Outsourcing Mobile Security in the Cloud

Gaëtan Hurel, Rémi Badonnel, Abdelkader Lahmadi, Olivier Festor

Outsourcing Mobile Security in the Cloud

Gaëtan Hurel, Rémi Badonnel, Abdelkader Lahmadi and Olivier Festor

Université de Lorraine, LORIA, UMR 7503, France
INRIA Grand Est - Nancy, France

Abstract. In order to prevent attacks against smartphones and tablets, dedicated security applications are deployed on the mobile devices themselves. However, these applications may have a significant impact on the device resources. Users may be tempted to uninstall or disable them with the objective of increasing battery lifetime and avoiding configuration operations and updates. In this paper, we propose a new approach for outsourcing mobile security functions as cloud-based services. The outsourced functions are dynamically activated, configured and composed using software-defined networking and virtualization capabilities. We detail also preliminary results and point out future research efforts.

1 Introduction

The large-scale deployment of smartphones and tablets [1][2] has led to new security attacks. Because mobile devices are used for a wide range of applications (e.g. call, sms, web, work, banking), they often carry significant amounts of sensitive information that may be stolen. Mobile application markets act as an important threat vector since controls performed on submitted applications are not often available or too weak to detect potential hidden malwares [11]. The problem gets worse as end users do not systematically activate mobile security applications because they do not want to reduce the battery lifetime of their device. In that context, we propose a new approach for outsourcing mobile security so that mobile devices could benefit from remote security functions deployed in cloud infrastructures, therefore minimizing local resource consumption and user involvement [9]. In addition, moving security functions from end-user devices to cloud servers could significantly reduce the overall time spent on associated management tasks (e.g. updates and configurations) and related risks (e.g. misconfigurations). For that purpose, we define a cloud-based architecture able to integrate a large set of security functions for mobile devices. This architecture aims at outsourcing such functions in the cloud and dynamically deploying and combining them using Software-Defined Networking (SDN) and virtualization technologies such as Network Function Virtualization (NFV). Our main goal is to investigate to what extent mobile security can be efficiently outsourced in the cloud, and to evaluate the potential benefits such a strategy can introduce. The remainder of the paper is organized as follows. Related work is discussed in Section 2. We describe our proposed approach for cloud-based mobile security using SDN and virtualization in Section 3. Section 4 details preliminary results, while conclusions and future work are given in Section 5.

2 Related work

Several cloud-based approaches have already been proposed in the literature in order to provide security solutions for mobile devices. Some solutions exploit cloning methods using virtualization to execute security checks, such as Portokalidis et al. [12] and Kim et al. [8]. Some others directly outsource security functions of the mobile devices. Kilinc et al. [7] introduce a cloud-based applications firewall for Android devices, while Oberheide et al. [10] present a cloud-based antivirus for mobile devices of different platforms. More recently, Jin et al. [6] have focused on an SDN-based appliance to detect mobile malwares using traffic analysis performed at the network controller level. In [13], Sherry et al. explore a new design to efficiently and transparently outsource enterprise middleboxes in the cloud using virtualization. Although their work is not dedicated to mobile security, it confirms the potentiality of using the cloud capabilities to outsource security functions. We can observe that most of existing solutions are only partial as they focus on specific instances of the whole security threats set. In addition, they show a lack of flexibility and contextualization regarding how and when to use them. Our solution differs in two main points, namely (i) the way to choose relevant security functions for mobile devices according to their context and current risks, and (ii) the way to outsource, activate and dynamically compose those security functions using SDN and virtualization technologies.

3 Mobile Security as a Service

We propose a new strategy for delivering composable and dynamic security functions for mobile devices, as a transparent service in the cloud. In comparison with traditional on-device models, security is no more performed through a relatively static heap of functions which are executed on mobile devices. Instead, it is *mainly* based on a set of security functions hosted in the cloud and dynamically composable depending on the current context and risk level. Following the cloud terminology, our solution can be classified as a *Mobile Security as a Service (MSaaS)* strategy. The rationale behind moving security functions in the cloud is that setting up a large number of applications and maintaining them to entirely cover the security threats set is a difficult and overwhelming task, even for expert users. Furthermore, users' requirements regarding security of their devices and more generally mobile security threats may vary significantly over time and depending on the context. Our approach aims at addressing these resource consumption, dynamicity, and maintenance constraints. Cloud computing provides the necessary resources and elasticity for efficiently deploying security functions. In particular, we strongly believe that SDN and virtualization technologies can be exploited for facilitating the dynamic composition and transparent deployment of these functions in the cloud. Security functions will be set up as standard cloud services or by leveraging the NFV paradigm, where Virtualized Network Functions (VNF) are deployed on commodity hardware and particularly designed to ease service chaining.

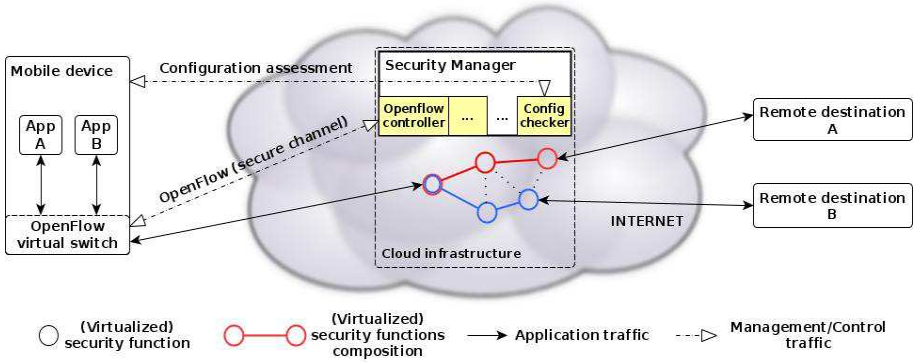

Fig. 1: Our cloud-based mobile security architecture.

The proposed solution is depicted in Figure 1 and involves three distinct entities, namely (i) the mobile device which has several running applications and an integrated OpenFlow-based virtual switch, (ii) the security manager which is hosted by a cloud provider and manages security functions using specific modules (e.g. OpenFlow controller), and (iii) the remote destinations interacting with the mobile device. When an application wants to communicate with a remote destination, all the messages from and to that application are handled by the virtual switch of the device. At the beginning of the communication, the switch may probe an OpenFlow controller configured by the security manager in order to know how to route the related messages for applying security treatments on them. Depending on the risks and context, the manager activates the appropriate security functions and design a customized security composition in a proactive or reactive manner. By pushing the necessary OpenFlow rules within the cloud provider network, the controller then links those security functions to finalize the given composition building and notifies the switch. This one finally makes all the incoming and outgoing messages pass through that composition before reaching the final destination. Therefore, most of the security checks are applied *in the cloud* instead of *on the devices*. Security compositions are designed by the manager according to several factors such as the originating application, the remote destination and the network properties. For example, a mobile application requiring access to the enterprise intranet would need to use a security composition including at least an anti-malware and a data leakage prevention mechanism. On the other hand, a well-known gaming application should deserve less requirements from a security point of view, and some tradeoffs regarding whether or not to use on-device mechanisms could be considered in order to prevent unnecessary communication delay for example. The features are not limited to traffic analysis - the security manager can host additional security functions such as a configuration checker capable of controlling the proper configuration of the mobile devices. Using our approach, most of the security intelligence will be moved at the security manager level, potentially minimizing users involvement.

4 Preliminary results

We have worked on the implementation of a first security function for our outsourcing architecture. The objective of this security function is to analyze in the cloud the configuration of mobile devices in order to identify their potential vulnerabilities. The assessments are performed using the Open Vulnerability and Assessment Language (OVAL)[3], which is an XML-based language widely used to standardize the way to represent vulnerable states and to perform associated assessments. Before fully outsourcing the assessment engine, we have first designed an assessment framework [5] where Android devices periodically fetch vulnerability definitions from a remote server and perform associated local assessments to detect vulnerable states. The solution shows good accuracy regarding vulnerability detection but involves significant usage of resources on the mobile devices during self-assessments. This observation has led us to completely outsource the assessment engine as security function in the cloud [4]. In this new design, mobile assessments are moved in the cloud to the remote server, which implements a probabilistic assessment model in order to distribute vulnerability evaluations across time. This new version consumes about 75% less resources on Android devices, while maintaining the same or even better accuracy regarding vulnerability detection. The reduction in usage of resources on the devices can be explained by two main reasons, namely (i) outsourcing assessments in the cloud offloads most of the work to the remote server, and (ii) the cloud is capable of hosting our probabilistic model in order to calculate partial assessments during each assessment period. The information collected about vulnerable configurations can then be exploited by the security manager in order to activate specific treatments for traffic targeting vulnerable devices.

5 Conclusions and perspectives

The cloud paradigm offers new perspectives to support security functions for mobiles devices. Currently, mobile security is a major issue despite existing applications, and this trend is likely to continue during the next years. As on-device architectural models show several limits including resource usage on the devices side, we propose a new strategy for decoupling and outsourcing security in the cloud and for achieving stronger and pervasive protection of mobile systems. In parallel, leveraging virtualization technologies and software-defined networking may particularly improve transparency and dynamicity with respect to deployment, chaining and composition of security functions. As future work, we plan to pursue our investigation on composition mechanisms and their exploitability for our solution. We are also interested in leveraging data gathering and sharing methods between security functions amongst cloud infrastructures to build large datasets. Such datasets could be useful to extract valuable information about mobile threats and attacks trends for example. In that context, we plan to explore correlation mechanisms and machine learning algorithms by taking advantage of the huge computation capacities offered by the cloud.

Acknowledgments

This work was partly funded by Flamingo, a Network of Excellence project (ICT-318488) supported by the European Commission under its Seventh Framework Program.

References

1. IDC Forecasts Worldwide Tablet Shipments to Surpass Portable PC Shipments in 2013, Total PC Shipments in 2015. `http://www.idc.com/getdoc.jsp?containerId=prUS24129713`. Last visited in february 2014.
2. More Smartphones Were Shipped in Q1 2013 Than Feature Phones, An Industry First According to IDC . `http://www.idc.com/getdoc.jsp?containerId=prUS24085413`. Last visited in february 2014.
3. The Open Vulnerability and Assessment Language (OVAL). `http://oval.mitre.org/`. Last visited in february 2014.
4. M. Barrère, G. Hurel, R. Badonnel, and O. Festor. A Probabilistic Cost-efficient Approach for Mobile Security Assessment. In *Proceedings of the 9th IFIP/IEEE International Conference on Network and Service Management (CNSM'13)*, 2013.
5. M. Barrère, G. Hurel, R. Badonnel, and O. Festor. Ovaldroid: An OVAL-based vulnerability assessment framework for Android. In *Proceedings of the 13th IFIP/IEEE International Symposium on Integrated Network Management (IM'13)*, pages 1074–1075, 2013.
6. R. Jin and B. Wang. Malware Detection for Mobile Devices Using Software-Defined Networking. In *Proceedings of the 2nd GENI Research and Educational Experiment Workshop (GREE 2013)*, pages 81–88, 2013.
7. C. Kilinc, T. Booth, and K. Andersson. WallDroid: Cloud Assisted Virtualized Application Specific Firewalls for the Android OS. In *Proceedings of the 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2012)*, pages 877–883, 2012.
8. T. Kim, Y. Choi, S. Han, J. Y. Chung, J. Hyun, J. Li, and J. W. Hong. Monitoring and Detecting Abnormal Behavior in Mobile Cloud Infrastructure. In *Proceedings of the 12th IEEE/IFIP Network Operations and Management Symposium (NOMS 2012)*, page 1303–1310, 2012.
9. Q. Li and G. Clark. Mobile security: A look ahead. *IEEE Security and Privacy*, 11(1):78–81, 2013.
10. J. Oberheide, K. Veeraraghavan, E. Cooke, J. Flinn, and F. Jahanian. Virtualized In-Cloud Security Services for Mobile Devices. In *Proceedings of the 1st Workshop on Virtualization in Mobile Computing (MobiVirt'08)*, page 31–35, 2008.
11. N. Percoco and S. Schulte. Adventures in BouncerLand: Failures of Automated Malware Detection within Mobile Application Markets. - *Black Hat USA 2012*. `http://media.blackhat.com/`, 2012. Last visited in february 2014.
12. G. Portokalidis, P. Homburg, K. Anagnostakis, and H. Bos. Paranoid Android: Versatile Protection for Smartphones. In *Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC'10)*, page 347–356, 2010.
13. J. Sherry, S. Hasan, C. Scott, A. Krishnamurthy, S. Ratnasamy, and V. Sekar. Making Middleboxes Someone else's Problem: Network Processing As a Cloud Service. In *Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication*, pages 13–24. ACM, 2012.