ESUKOM: Smartphone Security for Enterprise Networks

Ingo Bente[1] · Josef von Helden[1] · Bastian Hellmann[1] · Joerg Vieweg[1] · Kai-Oliver Detken[2]

[1]Trust@FHH Research Group – Fachhochschule Hannover
Ricklinger Stadtweg 120, D-30459 Hannover
{ingo.bente | josef.vonhelden | bastian.hellmann | joerg.vieweg}@fh-hannover.de

[2]DECOIT GmbH
Fahrenheitstraße 9, D-28359 Bremen
detken@decoit.de

Abstract

The ESUKOM project aims to develop a real-time security solution for enterprise networks that works based upon the correlation of metadata. The ESUKOM approach focuses on the integration of available and widely deployed security tools (both commercial and open source like Nagios, iptables or Snort) by leveraging the Trusted Computing Group's IF-MAP protocol. A key challenge for ESUKOM is to adequately address the emerging use of smartphones in business environments. The ESUKOM approach aims to correlate metadata in order to increase the security of smartphone supporting IT environments.

Introduction

The ESUKOM project aims to develop a real-time security solution for enterprise networks that works based upon the correlation of metadata. A key challenge for ESUKOM is the steadily increasing adoption of mobile consumer electronic devices (smartphones) for business purposes that generates new threats for enterprise networks. The ESUKOM approach focuses on the integration of available and widely deployed security measures (both commercial and open source) based upon the Trusted Computing Group's IF-MAP (Interface to Metadata Access Point) specification. IF-MAP is part of a suite of protocols for network security developed by the Trusted Network Connect (TNC) Working Group. The IF-MAP standard enables heterogeneous systems to share arbitrary information in real time.

The idea of ESUKOM is to integrate services that are available in typical enterprise environments in order to share security relevant information via a single metadata pool. A metadata object reflects some information of the enterprise environment (such as authenticated users or currently connected devices). The notion of what a metadata object actually represents is not restricted by the ESUKOM approach. All metadata objects are constructed according to a well-defined, extensible metadata model. By establishing a common metadata pool, already deployed security measures can easily share their knowledge with other services. We envision that this will provide benefits for both the security and the manageability of enterprise networks.

Nowadays, a reliably working IT infrastructure is essential for any enterprise. IT services are inherently necessary in order to support employees by their daily work. Those IT services get even more important when they are also exposed to external customers. Thus, they have also become a worthwhile target of attack. The current threat level is known to anybody who follows the well-known websites that post IT-Security related news. Especially industrial espionage is a major subject for concerns.

One of the key challenges that modern enterprise environments have to face is the steadily increasing adoption of smartphones. Smartphones emerge to small mobile computers with lots of processing power and storage capabilities. Enterprises can benefit from their versatility, using services that allow them to communicate with their employees immediately ant any given time. For the ESUKOM project, smartphones play a key role when current threats for IT infrastructures are considered. Threats that are known from commodity devices like laptops and desktop PCs are now also present on modern smartphones. In order to provide appropriate countermeasures, the special characteristics of smartphones must be taken into account:

1. **Mobility:** Ultra-portable smartphones are used in different environments with different security levels. Physical access to those devices eases to mount a successful attack.
2. **Dynamic networking:** Smartphones are dynamically connected to arbitrary networks. This includes unsecure networks like the Internet as well as more secure networks like a company’s LAN. Furthermore, smartphones are able to establish ad hoc mesh networks by leveraging various communication techniques like Bluetooth.
3. **Application-based architecture:** Modern smartphone platforms enable the users to customize their phones by installing additional, third party applications. Dedicated online stores normally provide these applications. The details of the application provisioning process are platform specific. Applications can leverage the phone’s resources in order to provide their functionality (such as using GPS for location-based services).

Smartphones are widely used across companies in order to manage appointments and contacts and to communicate via email. However, security policies specifically addressing smartphones can hardly be enforced by technical measures in practice. In order to mitigate the threats that are imposed by smartphones, companies need to adapt their currently deployed security measures.

Contributions

This paper presents the first results of the ESUKOM project. The contribution is twofold: (1) we provide a threat analysis that addresses the use of smartphones in enterprise environments. Based on this analysis, key features are derived that mitigate the identified threats. (2) In order to realize the proposed key features, we suggest the ESUKOM approach. It features a centralized metadata pool that reflects the current status of the network. We provide a metadata model that encapsulates the special characteristics of modern smartphones, thus enabling smartphone specific security decisions. By correlating the gathered metadata objects, sophisticated security measures can be provided.

Outline

The remainder of this paper is organized as follows: information on the technical background and the ESUKOM project itself is given in section 2. The threat analysis of smartphones and the derived key features that aim to mitigate them is given in section 3. The current status of the trustworthy metadata correlation approach is presented in section 4. We discuss related work in section 5. Finally, we conclude and highlight areas of future work in section 6

Background

Trusted Computing Group

Modern IT-networks have changed during the last years, from static and homogenous to dynamic and heterogeneous. The amount of mobile devices like Smartphones and notebooks that join and leave a network at any time has increased. As these mobile devices are sometimes not under control by the administrators of the network, the security state of a single device is crucial to the security of the whole network. The Trusted Computing Group (TCG) [Trus07], which is a non-profit organization, has defined an approach to this situation. They specify an open, vendor-neutral framework for trustworthy hardware and software. The term of Trust in the means of the TCG is, that a component that is called trustworthy has to behave as it can be expected, regardless if the behavior itself is good or bad. That is, a trustworthy malware program can be trusted to always behave badly. The decision, if a system is trustworthy or not, relies on securely obtaining the status of a platform with all installed components.

Trusted Network Connect

Trusted Network Connect (TNC) is a Network Access Control approach by the TCG. The main purpose is to control the access of an endpoint to a network, based on the integrity state of that specific endpoint. The measured state is compared to a policy, which was defined by the network operator of a TNC protected network. For example, an enterprise could enforce that any endpoint must have Antivirus software running and that its virus signatures are up-to-date. To securely gather the required information on an endpoint, special software components [Trus09] are used, which also communicate this information to the TNC protected network. In the context of TNC this is called assessment. In case the integrity check fails, several network access restrictions are possible, like a port-based control in 802.1x based networks or restricting access by a firewall filter when using VPNs. Together with its open architecture, TNC distinguishes from other Network Access Control solutions by using the capabilities of Trusted Platforms as proposed by the TCG. By using the TPM of a Trusted Platform, the TNC handshake can be seen as the Remote Attestation of an endpoint, thus showing that TNC is by design capable of doing such a Remote Attestation.

A TNC extended network consists of three different components, namely the Access Requestor (AR), the Policy Decision Point (PDP) and the Policy Enforcement Point (PEP). The Access Requestor is the client that wants to access the network and thus has to authenticate itself to the PDP. During this authentication the client has to proof its integrity state. The PDP then decides if the AR is allowed access to the network, based on the identity and integrity state of the client and by comparing this information with its policies. Afterwards it communicates its recommendation to the PEP, which then enforces it by granting or denying network access. In a 802.1x based network, the PDP could be a server inside the TNC enabled network, the PEP a 802.1x capable switch, and the network access would be controlled by opening or closing ports on the PEP.

IF-MAP

The IF-MAP specification by the Trusted Network Connect subgroup of the Trusted Computing Group describes a protocol for exchanging metadata in a client-server based environment.

Its main purpose is to interoperable exchange security related data between components in a network. So-called MAP clients can publish new metadata to a MAP server and also search for metadata. They also can subscribe to specific metadata and will get informed, when new metadata is published.

The specification in its actual version 2.0 is separated into several documents. The basic communication protocol based on SOAP is specified in [Trus10a] and metadata definitions for network security are defined in [Trus10b]. Thus, new metadata definitions for non-security environment can be specified without changing the specification for the underlying protocol.

Smartphone Security

1.1.1 Android

Android is both an operating system and application framework designed for mobile devices like smartphones and tablets. Google develops it under an open-source license. An Android system offers possibilities to extend it with third party applications, called apps. Apps can be downloaded from the so-called Android market and are installed by the user. The Android SDK provided by Google allows anyone to develop own applications. The bottom layer of Android is based on the Linux kernel in version 2.6, which handles the hardware resources. In the layer above lies the Android runtime as well as some native C and C++ libraries like SSL or WebKit. The runtime environment consists of Java libraries and a virtual machine called DalvikVM. It launches and runs the Android apps, each one in an own instance. A layer called Application framework resides above the runtime layer and provides high-level services in the Java programming language. These services allow easy handling of windows in the GUI, access to the file system or exchanging data between applications. The top layer is the application layer that holds functions like phone, contacts or applications that use the build-in sensors like GPS or motion-sensors. These applications use the underlying libraries and services. Apps developed by third parties also reside in this layer.

1.1.2 Android Security Model

Android's security model consists of two main concepts. In the first place, every application gets a unique process ID and an own user at installation time, as well as an own directory. At runtime, every app runs in a sandbox so it cannot act malicious to other apps. All communication between apps uses specific services of the Android SDK.

Secondly, the access of applications to vital parts of the system like sending SMS or starting a phone call is controlled via permissions. If an application wants to use such services, it has to define the necessary permissions in its Manifest file. At installation time, the user has to grant or deny the use of the permissions to the application. When the app is running, every access to services that are not registered by their permissions in the Manifest file or that were declined by the user during the installation will throw an exception.

The ESUKOM Project

ESUKOM is a research project funded by the German Federal Ministry of Education and Research. It was launched in October 2010. The overall goal of the ESUKOM project is the prototypical development of a security solution with open source software (OSS) that works based upon the Trusted Computing Group’s IF-MAP specification. In order to achieve this goal, the following tasks will be accomplished:

1. **Implementation of IF-MAP software components** A MAP server and a set of MAP clients will be developed. The MAP server as well as most of the MAP clients will be published under an open source license in order to ease their dissemination. Currently, at least the well-known open source tools Nagios, iptables and Snort will be extended with IF-MAP client functionality, in addition to commercial products that are provided by the ESUKOM consortium members.
2. **Development of an advanced metadata model** The IF-MAP specification currently defines a model for metadata that specifically targets use cases in the area of network security. This metadata model will be extended and refined within the ESUKOM project. We aim to add new types of metadata as well as to improve drawbacks of the current metadata model.
3. **Development of correlation algorithms** The analysis and correlation of metadata graphs that are managed by a MAP server is a challenging task. The available specifications give only rough indications how a user might benefit from such a common data pool. We aim to develop algorithms and approaches in order to ease the analysis of large metadata graphs.
4. **Integration of deployed security tools** Another important goal is the conceptual integration of security tools that are already deployed. It must be clarified which sort information should be shared across which existing tools.

To address the threats imposed by modern smartphones that are used in enterprise environments is the mandatory objective. Further information can be found on www.esukom.de.

Smartphone Threat Analysis

The following section analyses threats that arise when using Smartphones in a business environment. This emphasizes the influence of the features modern Smartphones possess on to the overall security of business networks. Only by identifying these specific threats, appropriate countermeasures may be developed.

So-called malware poses an essential problem within this context. According to current predictions, there will be a soaring spread of such malware in the following years. For example, 10% more malware was discovered in the first half of 2010 than in the second half of 2009. Furthermore, the malware discovered in the first half of 2010 is more than what has been discovered in whole 2008 [BeBe10].

Being more and more used and due to their increasing capabilities, Smartphones and other mobile devices (e.g. Tablet computers) become preferred targets of such malware [Wals09]. The number of shipped Smartphones increased to more than 54 million devices, which is a growth of about 57% compared against the previous year. Although the number of known malware is rather low compared against PC platforms (about 40 million malware programs for PC platforms versus about 600 for Smartphones), forecasts assume, that his number will increase dramatically within the next 12 months [Culv10].

Due to these threats and the increased usage of such devices within business networks, a lot of additional attack vectors, which need to be taken into account by network administrators, arise. The German Federal Office for Information Security (BSI) issued a recommendation to no longer use Smartphones (especially iPhones and BlackBerrys) within business networks. Exceptions from this recommendation should only be made if the devices support Simko-2-encryption. [Spie10]

Threat Analysis

The relevant threats for ESUKOM are located within the field of Smartphone (resp. mobile consumer electronic devices) usage in business networks. The following features are therefore defined for Smartphones within this context.

- Inherent sensors: Modern Smartphones possess a high number of sensors, thus allowing to easily gain audio, video and location based information.
- High connectivity: Smartphones are able to communicate through a variety of channels, e.g. Wireless LAN, 3G network connectivity, Infrared (IrDA) protocols or Bluetooth.
- Internet connected: A mobile utilization of the Internet is nowadays possible with a Smartphone. Due to appropriate pricing schemes, services that require a high amount of data transfer volumes may also be used.
- Resource Paradox: Smartphones provide more and more capable hardware components. While there are currently devices with gigahertz processors and more than 256 MB of RAM available, this provided computing power is limited due to the rather small battery capacity.
- App-based architecture: Applications to be used by Smartphones are normally published within special online platforms (commonly called App-Stores). Derived by this development, malicious applications for Smartphones are often called MalApps.
- Platform-variety: There are open-source and closed-source Smartphone platforms by now. The most important platform developers are Apple with their iOS based iPhones, Google with their Android platform as well as Research in Motion (RIM) with their Blackberry devices.

This feature list allows the definition of so called target of attacks (ToA). A ToA may be either the target of a passive or active attack mounted within the context of the business network. A successful attack results in a threat. The following ToA are considered in the context of ESUKOM.

1. Physical environment: The physical environment where the Smartphone is located within is being attacked.
2. Smartphone: The Smartphone itself or data stored on the Smartphone is the target of the attack.
3. It-infrastructure: Smartphones act as man-in-the-middle, thus allowing attacks which target the infrastructure where the Smartphone is connected to.

By using this scheme it is possible to categorize appropriate threats and attack scenarios. The following section provides a short non-complete ToA-categorized summary of threats.

ToA Physical Environment

This type of attack aims on sniffing data from the physical environment by using the Smartphone. This data may be potentially critical and classified. Considering which data is being collected, different threats arise:

- Violation of privacy, for example eavesdropping of personal calls.
- Industrial espionage, e.g. taking photos of critical business processes.
- Creation of movement profiles.

Example attacks within this category are so called sensory malware attacks, where a MalApp uses the appropriate sensor of the Smartphone, or insider sniffing attacks.

ToA Smartphone

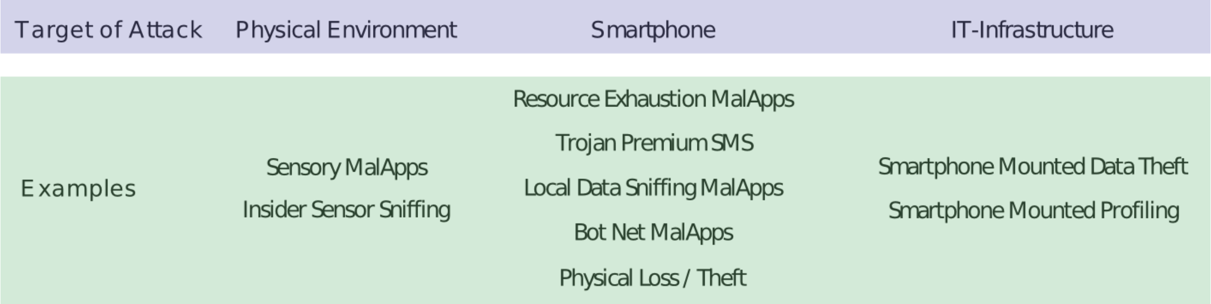
There are several threats that arise if an attack targets the Smartphone itself. There may be for example the threat of:

- Stealing data directly from the Smartphone, for example sensitive information.
- Exhausting the resources of the Smartphone. This could be achieved by simply mounting a denial of service attack or by using the accounting information of the Smartphone.
- Placing MalApps on the Smartphone.

Attacks in this category are for example a distributed denial of service attack mounted by Smartphones where a Botnet MalApp has been placed on. Furthermore a simple loss of the physical Smartphone device is also handled by this category.

ToA IT-infrastructure

Attacks within this category use the Smartphone as a man-in-the-middle to attack the network itself. These attacks are in general similar to commonly known types of network attacks as the Smartphone only acts as attacker. Example attacks could be a so-called Smartphone mounted data theft or some kind of network profiling. An overview of exemplary attacks according to their ToA is given in figure 1.



Target of Attack	Physical Environment	Smartphone	IT-Infrastructure
Examples	Sensory MalApps Insider Sensor Sniffing	Resource Exhaustion MalApps Trojan Premium SMS Local Data Sniffing MalApps Bot Net MalApps Physical Loss / Theft	Smartphone Mounted Data Theft Smartphone Mounted Profiling

Fig. 1: Exemplary Attacks grouped by Targets of Attack

Key Features

Based upon the threat analysis the following set of desirable key features for the ESUKOM solution were identified:

- Anomaly Detection: Consolidation of metadata that was created by different components in order to detect outliers, indicating potential fraud activities. Furthermore, smartphone driven attack patterns (like sensory malware approaches) will be analyzed.
- Smartphone Awareness: Identification of smartphones within the business environment, enabling to provision services that are specifically tailored towards them or to make policy decisions based upon the type of smartphone.
- Single Sign Off: Immediate and global de-provisioning of user accounts, ensuring that revoked credentials cannot be used anymore within the respective environment, no matter which service or device is used.
- Secure Evidence: Generation and integration of evidence records that proof the integrity of metadata objects within the MAP server, thus increasing the trustworthiness of the IF-MAP data set itself.

- Identity Awareness: Making the user's authenticated identity available within a business environment beyond the scope of the authenticating entity, thus enabling use cases like automated, identity based configuration of low level security tools (for example packet filters).
- MalApp Detection: To defend against the spread of potentially malicious applications and to limit the amount of damage they can cause to the respective business environment. This also implies to develop new means in order to assess the security state of a smartphone including its installed applications and their respective privileges that go beyond well-known approaches like Trusted Computing or application certification.
- Location-based Services: To provision services based upon the smartphone's location as well as to support detection capabilities (like the Anomaly and MalApp detection components) by providing location information on users and devices.
- Real-time Enforcement: To enable immediate reaction on identified anomalies by any component that can help to mitigate the potential damage (like flow controllers and network enforcement points).

By implementing this set of key features through open standards, the ESUKOM approach will enable existing business environments to successfully face the challenges that are introduced by the increasing number of smartphones in use. Furthermore, we aim to push the research on mobile phone security in general by developing new security metrics for the most prominent platforms as well as to prove the feasibility of a network oriented approach for smartphone security by implementing a prototype IF-MAP infrastructure.

Trustworthy Metadata Correlation

In order to realize the key features mentioned above, the ESUKOM approach relies on the concept of trustworthy metadata correlation based upon the IF-MAP protocol. This section introduces the current status of this approach. Any security relevant data, whether it stems from a smartphone or a service that is provided by the IT infrastructure (such as an IDS, a Firewall or an AAA service), is expressed according to a well-defined metadata model. In addition, a trust model is defined that enables to reason about the trustworthiness of the metadata instances. Both the metadata model and the trust model are based on the IF-MAP protocol. An open question is still to evaluate the correlation approaches that perform best in order to realize the desired key features.

Metadata Model

The metadata model is the fundamental basis for any further analysis and correlation approaches that are performed. The challenge is to encapsulate both smartphone specific features as well as other metadata of interest that might be generated by arbitrary services in the network in a common model. In addition to only name the relevant metadata concepts, it is also necessary to model the relationships between them.

The current version of the metadata model developed within ESUKOM is based upon the IF-MAP metadata model. That is, the basic components are identifiers, metadata objects and links. However, smartphone specific features are currently not part of the IF-MAP protocol. In order to realize the described key features, it is necessary to (1) name smartphone features of interest and to (2) integrate those features into the IF-MAP protocol.

To decide whether a certain smartphone feature might be of interested for further processing or not is hard. Within the Andromaly project [SKE+11], 88 different features were taken into account in order to detect malicious applications. Each feature even might perform differently, depending on the correlation method that is used.

At this stage, the ESUKOM approach suggest a set of few smartphone features that should be taken into account for further correlation tasks. However, since the metadata model itself is extensible, arbitrary features can be added later on. The current set focuses on Android specific features and the phone's built-in sensors (features of other systems are omitted for brevity). It is depicted in figure 2. Features (white boxes) are hierarchically grouped in categories (grey boxes) and can have alphanumerical values. All features can be easily obtained via standard Android API calls, thus avoiding the burden to extend the Android middleware itself.

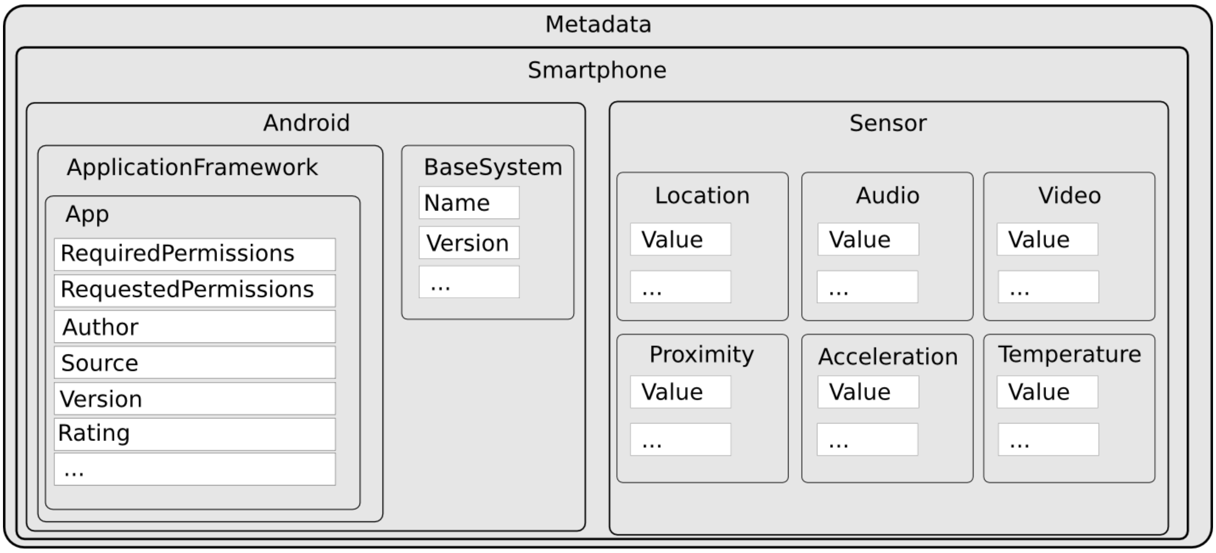


Fig. 2: Smartphone Metadata

In order to integrate these new features to the IF-MAP protocol, two requirements must be fulfilled: (1) the features need to be expressed by means of an XML schema that complies to other standard IF-MAP metadata types (which is trivial) and (2) it must be defined how these new metadata types can be used within IF-MAP. That is, how they fit into the IF-MAP metadata graph. In the current model, the new metadata types are attached to a device identifier that represents the corresponding smartphone.

Trust Model

A Trust Model is required in order to use data for any further correlation approaches. That is, the Trust Model ensures the integrity of the data that is used as input for the correlation. Without ensuring this integrity, due to potential wrong data, the results of the correlation may be useless.

The Trust Model is currently under development within ESUKOM and is not yet fully defined. However, there is a first approach that allows to reason about the integrity of the data. This approach adds the concept of a so-called Trust Level (TL) to the metadata graph. The TL expresses the trustworthiness of a certain data set. That is for IF-MAP, the TL expresses the integrity of the data that has been published into the metadata graph. Besides the concept of adding a Trust Level, there is also a process model, which defines how the Trust relation evolves. The model is divided into three core phases: initialization, reasoning and update. The initialization phase establishes the TL value. The reasoning phase allows us to issue about the TL, for example within a correlation process. Finally, the update phase recalculates the TL according to events that may have happened.

In addition to the concept of the TL and the appropriate process model, there is a first implementation approach for IF-MAP. The TL is expressed as a so-called Trust Token (TT), which is published into the metadata graph. In particular, published into means that the TT is attached to an IF-MAP client. Using this mechanism, all data published by this IF-MAP client is connected to the TT, thus allowing to reason about the integrity of this data.

As already stated, this topic is currently under development as both approaches are only the first prototypes. Due to this, they need to be extended and evaluated in order to fulfill the requirements developed within ESUKOM.

Correlation Approaches

The extended metadata graph forms the basis for any further correlation approaches. Those approaches can now benefit from both the ability to consider network generated metadata and smartphone specific metadata, in addition to the trust tokens that vouch for the trustworthiness of the participating entities.

It is currently investigated which correlation approaches are feasible and perform best for the desired key features. The current candidates include rule- and case-based reasoning, neuronal networks and dependency graphs. However, an evaluation of these approaches is subject of future work.

Related Work

The field of smartphone security is still gaining momentum. Kirin proposed by Enck et al. [EnOM09] is a security service for the Android platform. Kirin aims to mitigate malware at install time by checking the respective application's security configuration against a predefined policy. Kirin is a host-based security extension. In contrast to that, ESUKOM aims to realize a network-based approach in order to mitigate malware threats.

Ongtang et al. [OMEM09] propose the Saint framework. As Kirin, it is a security extension for the Android framework. Saint addresses the issue that the Android platform does not provide sophisticated means in order to enforce policies on the inter application communication on a single phone. The only way to regulate this type of communication is by using the Android permissions labels. Saint introduces are more sophisticated approach. It supports two types of policies: (1) install-time and (2) run-time policies. The install-time policy allows the user to define under which conditions a permission label P defined by an application A is granted to another application B at install-time. Run-time policies on the other hand allow that the IPC that takes place at run-time is regulated according to the respective policy. A remarkable feature of these run-time policies is that it is possible to include conditions based on context information like location, time or the status of communication interfaces like Bluetooth. Furthermore, conditions can cover requirements related to the application developer's signature key.

Porscha [OnBD10] is a Digital Rights Management (DRM) extension for Android. They address the drawback that today's smartphones, including Android based phones, provide almost no means to enforce DRM policies on content that is delivered to the phone. Porscha supports to enforce policies within two separate phases: (1) when the content is in transit, which means when it is delivered to the respective phone and (2) when the content is located on the platform. Porscha allows that content is bound both to a particular phone as well as to a set of endorsed applications on the phone. Furthermore, the use of delivered content can be constrained (for example allowing to play a video within 48h of the purchase date). Such a DRM mechanism could be leveraged in an enterprise environment in order to protect sensitive data.

Portokalidis et al. [PHAB10] propose the Paranoid Android system. Similar to our approach, they follow a network-based paradigm. Remote servers host exact replicas of the smartphones. Based on these virtual replicas, various security checks are performed. In order to establish security measures that are independent of the smartphones resource constraints, the authors suggest that security services in terms of attack detection is provided as a cloud service. A monitoring component on the smartphone, called tracer, gathers execution traces. These traces are then send to a component located on the remote server, called replayer. The execution trace covers all necessary information to replay the execution that has taken place on the smartphone within its virtual replica (such as system calls that pass data from kernel to user space or operating system signals). The ESUKOM approach aims to abstract the smartphone status, thus avoiding the overhead of running *N* replicas for *N* smartphones. Furthermore, ESUKOM does not restrict its analysis components to solely work on smartphone metadata but supports to correlate smartphone specific aspects with other aspects of the network infrastructure.

Conclusions and Future Work

Smartphones that are used in business environments introduce new threats that have to be addressed by appropriate security measures. Recent work in the field of smartphone security has shown that their special capabilities can be abused to mount successful attacks. Approaches to mitigate some of these threats exist, but often require special extensions for the smartphone platform in use.

The ESUKOM approach aims to address smartphone threats by introducing a network based correlation mechanism based on the TCGs’ IF-MAP protocol. By integrating metadata from arbitrary security services as well as from the smartphones themselves, analysis techniques will be employed in order to detect security issues like the presence of malicious applications.

The current status of the ESUKOM approach enables to gather a set of relevant metadata from existing security services (such as VPNs, Firewalls and IDS tools) as well as from Android based smartphones. However, the implementation and evaluation of concrete correlation approaches is a subject of future work.

Acknowledgements

We would like to thank the ESUKOM partners for their valuable feedback and comments on this paper. This work was funded by the Federal Ministry of Education and Research under grant number 01BY1050.

References

[EnOM09] Enck, William and Ongtang, Machigar and McDaniel, Patrick: On lightweight mobile phone application certification. In Proceedings of the 16th ACM conference on Computer and communications security (CCS '09). 2009, p. 235-245.

[OMEM09] Ongtang, Machigar and McLaughlin, Stephen and Enck, William and McDaniel, Patrick: Semantically Rich Application-Centric Security in Android. In Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC’09). 2009, p. 340-349.

[OnBD10] Ongtang, Machigar, Butler, Kevin and McDaniel, Patrick: Porscha: policy oriented secure content handling in Android. In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC '10). 2010, p. 221-230.

[PHAB10] Portokalidis, Georgios, Homburg, Philip, Anagnostakis, Kostas and Bos, Herbert: Paranoid Android: versatile protection for smartphones. In Proceedings of the 26th Annual Computer Security Applications Conference (ACSAC '10). 2010, p. 347-356.

[SKE+11] Shabtai, Asaf and Kanonov, Uri and Elovici, Yuval and Glezer, Chanan and Weiss, Yael: “Andromaly”: a behavioral malware detection framework for android devices. In Journal of Intelligent Information Systems. Springer Netherlands. 2011, p. 1-30.

[Trus10a] Trusted Computing Group: TNC IF MAP Binding for SOAP Version 2.0 Revision 36. 2010.

[Trus10b] Trusted Computing Group: TNC IF-MAP Metadata for Network Security Version 1 Revision 25. 2010.

[BeBe10] Benzmüller, Ralf and Berkenkopf, Sabrina: GData Malware Report Halbjahresbericht Januar-Juni 2010. Retrieved on 08.11.2010 http://www.gdata.de/uploads/media/GData_MalwareReport_2010_1_6_DE_mail2.pdf

[Wals09] Walsh, Lawrence: More Virulent Smartphone Malware on the Horizon, 2009. Retrieved on 05.11.2010. http://www.channelinsider.com/c/a/Security/More-Virulent-Smartphone-Malware-on-the-Horizon-365284/

[Culv10] Culver, Denise: Smartphones: The New Hacker Frontier, 2010. Retrieved on 10.11.2010 http://www.lightreading.com/document.asp?doc_id=196519

[Spie10] Spiegel Online: Sicherheitsbedenken – Regierung verbietet Mitarbeitern Blackberry und iPhone. 2010. Retrieved on 05.08.2010 http://www.spiegel.de/netzwelt/netzpolitik/0,1518,710227,00.html.

Index

Trusted Computing, Trusted Network Connect, IF-MAP, Smartphone Security Metadata Correlation