SPONSORED BY THE

Federal Ministry of Education and Research

ESUKOM

Trustworthy Anomaly Detection for Smartphones

Ingo Bente[1] Gabi Dreo[2] Bastian Hellmann[1] Joerg Vieweg[1] Josef von Helden[1]

[1]Trust@FHH Research Group, Hochschule Hannover

[2]Universität der Bundeswehr, München

Introduction

- Modern smartphones are widely used in corporate IT environments.
- They introduce new threats such as mobile malware.
- Most mobile malware seen in the wild tries to exfiltrate information of the user or aims at abusing premium messaging services.
- Even worse, also benign apps can be a threat (e.g. for user privacy).
- Anomaly detection methods have been successfully used to identify mobile malware.
- Drawback of current approaches: context- and trust-information about features is not considered.
- TCADS aims at adding context- and trust-related information to improve anomaly detection techniques to identify mobile malware.

Motivating Scenario

- Emerging adoption of smartphones in corporate IT infrastructures puts sensitive company data at risk.
- The impact of mobile malware can be huge. The threat addresses
  - ▷ the smartphone itself (i.e. data on the device),
  - ▷ the corporate IT infrastructure it is used in and
  - ▷ the physical environment the device is used in (sensor sniffing attacks).
- Today, companies have little control over smartphones that are used within their corporate, IT infrastructure.
- There is currently no sophisticated solution available that allows to detect mobile malware based on anomaly detection.
- TCADS aims at providing a framework for monitoring smartphones to detect anomalies that are caused by mobile malware.
- Novel aspect: context- and trust-related information are considered during the anomaly detection phase.

Requirements

- Distributed Feature Collection
- Centralized Feature Correlation
- Context- and Trust-related Analysis
- Policy-based Decision Making
- Flexibility and Extensibility of the Framework
- Lightweight Smartphone Extensions

Architecture Overview

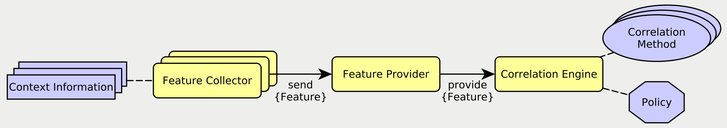

Figure: TCADS Highlevel Architecture.

- Feature Collector gathers features for anomaly detection.
- Feature Provider stores and manages collected features.
- Correlation Engine employs policy-based anomaly detection.

Abstract Model

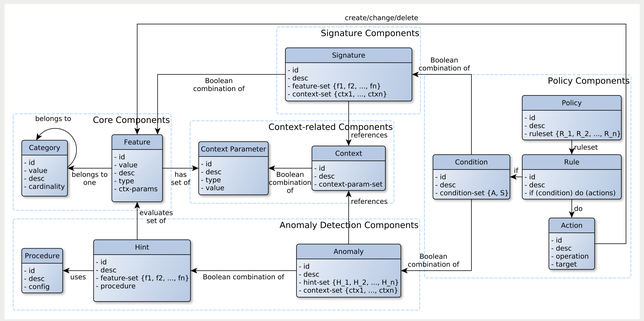

Figure: Abstract Model of TCADS system.

- Core Components
  - ▷ Building blocks to model relevant aspects of a domain.
  - ▷ Feature hierarchy by means of categorization.
- Context-related Components
  - ▷ Encapsulate context-information of features.
- Signature Components
  - ▷ To define patterns based on collected features.
- Anomaly Detection Components
  - ▷ Support to express anomalies based on collected features.
  - ▷ Integration of arbitrary detection methods.
- Policy Components
  - ▷ Simple policy to encapsulate domain-specific knowledge.

Training and Testing

- Training based on policy to create device-specific profiles.
- Testing leverages profiles to employ anomaly detection.

Trust Extension

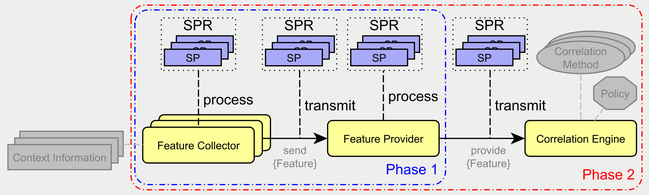

Figure: Trust extended TCADS system.

- Trust extension adds Security Properties ($\boldsymbol{SP}$) to every operation which is used to process or transmit a measured feature.
- Based on these properties, a reasoning of the feature's trustworthiness (i.e a Trust Level) can be performed by the Correlation Engine.
- The Feature Provider is responsible for performing the actual task of calculating the trustworthiness of every feature upon the mentioned $\boldsymbol{SP}$s.
- In detail, the calculation is based on ratings of $\boldsymbol{SP}$s and some intermediary steps: $\{\boldsymbol{SPR}, \{\omega\} \xrightarrow{rF} \boldsymbol{SL}\}_{operation} \xrightarrow{tF} \boldsymbol{TL}_{\zeta}$.

Example

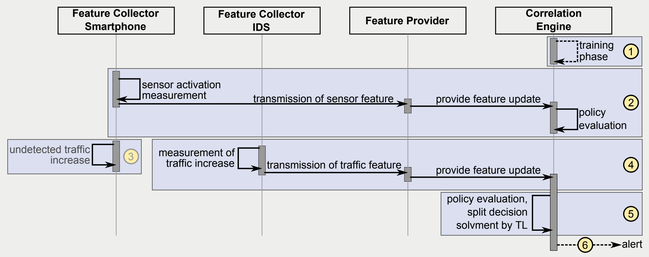

Figure: Step-by-step flow of the example.

- (1)Training phase, (2) measurement of sensor activation and (3) transmission of stolen data.
- (4) IDS recognizes the increase of IP traffic, (5) solving of split decision, (6) alert generation.

Conclusion and Future Work

- TCADS introduces trustworthy anomaly detection for smartphones.
- Conceptual model sounds reasonable, basic building blocks are implemented (based on open standard IF-MAP).
- Training and testing data is currently gathered to perform evaluation.