Consortium

CASSIDIAN
ERNW Living Security.
Fraunhofer AISEC
Hochschule Augsburg University of Applied Sciences
Nokia Siemens Networks
RWTH AACHEN UNIVERSITY

ASMONIA

Attack analysis and Security concepts for
MObile Network infrastructures
supported by collaborative Information exchAnge

SPONSORED BY THE
Federal Ministry of Education and Research

Countering Mobile Malware in the Network and directly on Smartphones

André Egners
RWTH Aachen University

07.05.2013

Motivation

- Mobile malware is on the rise
  - Easy to write malware with arbitrary functionality
  - Sensitive data on the phone attracts data thieves
  - Easy to distribute malware via uncontrolled app stores and websites
- Available anti mobile malware solutions are immature
  - Signature-based approaches and anomaly-based approaches proposed
  - Quality of solutions hard to measure/compare, depends on
    - Environment and type of misbehavior
    - Trained model in the anomaly-based variants

The General Problem

- Malware, Trojan, (Viruses)
- General issues with classical anti-virus products
  - Signature-based
    - Requires external experts for malware analysis and signature generation
    - Only able to detect malware that has been captured before
    - Comes with computation and storage overhead
- Are not well suited for smartphones
  - Still significantly slower
  - Frequent scanning is energy intensive

Our contributions

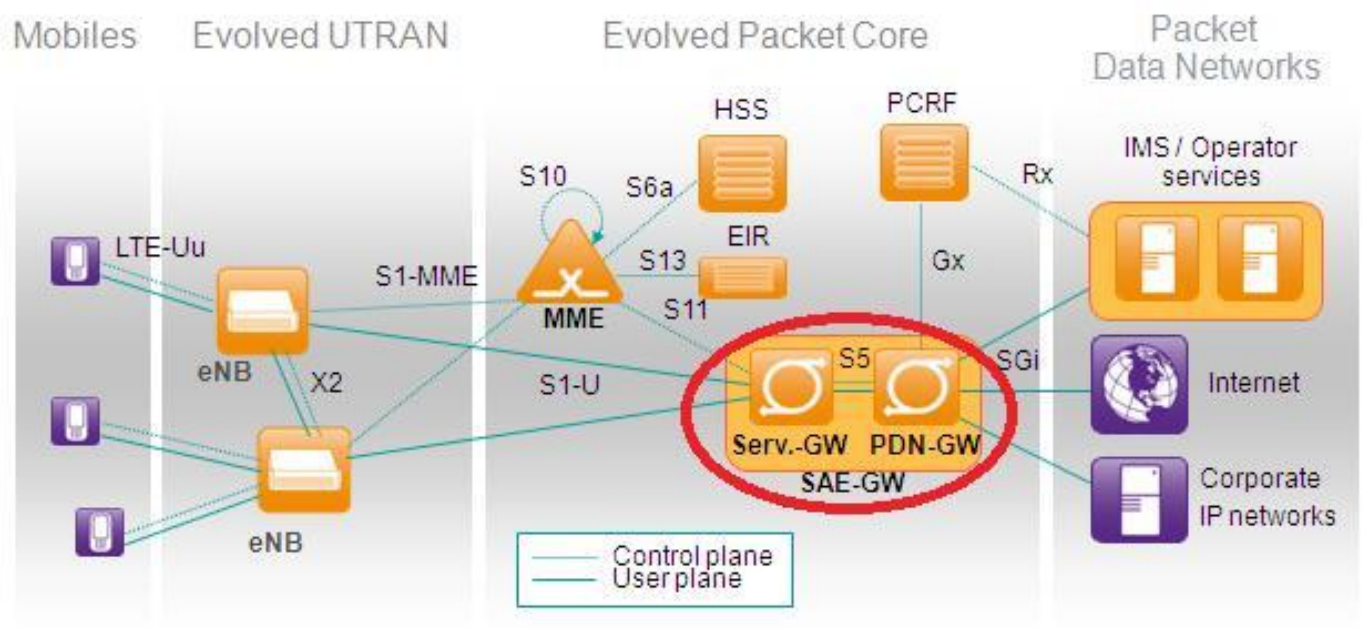
- Dynamic and static analysis of mobile malware
  - Classification of mobile malware based on traffic observable by a network operator
- 4G MOP sensor for in-network detection of mobile malware
  - Self-learning malware detection at the mobile operator
- Anomaly-based detection of mobile malware on the smartphones
  - Based on anomalies found in system call traces
  - Detection on per-app basis

Mobile Malware

- Our classification from the mobile operator’s perspective
- Results from static and dynamic analysis of mobile malware families
  - **SMS only***
    - Premium SMS, Bombers
    - Mobile spyware, Botnets
  - **HTTP only***
    - Mobile spyware
    - Botnets
  - **Hybrid architecture ***
  - Other types

* our focus

In-Network Detection

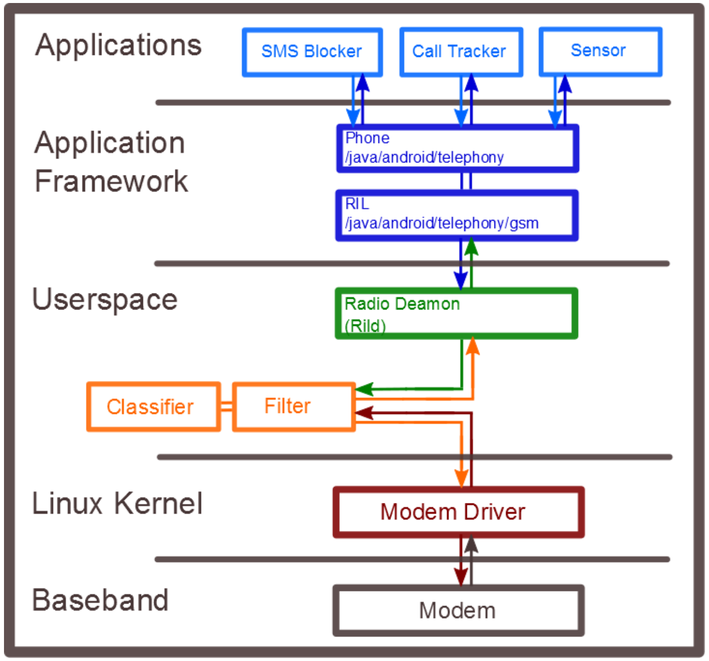


Sensor Requirements

- Must requirements
  - Independent security unit
  - Easy to deploy and maintain
  - Extendible architecture
- Should requirements
  - Real-time filtering and detection
  - Diverse learning approaches
  - Online learning

Sensor Simulation & Demo

- List-based
  - Black & white
- Rule-based
  - Call modes
- Pattern-based
  - Regex C2 commands

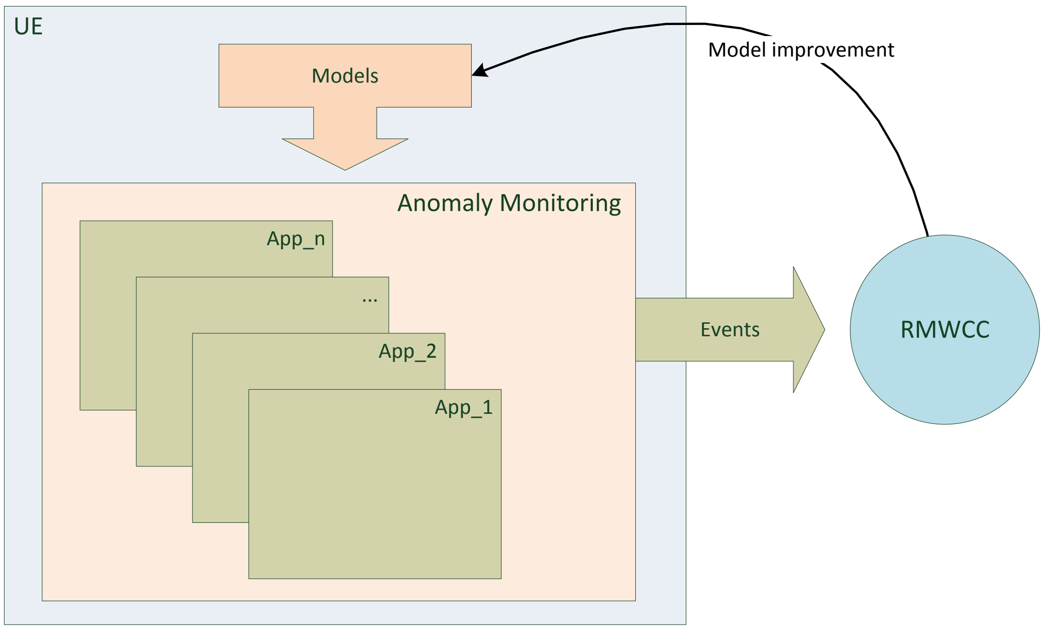


Alternative Detection Methods

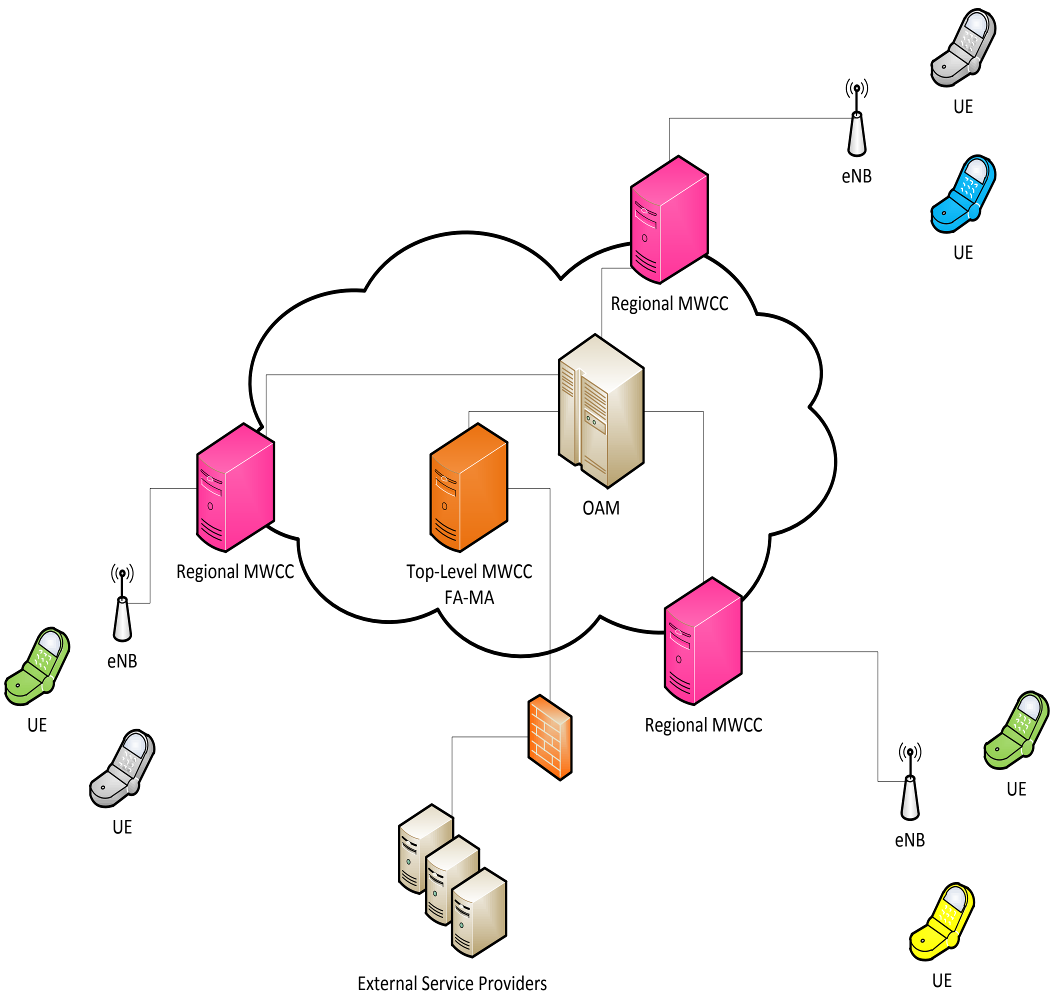
- Monitor behavior of
  - User
  - App
  - Phone
  - …
- Compare *traces* of monitored behavior to model of benign behavior
  - Detect as suspicious if significantly different from benign behavior
  - Iterative learning
- Allows partial matching to known good behavior

Anomaly Detection (UE)

- UE System Call Monitoring
  - App → process
  - Logical coherence
  - Pre-trained models of benign behavior



Anomaly Detection Backend



Backend Communication

- All mechanisms are transported using IP
- Event messages BSON encoded
  - Lightweight, traversable, efficient
- Regional Malware Collection Center
  - Signaling similar to S11 MME-SGW
- Top-level Malware Collection Center
  - Triggers more detailed event information
  - Initiate reactive measures (e.g., UE isolation)

http://bushwarriors.org

Summary & Conclusion

- Manifold malware detection is necessary
- Our two-fold approach provides
  - In-network filtering and detection
  - UE-centric detection on per-app basis
- Intelligence aggregation within the MNO domain

sciencedaily.com