Trustworthy Anomaly Detection for Smartphones

Ingo Bente
Trust@FHH Research Group

Gabi Dreo
Universität der Bundeswehr München

Bastian Hellmann
Trust@FHH Research Group

Joerg Vieweg
Trust@FHH Research Group

Josef von Helden
Trust@FHH Research Group

1. OUR CONTRIBUTION

Due to the increasing level of utilization, smartphones are commonly used in enterprise environments nowadays. This introduces new threats to such environments like mobile malware with different behavior (mostly exfiltration of user information or abuse of premium services [1]). However, there is currently no established way for an enterprise to assess the security state of connected smartphones in order to prevent or at least limit the potential amount of damage that compromised devices can cause.

To circumvent this problem, we propose a novel network-based, distributed anomaly detection system for smartphones. Our system is based upon the distributed collection of arbitrary, static and dynamic smartphone features. The semantic of a feature can vary greatly (e.g. battery level, permissions of installed applications). The term *distributed* refers to the collection of features. Our approach is not limited to features that can be obtained directly on a device, but also includes features that are provided by other services running in the respective environment (like an Intrusion Detection System) or even external services (for example features obtained by crawling the Android Market). Furthermore, we tag each collected feature with two kinds of information: (1) context information and (2) trust information. Context information addresses environmental parameters like location or time that were given when the feature was collected. Trust information provides means to reason about the trustworthiness of a given feature. Thus, a context-related, trustworthy anomaly detection based on the collected features can be performed. The system is currently developed within the ESUKOM project[1]. Existing approaches primarily address a limited set of features and do not consider context and trust information (e.g. [2]).

2. ARCHITECTURE AND MODEL

Figure 1 depicts the basic architecture of our approach. There are three types of components: (1) *feature collectors*, (2) a *feature database* and (3) a *correlation engine*. Feature collectors gather arbitrary features, tag them with context and trust information and send them to a central Feature Database. The context information is composed of parameters like the current time or location. A feature's trust information includes a set of security properties (SecProps) that describe the feature collector. Based on these security properties, the trustworthiness of the respective feature can be derived later. The feature database is responsible for storing all features that are collected and transmitted by the feature collectors. The correlation engine accesses the feature database in order to perform a variety of anomaly detection methods. Anomalies are described within a policy. Each anomaly definition states the set of features that should be processed and the detection method that should be used (e.g. statistical methods, classifiers, clustering).

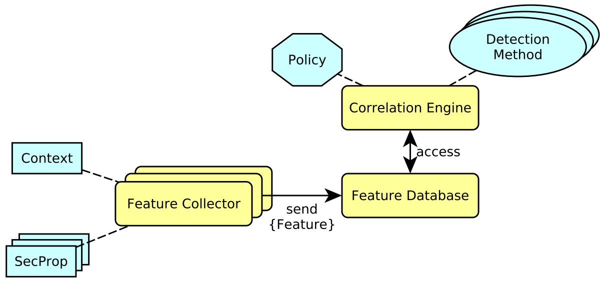

Figure 1: Architecture and Information Model

3. CONCLUSION AND FUTURE WORK

Our approach introduces the idea of context-related, trustworthy anomaly detection for smartphones. The overall architecture, the information model and the correlation interfaces are defined. While the approach itself sounds promising, we have not yet tested it in a real world scenario. Our next step is to gather training data in three different ways: (1) by crawling the Android Market, (2) by observing self written and real world malware and (3) by performing a usage study on Android powered devices. Based on this data, the effectiveness of our approach will be evaluated.

4. REFERENCES

[1] A. P. Felt, M. Finifter, E. Chin, S. Hanna, and D. Wagner. A survey of mobile malware in the wild. In *Proceedings of the 1st ACM workshop on Security and privacy in smartphones and mobile devices*, SPSM '11, pages 3–14. ACM, 2011.

[2] A.-D. Schmidt, F. Peters, F. Lamour, and S. Albayrak. Monitoring smartphones for anomaly detection. In *Proceedings of the 1st international conference on MOBILe Wireless MiddleWARE, Operating Systems, and Applications*, MOBILWARE '08, pages 40:1–40:6. ICST, 2007.

[1] http://www.esukom.de