectors, the increasing use of complementary access to the mobile core network, via Wi-Fi and femtocells, introduces new vulnerabilities to the core network [5]. The amount of data carried over complementary access should not be underestimated; according to Cisco [3], 429 petabytes per month of global mobile data was offloaded onto the fixed network through Wi-Fi or femtocell radio access, which represents 33% of total mobile traffic in 2012. Cisco also estimates that mobile data offload will reach 9.6 exabytes per month by 2017, which will be 46% of total mobile traffic.

Smart mobile devices are also increasingly at the center

of security systems for managing small or large emergencies in built environments, or during sports or entertainment events [6,7], and they are also used increasingly for search of difficult-to-get sensitive information [8]–[10]. Thus such technologies will necessarily be targeted and may be breached in conjunction with other physical or cyber attacks, as a means of disrupting safety and confidentiality of individuals and emergency responders [11]–[13].

In order to address the growing mobile threat, there is an urgent need to detect, analyze and understand the new vulnerabilities and threats in the smart mobile ecosystem, which are a result of the evolution of mobile networks and smart devices, the changing way users interact with technology, the popularity of smart devices, and the heterogeneity of the wireless interfaces, supported platforms and offered services. In order to advance in the fast moving field of cyber-security and to counter existing and potential mobile threats, we need to be proactive and work on predicting threats and vulnerabilities to build our defenses before threats materialize. To this purpose, the EU FP7 NEMESYS project¹ will develop a novel security framework to gather and analyze information about the nature of cyber-attacks targeting mobile devices and the mobile core network, as well as identify and predict abnormal behaviour observed on smart mobile devices and the mobile network so that appropriate countermeasures can be taken.

II. THE CURRENT MOBILE THREAT LANDSCAPE

Smart devices are open to both traditional and mobile-specific threats due to the multiple roles smart mobile devices play and the heterogeneity of mobile communication technologies and networked services [14]. Among the traditional threats that smart mobile devices face, we include physical attacks that require physical access to the device, device-independent attacks such as eavesdropping on the wireless medium or man-in-the-middle attacks, e-mail-based spam and phishing, and IP-based attacks. Current IP-based attacks encountered on mobile devices [15] have been found to be largely similar to those on non-mobile devices [16,17], but we are more interested in the traits of attacks that are tailored specifically for mobile devices. With the growing popularity of smart devices, mobile-specific threats have evolved from SMS/MMS-based denial-of-service (DoS) attacks [18,19] to more sophisticated attacks that usually come in the form of malware and target both the core network and the mobile users. The ability of smart devices to install and run applications not only from official markets but also from unknown sources exposes them to malware [4,20], and while the mobile malware threat is not new [21], it is clearly evolving and growing as attackers experiment with new business models by targeting mobile users [22,23]. We next provide a taxonomy of mobile malware based on behavioral classification, and present an overview of malware detection techniques.

¹<http://www.nemesys-project.eu/nemesys/>

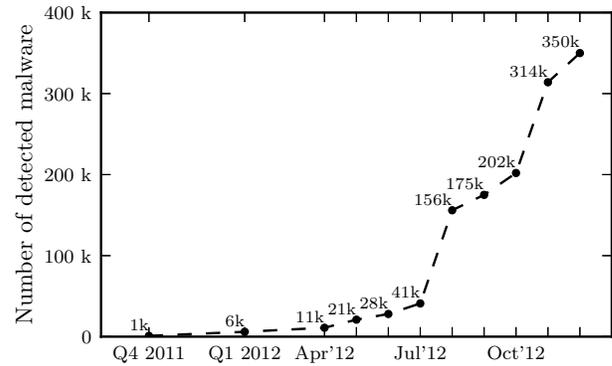


Fig. 1. The number of detected Android malware in 2012 [25]. The data shows a rapid increase in malware, especially in Q3-Q4 2012, which was due to aggressive adware.

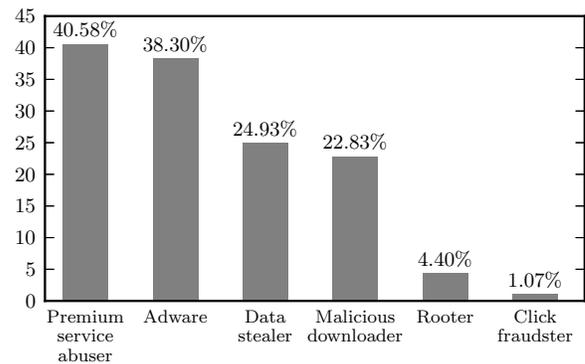


Fig. 2. The distribution of malware types for the top ten Android malware families in 2012 (TrendLabs [25]).

A. Mobile Malware

Android has been the most targeted mobile platform in 2012, with almost 99% of all encountered mobile malware being designed for Android [24]. The number of malicious Android applications detected by Kaspersky Lab in 2012 was more than 35,000, which reflects a six-fold increase from 2011 [23]. Figure 1 shows the rapid growth of Android malware in 2012 based on data from TrendLabs [25], which shows the significance of the growing mobile malware threat. 2012 has also seen the emergence of the first mobile botnets [24]. A botnet is a collection of Internet-connected devices acting together to perform tasks, often under the control of a command and control server. In wireline networks, malicious botnets are used to generate various forms of spam, phishing, and distributed denial-of-service (DDoS) attacks. Mobile botnets extend such capability to cellular networks, give cyber-criminals the advantages of control and adaptability, and pose a significant threat to the mobile core network as they could be used to launch debilitating signaling-based DoS attacks [26] and [27]–[29].

Mobile malware uses various infection vectors in order to gain access to the device; the top two main categories of attacks based on the vulnerabilities they use are:

- *Exploiting* hardware or software vulnerabilities of devices to completely bypass the user and install malware. Some

of the exploits used to attack smart devices are near field communication (NFC) technology, third-party kernel drivers, Android firmware vulnerabilities, and mobile web browsers. For example, some malicious websites use mobile browser exploits to install malware on the device without any user interaction other than visiting the site. Android firmware and third-party driver exploits have been used by malware to elevate their privileges and thus gain root access to the device, allowing them to practically do anything they want without the user's knowledge [30].

- *Social engineering* is by far the most common method used to infect smart mobile devices, where users are “tricked” into installing the malware themselves. Social engineering includes all techniques that exploit the human user, such as phishing, application repackaging, etc., in order to infect the device. Social engineering is popular since it does not require any technical investment by the attacker, i.e. the identification of a new exploit and the development of a delivery system that uses it. Upcoming malware will continue to employ social engineering in new ways; for example, we have already witnessed the first malicious QR codes, which need to be scanned by the user for their activation.

Independently of how it infects the device, once the malware is installed, it performs one or more malicious activities, which are classified in Table II according to their behavior. Figure 2 shows the distribution of malware types for the top ten Android malware families in 2012, based on data from TrendLabs [25]. The data shows that some malware families exhibit multiple malicious activities (e.g. both premium service abuse and data stealing), and that premium service abuse has been the favorite malware type, most probably because it is simple to create and allows a direct source of revenue for the cyber-criminal. It is closely followed by adware, which generates indirect profit through advertisement fraud.

B. Malware Detection Techniques

The traditional approach to malware detection is *signature-based*, where signatures for identified malware are extracted and used to detect new infections of the same malware on other devices. While this can be very effective for controlling an outbreak, it cannot defend against malware unless samples have already been obtained and analyzed. Therefore, new and unknown malware cannot be detected via signature-based approaches. In order to detect previously unknown malware, *behavioral methods* are useful in which the activities of an application are analyzed via either static or dynamic analysis. *Static analysis* provides a quick and efficient way to detect malware without executing them, but they are ultimately limited in their effectiveness unless the source code for the application is available. Unlike static analysis, *dynamic analysis methods* execute the application code in an isolated environment, for example a virtual machine or a sandbox, so its behavior can be directly observed. Dynamic analysis techniques include function call monitoring, function parameter

TABLE II
MALWARE BEHAVIORAL CLASSIFICATION.

Activity: Description
Stealing user information: Steals user information and credentials. The most commonly targeted data are the contact list, IMEI and IMSI numbers, API authentication keys, banking credentials, user's location, network operator, phone ID and model, phone number, and text messages.
Monitoring: Tracks user's location, records conversations, takes photos. Spyware is considered to exhibit this type of behavior.
Adware: Presents unwanted advertisements to the user. Most mobile adware have evolved to incorporate other types of behavior, such as monitoring user activity, especially browsing behavior, and stealing user information. Malicious advertisement networks are increasingly finding their way into legitimate applications and being used as infection vectors.
Premium service abuse: Sends premium SMS/MMS, makes premium calls, subscribes the user to premium services without the user's knowledge. Cyber-criminals often make direct financial gain from such premium service abuse.
Click fraud: Generates “clicks” on ads shown on websites and applications, generating indirect financial gain to the cyber-criminal through payment from the advertisement networks.
Search engine optimization: Manipulates the search results shown on the mobile browser and other applications to improve website rankings in search engine results.
SMS and e-mail spam: Sends spam SMS and e-mail either to the user's contacts or to a specified list of people. Could be used for phishing attacks.
Malicious downloading: Downloads malicious content onto the device. Mainly used to evade detection by malware detectors and the user.
Botclient: Turns the device into a botclient that receives commands from a remote command and control server. Once part of a mobile botnet, the device can be used to launch a variety of attacks, ranging from spam to DDoS attacks on the network.
Rooting: Roots the device to allow execution of otherwise restricted commands and programs. Malware that has root access potentially has full control of the device.
Ransom: Locks the device and demands a ransom to be paid in order to unlock the device.
Destruction: Causes physical damage by deleting important files or personal information.
Denial-of-service: Launches a denial-of-service attack either on the mobile device itself or on the core network. The mobile device may be attacked by repeatedly switching the device off or depleting the battery.

analysis, information flow tracking, and instruction tracing. An overview of mobile malware detection methods is presented in [31], and a more comprehensive survey is given by [32]. In the rest of this section, we will only consider behavior-based detection methods.

Based on where the detection is performed, we can classify malware detection methods into three categories. *Client-side detectors* reside in the mobile device, but are constrained by its limited physical resources, especially battery. *Network-side detection* methods analyze mobile network traffic from many users and offer a complementary means for detecting attacks targeting mobile users. They can be used in conjunction with client-side methods to improve detection rates, and provide a broad view of malicious activities within a carrier's network, enabling detection of anomalous behavior that would not be

visible on a per user basis. However, network-based methods are limited in that they can only monitor and analyze mobile traffic that goes through the cellular network, and therefore may not be suitable for certain malware types, such as malware that exclusively uses Wi-Fi for communication. *Cloud-based detection* offers a trade-off between network-level analysis and on-device security by offloading intensive security analysis and computations to the cloud while monitoring internal mobile device events as well as different types of wireless communications from many users.

III. THE NEMESYS APPROACH

Our initial research has identified the following open issues with respect to the general problem of cyber threats against smart mobile devices:

- *Missing infrastructure for collecting attack traces.* Without an infrastructure to collect attack traces against mobile devices, we will not be able to detect, analyze and understand the evolving attack strategies employed by cyber-criminals. These are crucial in order to develop effective mitigation strategies and to provide seamless services in the smart mobile ecosystem.

- *Virtualization.* By leveraging advances in mobile virtualization technology, we can protect mobile users from the consequences of malware by appropriately restricting access to device functionality. Virtualization would also allow an easy way to reset mobile devices to a state before infection.

- *Mobile honeypot development.* Honeypots are successfully used in wired networks in order to study the strategies of attackers and to protect production systems from attacks. However, the development of mobile honeypots is still at an early stage. For example, the mobile honeypot presented in [33] can connect to the Internet only over Wi-Fi or a wired connection. Although the mobile honeypot presented in [15] can connect to a UMTS network via a USB dongle, the honeypot uses desktop computers to emulate mobile devices. We aim to address the deficiencies of these early efforts by developing a high-interaction mobile honeypot using real mobile devices.

- *New potential for exploiting security vulnerabilities through mobile botnets.* While botnets are a well-known phenomenon in the wired Internet, we have just witnessed the first mobile botnets in 2012. Mobile botnets pose interesting questions as to their capabilities and uses since smart mobile devices possess many abilities not present on a desktop computer. Such mobile botnets could be used to attack mobile users (e.g. SMS spam) and the core network (e.g. DDoS attack); the ability of a large number of mobile devices to effectively attack the core network has been demonstrated in recent cases of legitimate but poorly-designed mobile applications. We need to explore the new threats posed by the emergence of mobile botnets in more detail.

- *Adaptability of cyber-criminals and rapidly changing cyber-crime tactics.* Cyber-criminals have become adept at modifying their strategies and tactics as methods are developed to counter their activities. Thus, security solutions should rely less on signatures and instead adopt other forms of detection.

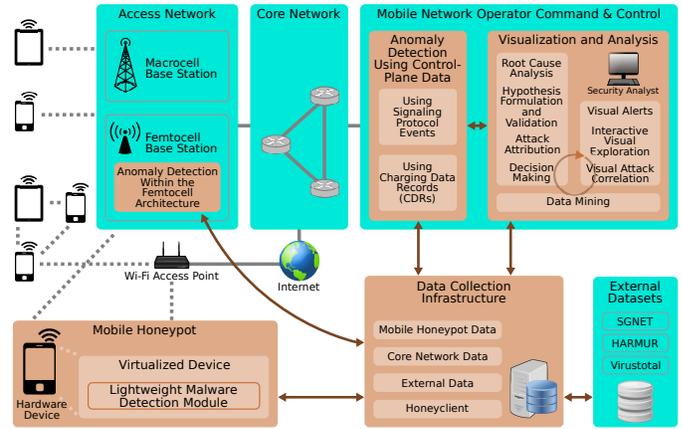


Fig. 3. The NEMESYS architecture

- *New types of attacks that cross service, platform and network boundaries.* Identification of anomalous behavior within a large set of heterogeneous data is difficult and time-consuming, particularly across layers. Statistical analysis is further challenged by rare anomalous events in massive amounts of data.

- *Attack attribution and understanding of the cyber-criminals' modus operandi.* The selection of the best mitigation strategy requires understanding of new phenomena and recognizing changes in how the malicious actors operate. This requires that attacks are analyzed in a detailed way, in order to "attribute" responsibility to an exact attacker or to protect the true targets.

In the EU FP7 NEMESYS project, we are developing a data collection, visualization and analysis infrastructure (Fig. 3) in order to address these open issues. The core of this architecture consists of a data collection infrastructure that incorporates high-interaction virtualized mobile honeypots and honeyclients in order to gather data regarding mobile attacks. The collected data is enriched by the data collection infrastructure through interaction with external sources and made available to anomaly detection, visualization and analysis modules running on the mobile network operator's site. The purpose of the anomaly detection mechanisms is to detect deviations from normal behaviour of mobile users and the core network in real-time. These mechanisms will utilize charging data records (CDRs) for the users and control-plane protocol data, combined with enriched mobile attack traces made available by the data collection infrastructure. In addition to monitoring abnormal behaviour of users connected to the core network through the radio access network, the architecture contains a module that performs anomaly detection within the femtocell complementary access system.

Enriched attack traces and normal behaviour statistics from the data collection infrastructure and the output of the anomaly detection module are fed into the visualization and analysis module. The visualization and analysis module will aid in the detection of existing and emerging threats in the mobile ecosystem through attack attribution, root cause identification,

and correlation of observed mobile attacks with known attack patterns. It will present large sets of data related to the observed attacks from heterogeneous sources and facilitate the role of the security analyst in reasoning, hypothesis testing and decision making.

A. Virtualized Mobile Client Honeypot

Honeybots are networked computer system elements that are designed to be attacked and compromised so we can learn about the methods employed by the attackers [34]. Traditional honeybots are servers that passively wait to be attacked, whereas client honeybots are security devices that actively search for malware, compromised websites and other forms of attacks. High-interaction client honeybots are fully functional, realistic client systems and they generally do not impose any limitations on the attacker other than those required for containing the attack within the compromised system. Despite their complexity and maintenance difficulty, high-interaction client honeybots are effective at detecting unknown attacks and they are harder to detect by the attacker [34]. They also enable in-depth analysis of the attacks during and after the attack has taken place.

As part of NEMESYS, we are developing a high-interaction virtualized client honeybot for the Android mobile platform in order to attract and collect mobile attack traces. We have chosen Android considering its popularity among mobile users and the extremely high ratio of malware targeting Android. Our virtualization technology logically partitions the physical device into two virtual machines (VMs): the *honeybot VM* and the *infrastructure VM*. The honeybot VM will host the largely unmodified mobile device operating system, and it will not have direct access to the device's communication hardware. The infrastructure VM will mediate all access to the communication hardware, and employ sensors to wiretap any communication and detect suspicious behaviour. It will also provide the event monitoring, logging and filesystem snapshot facilities, as well as transmit threat information to the NEMESYS data collection infrastructure. It will host a lightweight malware detection module in order to identify malicious applications running on the honeybot VM. For this purpose, both signature-based and behaviour-based approaches will be considered. In order to improve the efficiency of malware detection, we will identify and prioritize the most important attributes in the system state space to monitor. Our virtualization technology will ensure that an attack is confined within the compromised device and that it will not put other devices in the network at risk. Furthermore, through this approach, we will be able to stop malware from abusing premium services and from subscribing the user to services without her knowledge. Thus, the user will be spared from any financial distress that may arise as a result of using the mobile honeybot. The virtualization solution also enables taking full snapshots of the honeybot VM filesystem for further forensic analysis of an attack, as well as improving honeybot maintenance since a compromised honeybot could be restored more quickly.

Our initial research has shown that the infection vector of most mobile malware is social engineering, where users are "tricked" into installing the malware themselves. This observation has led us to the conclusion that the user should not be ignored in the construction of an effective mobile honeybot. To this end, we introduce the *nomadic honeybot* concept, which utilizes real smartphone hardware with the virtualization solution that will be developed within NEMESYS [35]. We plan to deploy nomadic honeybots by handing them out to a chosen group of volunteers, who will use the honeybot as their primary mobile device.

B. Data Collection Infrastructure

The data collection infrastructure will gather and store mobile attack traces that will be provided by the virtualized mobile client honeybot and the honeyclient, and combine them with data from the mobile core network and external sources for enrichment, correlation analysis, and visualization. As an initial step in the design of this infrastructure, we are identifying available external data sources relating to wireline network attacks which will enable correlation of data from multiple heterogeneous sources. Examples of such data sources are the SGNET [36], HARMUR [37], and VirusTotal databases. A source aggregator is being designed and developed to harvest and consolidate data from these sources and the NEMESYS mobile honeybot in a scalable database. Scalable design of the database is important in order to be able to efficiently store and handle large heterogeneous data sets. Once data from multiple sources have been consolidated, they will be enriched by analyzing the data itself or accessing external sources. For example, TCP/IP stack fingerprinting in order to identify the remote machine's operating system, and clustering of the traces are passive methods of data enrichment. On the other hand, DNS reverse name lookup, route tracing, autonomous system identification, and geo-localization are methods to improve characterization of remote servers but these functions may require access to external sources, possibly in real time. As a final step, the data collection infrastructure will help in the definition of the appropriate inputs representing normal and malicious network activity, which will then be used as the fundamental representation of information in the visualization and analysis module.

The *honeyclient* [38] being developed as part of the data collection infrastructure is similar in concept to the virtualized mobile honeybot, but instead of using real hardware and being driven by real users, the honeyclient uses an Android emulator driven by artificially generated user input to automate interaction with web sites, application markets and applications in order to collect mobile attack traces. The honeyclient consists of a crawler, client, and detector components. The crawler discovers web sites, application markets and applications of interest and generates a list of web pages to visit and applications to download. The client runs the Android emulator (e.g. on a desktop computer) and processes the list generated by the crawler, visiting the web sites using a mobile browser and downloading, installing and executing applications. The

behavior of the applications, e.g. function calls, and changes to the system as a result of executing the applications are recorded by the client, which are used by the malware detector to identify malware. The honeyclient provides data relating to identified malware and malicious web sites to the data collection infrastructure.

C. Anomaly Detection Using Control Plane and Billing Data

The anomaly detection module that operates at the mobile network operator's site is used for the identification and prediction of abnormal behavior observed on smart mobile devices and the mobile network. In addition to user-oriented attacks, mobile networks are vulnerable to a novel DoS attack called the signaling attack [26]. Signaling attacks seek to overload the control plane of the mobile network using low-rate, low-volume attack traffic, based on the structure and characteristics of mobile networks. Unlike conventional DoS attacks that focus on the data plane, the signaling attack creates havoc in the control plane of a mobile network by repeatedly triggering radio channel allocations and revocations. In order to identify such DoS attacks against the mobile network and attacks against the mobile users in real time, we will use signaling data from control-plane protocols and sanitized (anonymized) CDRs from mobile users, respectively. For this purpose, we will use normal user behavior statistics, as well as synthetic "typical" user playbacks, to create traces of signaling events and billing data so as to characterize and extract their principal statistics such as frequencies, correlations, times between events, and possible temporal tendencies over short (milliseconds to seconds) and long (hours to days) intervals. We will then employ Bayesian techniques such as maximum likelihood detection, neuronal techniques based on learning, and a combination of these two in order to design and develop robust and accurate change detection algorithms to detect the presence of an attack, and classification algorithms to identify the type of attack when it is detected with high confidence.

Novel femtocell architectures provide a specific opportunity for user-end observation of network usage, while they also have specifics for attacks within the femtocells [39]. To address attacks specific to femtocells, we will conduct a survey and evaluation of how users may be monitored and attacks detected within a femtocell, and how these are linked to overall mobile network events.

A number of novel ideas are also being investigated [40] such as modeling the signaling and billing network as a queueing network [41,42] to capture the main events that involve hundreds of thousands of mobile calls and interactions, while only a few may be subject to an intrusion or attack at any given time. Detection of anomalies is studied using learning with neural networks [43,44] that provide fast low-order polynomial detection complexity required for massive real-time data, and the need to detect and respond to threats in real-time. Such techniques can also benefit from distributed task decomposition and execution for greater efficiency [45], and realistic simulation of UMTS and LTE networks using the OMNeT++ simulation framework.

D. Root Cause Analysis, Correlation and Visualization

The role of the visualization and analysis module is to process the data obtained from the data collection infrastructure and the anomaly detection module in order to identify and reveal correlations between network events, and to provide a visual analytics framework for the security analyst to perform hypothesis formulation and testing. The data provided to this module represents a large and heterogeneous data set that needs to be presented in a meaningful way to the operator without overwhelming her or restricting available views and actions on the data. In addition to mere representation of data, the visualization and analysis module aims to provide visual analytics tools to the operator. This task is compounded by different uses of visualization by the operator: (i) real-time monitoring of the status of users and the mobile network, and (ii) exploratory data analysis. For real-time monitoring, the security status of a large set of mobile users and more importantly the mobile network need to be presented to the operator. This includes providing early alerts for abnormal behaviour, DoS attacks, malware spreading among the users of the mobile network, etc. The analytics module must also provide visual analytics tools so the analyst can perform attack attribution and correlation analysis with the help of algorithms running in the background. We will therefore focus on enabling a real-time analysis framework by means of incremental analysis and visualization methods [46], such as multi-level hierarchical screen visualizations that update smoothly rather than showing abrupt changes.

E. Future Work

The mobile threat grows with the increasing marketshare of smartphones and tablets, data due to smart devices, and the volume increase of malware that has been detected on mobile devices. Therefore the EU FP Project NEMESYS arrives in a timely manner to provide insight and effective methodologies for next generation network security for mobile wireless networks. In order to evaluate and validate the technologies that are being developed and to demonstrate their impact to interested parties, NEMESYS will construct a virtual testing environment based on guidelines provided by our industrial partners that is as close to a real mobile network as possible within feasibility limitations. The different modules being developed by various partners will be integrated in the virtual testing environment, and validation tests will be conducted based on realistic use-cases.

ACKNOWLEDGMENTS

The authors acknowledge the support provided by EU FP7 collaborative research project NEMESYS, Grant Agreement no. 317888, FP7-ICT-2011.1.4 Trustworthy ICT.

REFERENCES

- [1] (2013, Feb.) Mobile device market to reach 2.6 billion units by 2016. Canalsys. [Online]. Available: <http://www.canalsys.com/newsroom/mobile-device-market-reach-26-billion-units-2016>

- [2] M. DeGusta, "Are smart phones spreading faster than any technology in human history?" *Business Impact*, vol. Mobile Computing in Question, May 2012. [Online]. Available: <http://www.technologyreview.com/businessreport/mobile-computing-in-question/>
- [3] (2013, Feb.) Cisco visual networking index: Global mobile data traffic forecast update, 2012–2017. White Paper. [Online]. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf
- [4] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner, "A survey of mobile malware in the wild," in *Proc. 1st ACM W'shop on Security and Privacy in Smartphones and Mobile Devices*, 2011, pp. 3–14.
- [5] N. Golde, K. Redon, and R. Borgaonkar, "Weaponizing femtocells: The effect of rogue devices on mobile telecommunication," in *Proc. 19th Annual Network and Distributed System Security Symposium (NDSS'12)*, Feb. 2012, pp. 1–16.
- [6] E. Gelenbe, G. Gorbil, and F.-J. Wu, "Emergency cyber-physical-human systems," in *Proc. 21st Inter. Conf. on Computer Comms. and Networks (ICCCN'12)*. IEEE Computer Society, August 2012, pp. 1–7.
- [7] E. Gelenbe and F.-J. Wu, "Large scale simulation for human evacuation and rescue," *Computers & Mathematics with Applications*, vol. 64, no. 2, pp. 3869–3880, 2012.
- [8] E. Gelenbe and Y. Cao, "Autonomous search for mines," *European Journal of Operational Research*, vol. 108, no. 2, pp. 319–333, 1998.
- [9] E. Gelenbe, "Search in unknown random environments," *Physical Review E*, vol. 82, no. 6, p. 061112, Dec. 2010.
- [10] O. H. Abdelrahman and E. Gelenbe, "Time and energy in team-based search," *Physical Review E*, vol. 87, no. 3, p. 032125, Mar. 2013.
- [11] G. Gorbil and E. Gelenbe, "Opportunistic communications for emergency support systems," *Procedia Computer Science*, vol. 5, pp. 39–47, 2011.
- [12] G. Gorbil, A. Filippopolitis, and E. Gelenbe, "Intelligent navigation systems for building evacuation," in *Computer and Information Sciences II*, E. Gelenbe, R. Lent, and G. Sakellari, Eds. Springer London, 2012, pp. 339–345.
- [13] G. Gorbil and E. Gelenbe, "Disruption tolerant communications for large scale emergency evacuation," in *Proc. 2013 IEEE Inter. Conf. on Pervasive Computing and Communications Workshops*. IEEE Computer Society, Mar. 2013, pp. 540–546.
- [14] M. Becher, F. C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, and C. Wolf, "Mobile security catching up? Revealing the nuts and bolts of the security of mobile devices," in *Proc. 2011 IEEE Symp. on Security and Privacy*, May 2011, pp. 96–111.
- [15] M. Wahlisch, A. Vorbach, C. Keil, J. Schonfelder, T. C. Schmidt, and J. H. Schiller, "Design, implementation, and operation of a mobile honeypot," *arXiv Computing Research Repository*, vol. abs/1301.7257, Jan. 2013.
- [16] E. Gelenbe and G. Loukas, "A self-aware approach to denial of service defence," *Computer Networks*, vol. 51, no. 5, pp. 1299–1314, Apr. 2007.
- [17] E. Gelenbe, "Steps toward self-aware networks," *Communications of the ACM*, vol. 52, no. 7, pp. 66–75, Jul. 2009.
- [18] P. Traynor, W. Enck, P. McDaniel, and T. L. Porta, "Mitigating attacks on open functionality in SMS-capable cellular networks," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 40–53, Feb. 2009.
- [19] C. Mulliner, N. Golde, and J.-P. Seifert, "SMS of death: From analyzing to attacking mobile phones on a large scale," in *Proc. 20th USENIX Conf. on Security (SEC'11)*, Aug. 2011, pp. 363–378.
- [20] Y. Zhou and X. Jiang, "Dissecting Android malware: Characterization and evolution," in *Proc. 2012 IEEE Symp. on Security and Privacy*, May 2012, pp. 95–109.
- [21] D. Dagon, T. Martin, and T. Starner, "Mobile phones as computing devices: The viruses are coming!" *IEEE Pervasive Computing*, vol. 3, no. 4, pp. 11–15, Oct.-Dec. 2004.
- [22] (2012) State of mobile security 2012. Lookout Mobile Security. [Online]. Available: https://www.lookout.com/_downloads/lookout-state-of-mobile-security-2012.pdf
- [23] C. Raiu and D. Emm. (2012, Dec.) Kaspersky security bulletin 2012: Malware evolution. Kaspersky Lab. [Online]. Available: http://www.securelist.com/en/analysis/204792254/Kaspersky_Security_Bulletin_2012_Malware_Evolution
- [24] D. Maslennikov and Y. Namestnikov. (2012, Dec.) Kaspersky security bulletin 2012: The overall statistics for 2012. Kaspersky Lab. [Online]. Available: http://www.securelist.com/en/analysis/204792255/Kaspersky_Security_Bulletin_2012_The_overall_statistics_for_2012
- [25] (2013, Jan.) TrendLabs 2012 mobile threat and security roundup: Repeating history. Trend Micro. [Online]. Available: <http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-repeating-history.pdf>
- [26] P. P. Lee, T. Bu, and T. Woo, "On the detection of signalling DoS attacks on 3G/WiMax wireless networks," *Computer Networks*, vol. 53, no. 15, pp. 2601–2616, Oct. 2009.
- [27] P. Traynor, M. Lin, M. Ongtang, V. Rao, T. Jaeger, P. McDaniel, and T. L. Porta, "On cellular botnets: Measuring the impact of malicious devices on a cellular network core," in *Proc. 16th ACM Conf. on Computer and Comms. Security (CCS'09)*, Nov. 2009, pp. 223–234.
- [28] C. Mulliner and J.-P. Seifert, "Rise of the iBots: Owning a telco network," in *Proc. 5th Inter. Conf. on Malicious and Unwanted Software (MALWARE'10)*, Oct. 2010, pp. 71–80.
- [29] C. Mulliner, S. Liebergeld, M. Lange, and J.-P. Seifert, "Taming Mr Hayes: Mitigating signaling based attacks on smartphones," in *Proc. 42nd Annual IEEE/IFIP Inter. Conf. on Dependable Systems and Networks (DSN'12)*, Jun. 2012, pp. 1–12.
- [30] S. Liebergeld and M. Lange, "Android security, pitfalls and lessons learned," in *Information Sciences and Systems 2013 - Proc. 28th Int. Symp. on Computer and Information Sciences (ISCIS'13)*, ser. LNEE, E. Gelenbe and R. Lent, Eds. Springer, Oct. 2013, pp. 409–417.
- [31] M. Chandramohan and H. B. K. Tan, "Detection of mobile malware in the wild," *IEEE Computer*, vol. 45, no. 9, pp. 65–71, Sep. 2012.
- [32] M. Egele, T. Scholte, E. Kirda, and C. Kruegel, "A survey on automated dynamic malware-analysis techniques and tools," *ACM Computing Surveys*, vol. 44, no. 2, pp. 6:1–6:2, Feb. 2012.
- [33] Y. Song, X. Zhu, Y. Hong, H. Zhang, and H. Tan, "A mobile communication honeypot observing system," in *Proc. 4th Inter. Conf. on Multimedia Information Networking and Security*, Nov. 2012, pp. 861–865.
- [34] N. Provos and T. Holz, *Virtual Honeypots: From Botnet Tracking to Intrusion Detection*. Addison Wesley, Jul. 2007.
- [35] S. Liebergeld, M. Lange, and C. Mulliner, "Nomadic honeypots: A novel concept for smartphone honeypots," in *Proc. W'shop on Mobile Security Technologies (MoST'13)*, together with 34th IEEE Symp. on Security and Privacy, May 2013.
- [36] C. Leita and M. Dacier, "SGNET: A worldwide deployable framework to support the analysis of malware threat models," in *Proc. 7th European Dependable Computing Conference (EDCC'08)*, May 2008, pp. 99–109.
- [37] C. Leita and M. Cova, "HARMUR: Storing and analyzing historic data on malicious domains," in *Proc. 1st W'shop on Building Analysis Datasets and Gathering Experience Returns for Security (BADGERS'11)*, Apr. 2011, pp. 46–53.
- [38] L. Delosieres and D. Garcia, "Infrastructure for detecting Android malware," in *Information Sciences and Systems 2013 - Proc. 28th Int. Symp. on Computer and Information Sciences (ISCIS'13)*, ser. LNEE, E. Gelenbe and R. Lent, Eds. Springer, Oct. 2013, pp. 389–398.
- [39] R. Borgaonkar, K. Redon, and J.-P. Seifert, "Security analysis of a femtocell device," in *Proc. 4th Inter. Conf. on Security of Information and Networks (SIN'11)*, Nov. 2011, pp. 95–102.
- [40] O. Abdelrahman, E. Gelenbe, G. Gorbil, and B. Oklander, "Mobile network anomaly detection and mitigation: The NEMESYS approach," in *Information Sciences and Systems 2013 - Proc. 28th Int. Symp. on Computer and Information Sciences (ISCIS'13)*, ser. LNEE, E. Gelenbe and R. Lent, Eds. Springer, Oct. 2013, pp. 429–438.
- [41] E. Gelenbe and R. R. Muntz, "Probabilistic models of computer systems: Part I (exact results)," *Acta Informatica*, vol. 7, no. 1, pp. 35–60, 1976.
- [42] E. Gelenbe, "Probabilistic models of computer systems: Part II," *Acta Informatica*, vol. 12, no. 4, pp. 285–303, 1979.
- [43] E. Gelenbe and J.-M. Fourneau, "Random neural networks with multiple classes of signals," *Neural Computation*, vol. 11, no. 4, pp. 953–963, May 1999.
- [44] E. Gelenbe, "Natural computation," *The Computer Journal*, vol. 55, no. 7, pp. 848–851, 2012.
- [45] J. Aguilar and E. Gelenbe, "Task assignment and transaction clustering heuristics for distributed systems," *Information Sciences*, vol. 97, no. 1–2, pp. 199–219, 1997.
- [46] S. Papadopoulos and D. Tzovaras, "Towards visualizing mobile network data," in *Information Sciences and Systems 2013 - Proc. 28th Int. Symp. on Computer and Information Sciences (ISCIS'13)*, ser. LNEE, E. Gelenbe and R. Lent, Eds. Springer, Oct. 2013, pp. 379–387.