NEMESYS

Enhanced Network Security for Seamless Service Provisioning in the Smart Mobile Ecosystem

FP7 NEMESYS Project: Advances on Mobile Network Security

Elina Theodoropoulou
R&D Projects Section Manager
etheodorop@cosmote.gr
COSMOTE - Mobile Telecommunications S.A.

Nov 2015, Athens

www.nemesys-project.eu

Table of Contents

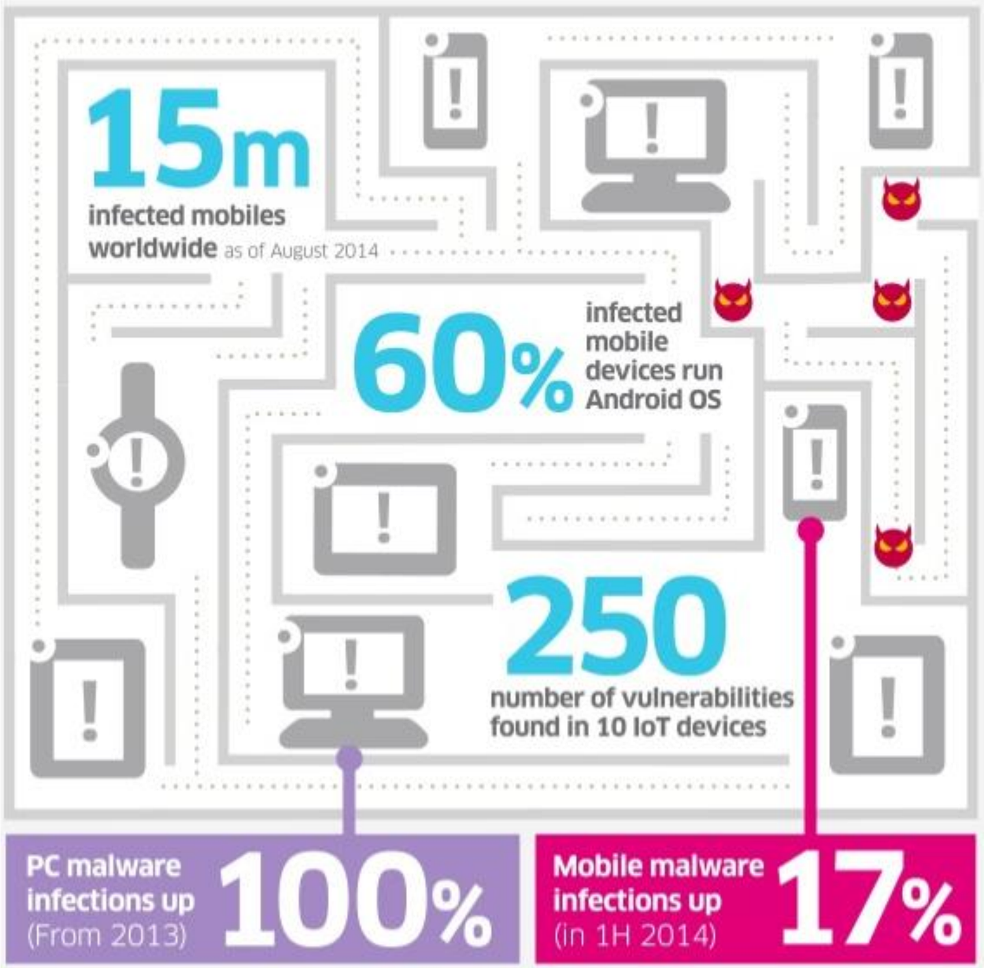
- Threats for Smart Mobile Ecosystem
- Mobile Network Operator’s Requirements
- The NEMESYS Solution
- Benefits for the Mobile Network Operator (MNO)
- Conclusions

Threats for Smart Mobile Ecosystem

The "Smart" Mobile Ecosystem

- Devices/Apps
  - Growing popularity of smart mobile devices | Different OSs/versions
  - Applications (personal data, always on access capability)
- Users
  - Increase in number / Exponential traffic growth
- Communication Technologies
  - 2G/GPRS/EDGE, 3G/HSPA/HSPA+, LTE/4G, femtocells, Wi-Fi, BT, NFC, etc.
  - Transition to flatter and more open network IP-based architectures
- Mobile threats | Increasing vulnerability
  - Growing mobile malware threat and new attack vectors against users (personal info, financial data, etc.) and the core mobile network (outage, billing data, etc.)
  - Low awareness about security and privacy risks

Mobile malware is on the rise



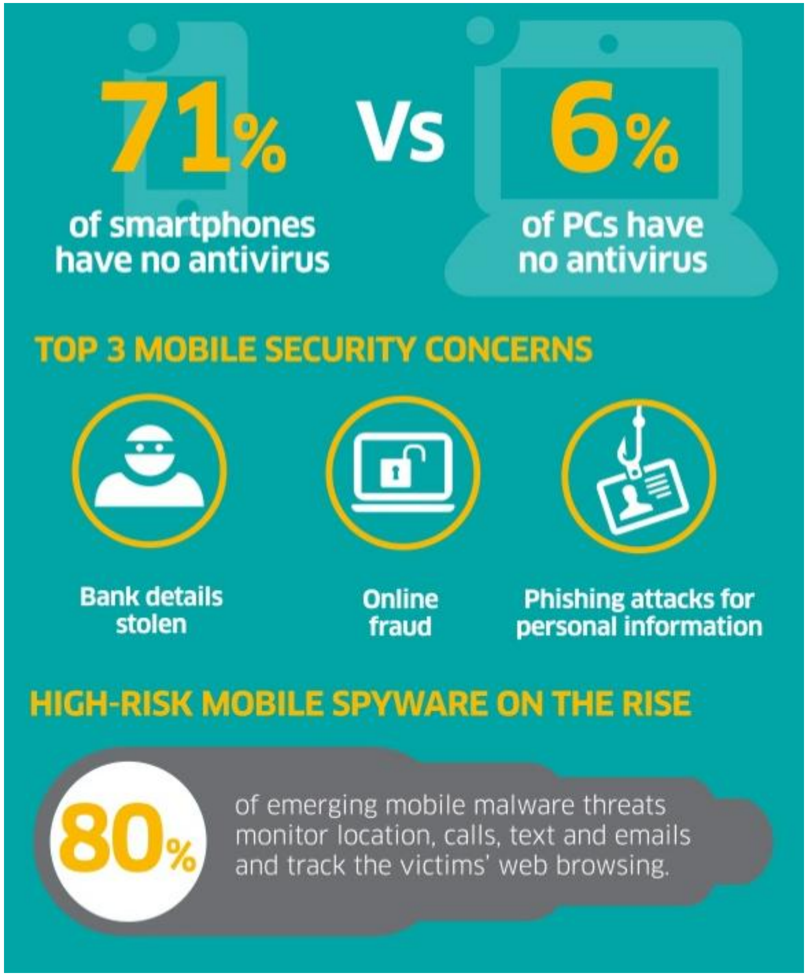
15m infected mobiles worldwide as of August 2014

60% infected mobile devices run Android OS

250 number of vulnerabilities found in 10 IoT devices

PC malware infections up (From 2013) 100%

Mobile malware infections up (in 1H 2014) 17%



71% of smartphones have no antivirus Vs 6% of PCs have no antivirus

TOP 3 MOBILE SECURITY CONCERNS

- Bank details stolen
- Online fraud
- Phishing attacks for personal information

HIGH-RISK MOBILE SPYWARE ON THE RISE

80% of emerging mobile malware threats monitor location, calls, text and emails and track the victims' web browsing.

http://www.alcatel-lucent.com/solutions/security-guardian-infographic

Open issues in mobile security

- New threats due to mobile botnets
- Changing cyber-crime tactics
- Anomaly detection and analysis within large sets of heterogeneous data
- Attack attribution and correlation
- Different levels of security for different mobile OSs
- User awareness
- …

Mobile Network Operator's Requirements

MNO requirements

In case of an attack, MNOs should be prepared to **respond immediately**, thus protecting their subscribers, defending their reputation and ensuring the viability of mobile business

To cope with the emerging security threats, investing in an advanced security solution is a matter of utmost importance for the MNOs who need a **holistic, flexible, effective, proactive, defensive and affordable security strategy** for the massive and undoubtedly complex mobile ecosystem.

MNO requirements – User related

- Availability of a lightweight real-time anomaly detection engine running on various end-user devices and various OSs.
- Real-time notification of an attack to the security analyst and immediate notification to the mobile user with specific instructions.
- The whole process must be transparent to the mobile user.
- No or extremely low impact on the end-user device performance (e.g. battery life, processing power).
- The anomaly detection engine has to be intrinsically secure (it should not be supposed to be vulnerable to attacks).

MNO requirements – System related

- A highly interactive, scalable, future proof, customizable and user-friendly presentation environment (GUI)
- Protection of users' privacy (use of anonymized data)
- Zero impact on access & core network performance/availability
- Be able to collect data from various sources, indicatively from terminals, network and external sources (e.g. databases)
- Always rely upon up-to-date data to identify new attack types
- Highly reliable (high positive detection rate) | Intrinsically secure (not vulnerable to attacks invalidating its results and usage)
- Be mobile network equipment (vendor) independent
- Be scalable/expandable and interoperable (future proof)

MNO requirements – System related (cont’d)

- Capable of “learning” from past experience (e.g. past attack patterns, problems resolution)
- Provide communication interfaces and protocols as well as security and access control
- Fast recovery in case of infection
- Provide high availability (99.99999%)
- Provide support on a 24x7 basis
- Be cost efficient
- Capable of generating new revenue streams (offer advanced security packages incl. secure m-banking and m-commerce)

The NEMESYS Solution

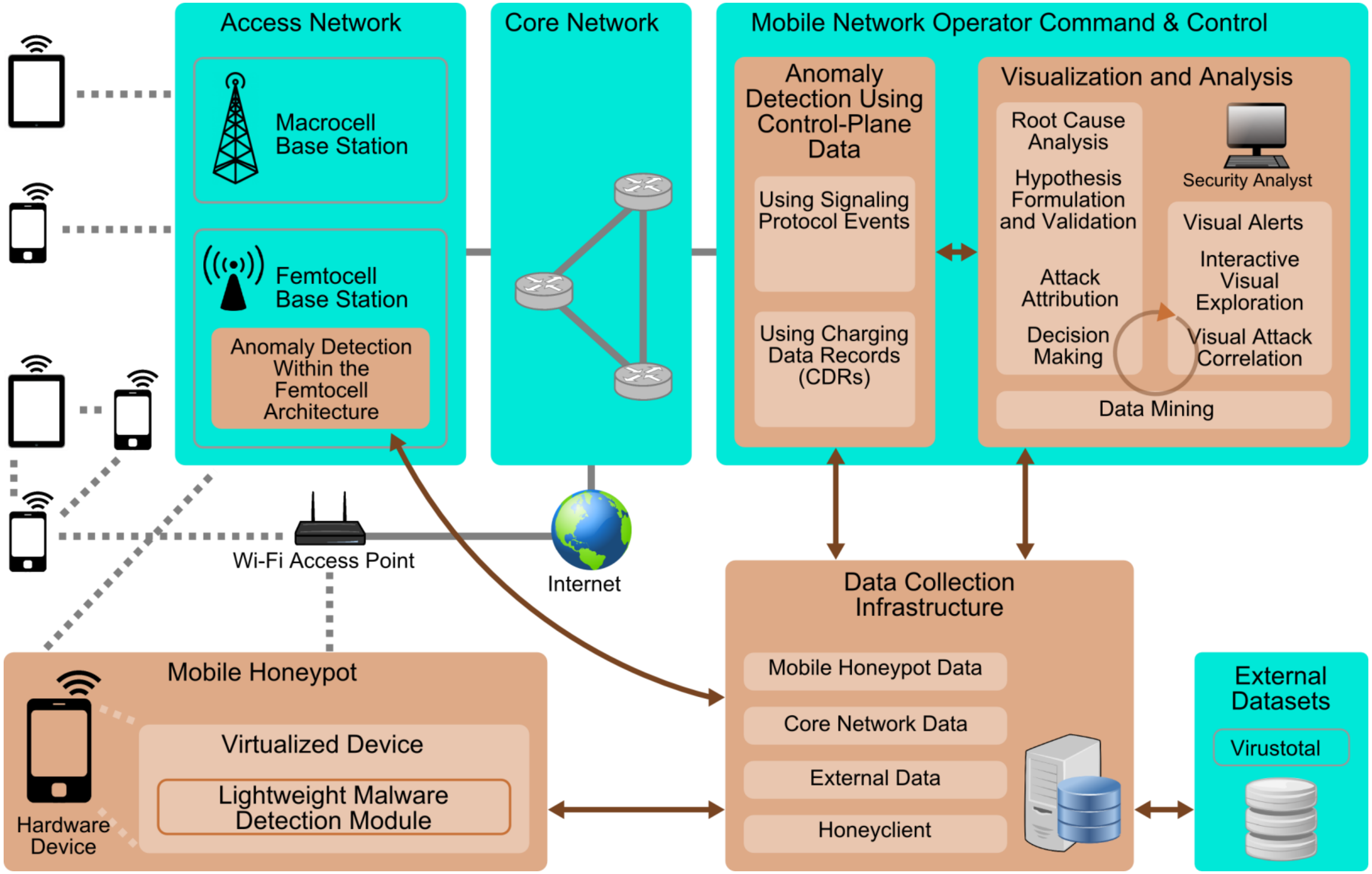
The NEMESYS project

Aim & Objectives

- Improve network and services security in the smart mobile ecosystem
  - Develop a data collection infrastructure incorporating mobile honeypots and honeyclients
  - Gather and analyze information on mobile attacks
  - Develop anomaly detection methods as well as visualization and analysis tools for the security analyst
  - Provide early warning of emerging and existing threats

The NEMESYS Solution

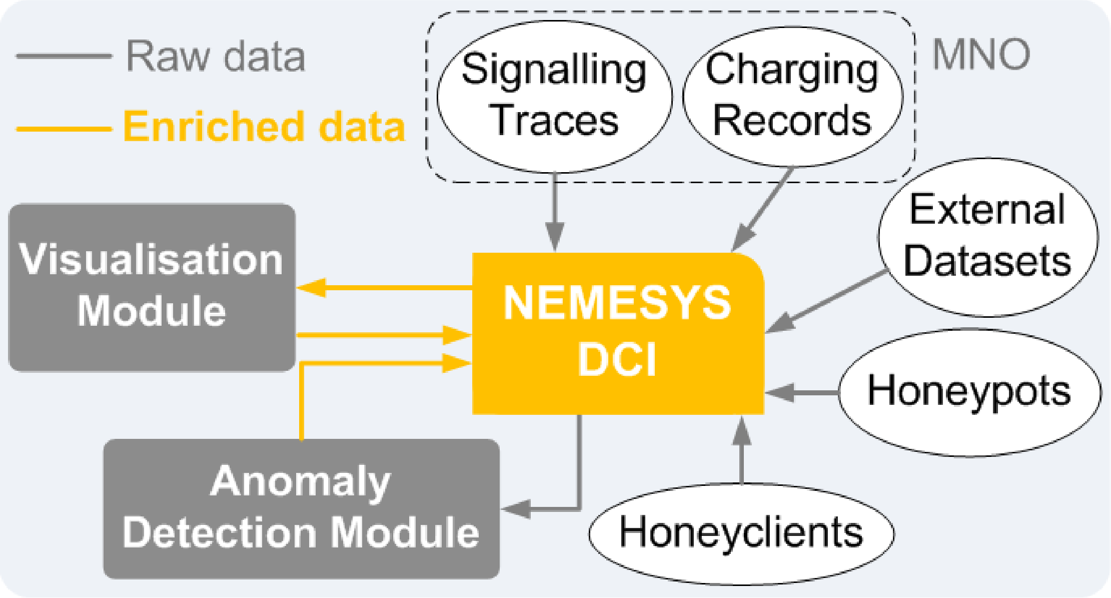
A novel security framework to gather and analyze data about cyber attacks targeting mobile devices and networks and track abnormal behaviours to take countermeasures



Access Network
Macrocell Base Station
Femtocell Base Station
Anomaly Detection Within the Femtocell Architecture
Core Network
Mobile Network Operator Command & Control
Anomaly Detection Using Control-Plane Data
Using Signaling Protocol Events
Using Charging Data Records (CDRs)
Visualization and Analysis
Root Cause Analysis
Hypothesis Formulation and Validation
Attack Attribution
Decision Making
Security Analyst
Visual Alerts
Interactive Visual Exploration
Visual Attack Correlation
Data Mining
Wi-Fi Access Point
Internet
Data Collection Infrastructure
Mobile Honeypot Data
Core Network Data
External Data
Honeyclient
External Datasets
Virustotal
Mobile Honeypot
Hardware Device
Virtualized Device
Lightweight Malware Detection Module

Data collection infrastructure (DCI)

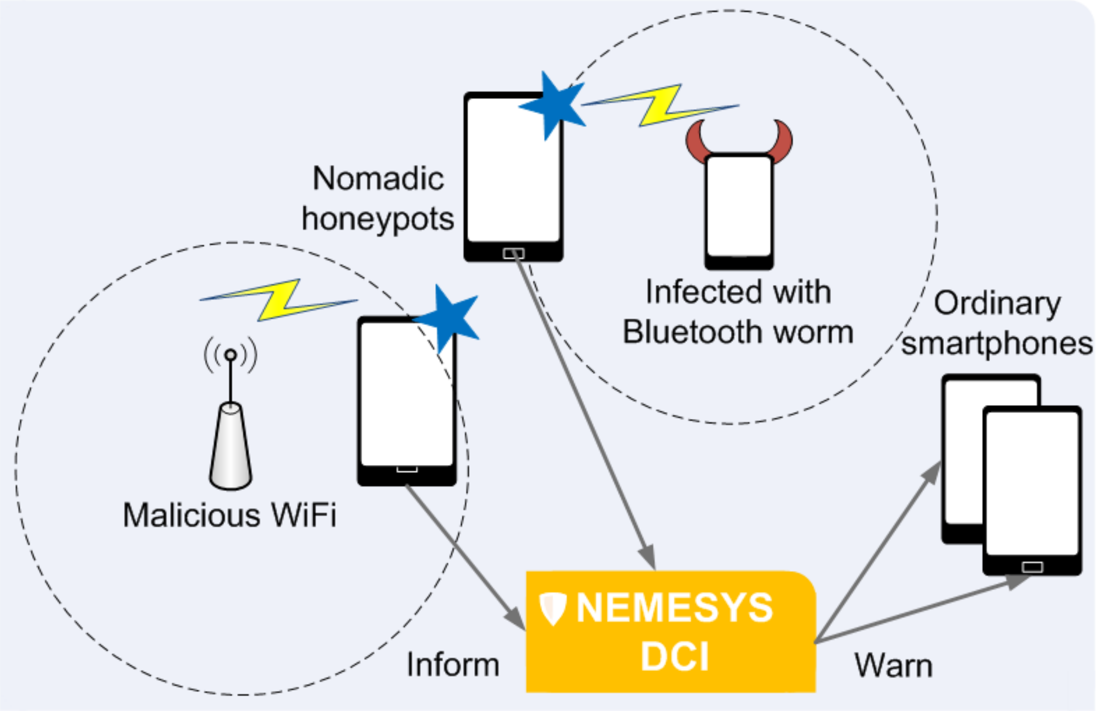
- Repository of information on mobile attacks from:
  - Mobile honeypots
  - Honeyclient
  - Mobile core network
  - External sources



- Perform data enrichment via information analysis

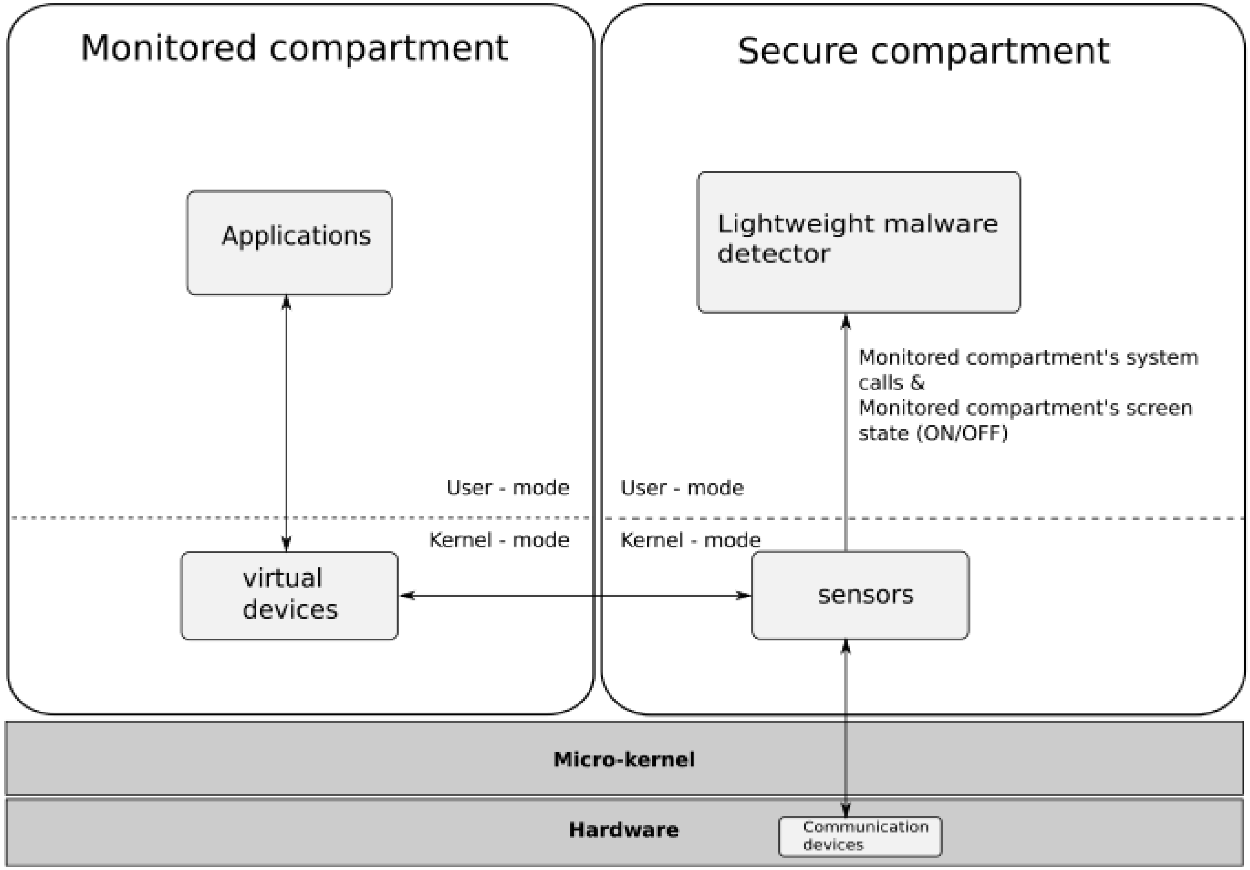
Mobile honeypot

- Mobile (nomadic) honeypots are deployed to volunteers' terminals so as to be probed, attacked and monitored
- Useful in detecting unknown attacks
  - Attacker cannot distinguish between a real phone and a honeypot
  - Monitoring cannot be disabled or modified by malware
  - Enable in-depth analysis during and after the attack



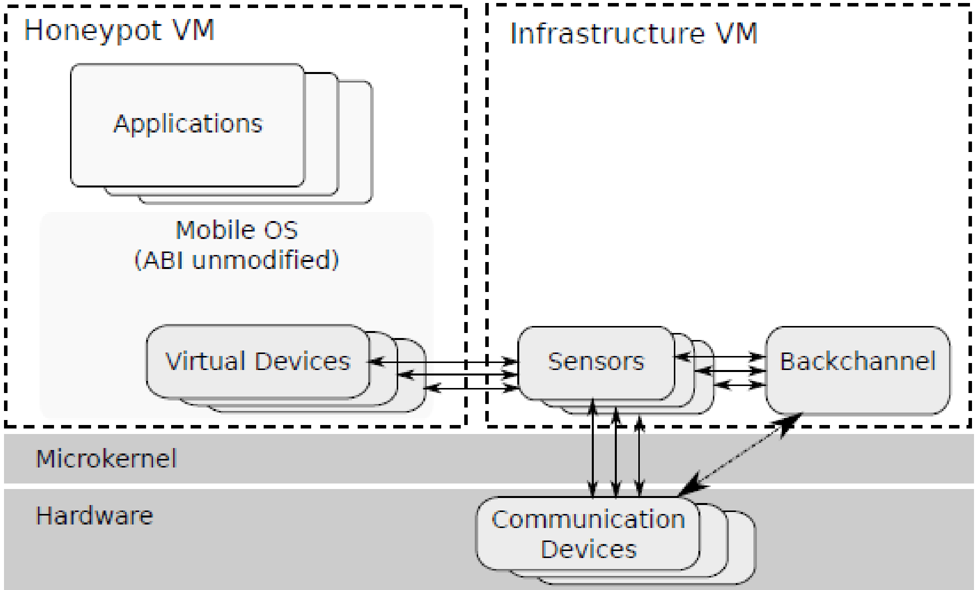
A prototype Samsung GSII honeydroid

- The Honeydroid (mobile honeypot) consists of 2 compartments: a monitored (vulnerable to attacks) and a secure compartment where the Light Malware Detector (LMD) is located



Honeypot virtualisation technology

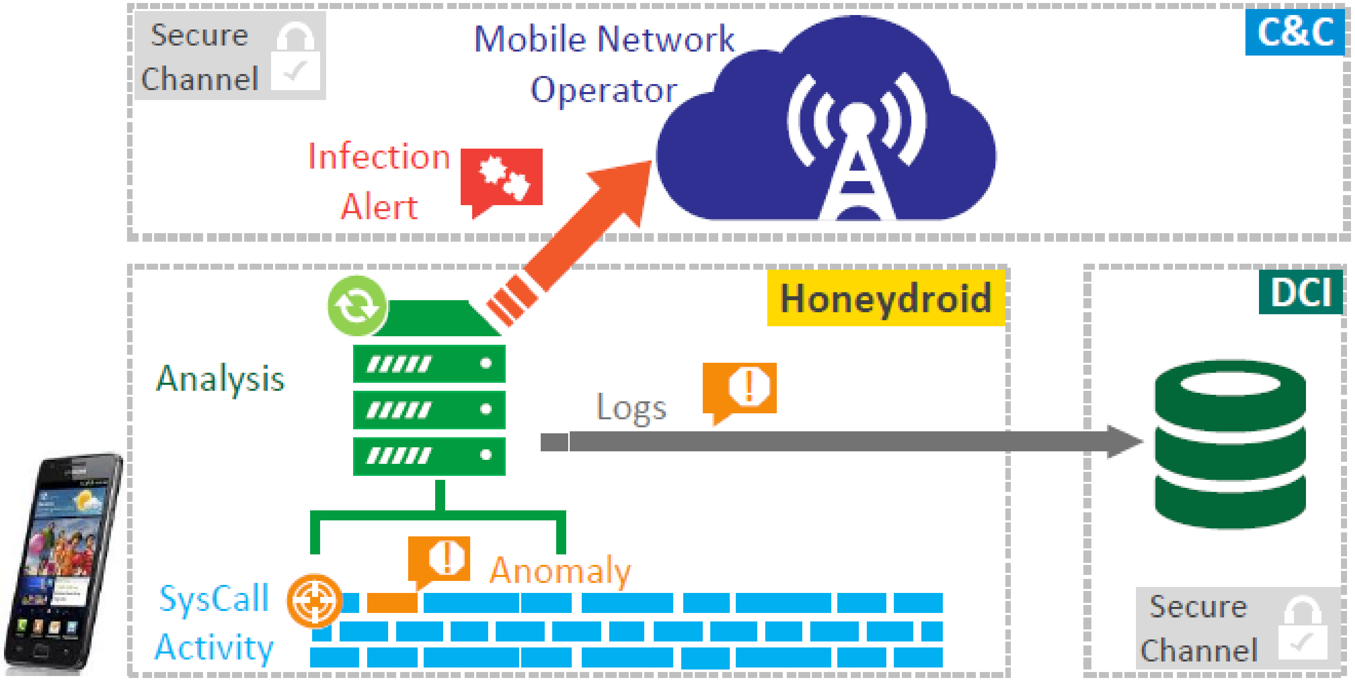
- Honeypot VM
  - Hosts the (unmodified) mobile OS
  - No direct access to communication hardware



- Infrastructure VM
  - Mediates access to communication hardware
  - Runs a lightweight malware detector to identify malicious behavior
  - Traps all suspicious communications
  - Provides the event monitoring, logging and file system snapshot facilities
  - Communicates with the NEMESYS data collection infrastructure to send mobile attack traces

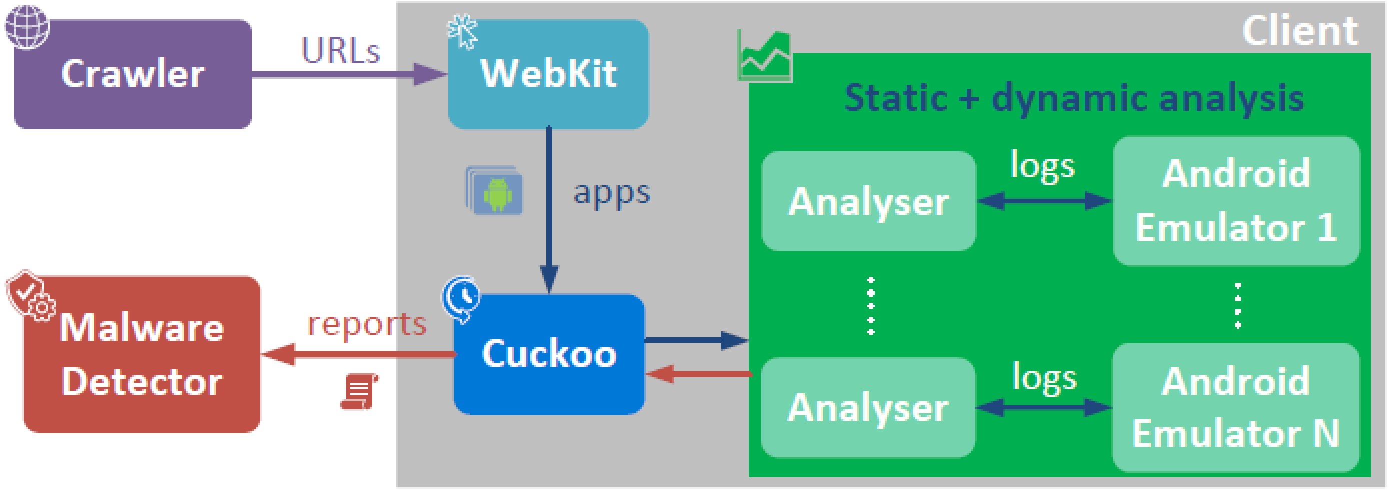
Lightweight Malware Detector (LMD)

- LMD collects several system calls in a regular period of time, analyses them and decides if the mobile device is infected or not.
- Upon deviation from the normal behavior, an alert is triggered and a snapshot of the file system is taken. The difference between two consecutive snapshots enables the analysis of the attack.
- LMD stores the system calls in DCI to study and improve the algorithms.



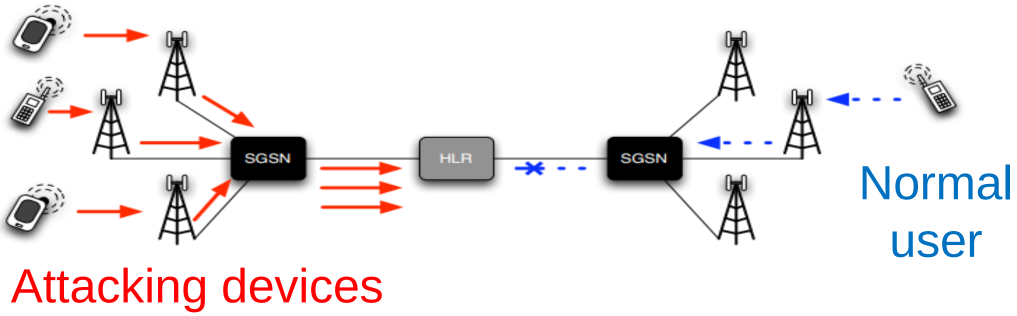
High interaction honeyclient

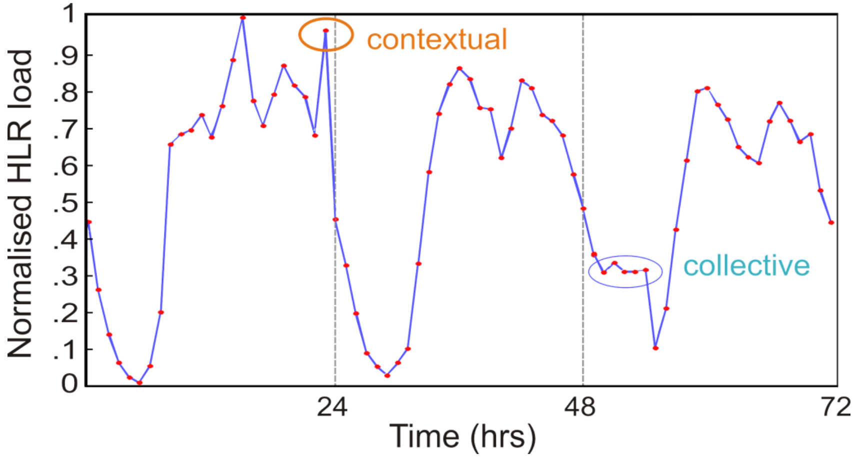
- Interacts with web servers to identify malicious mobile web pages and any malicious apps they host. It consists of three components:
  - **Crawler:** generates a list of websites of interest for the client to visit
  - **Client:** runs Android emulators + app analysers, and stores the results
  - **Malware detector:** identifies malicious content



Anomaly detection using control plane data

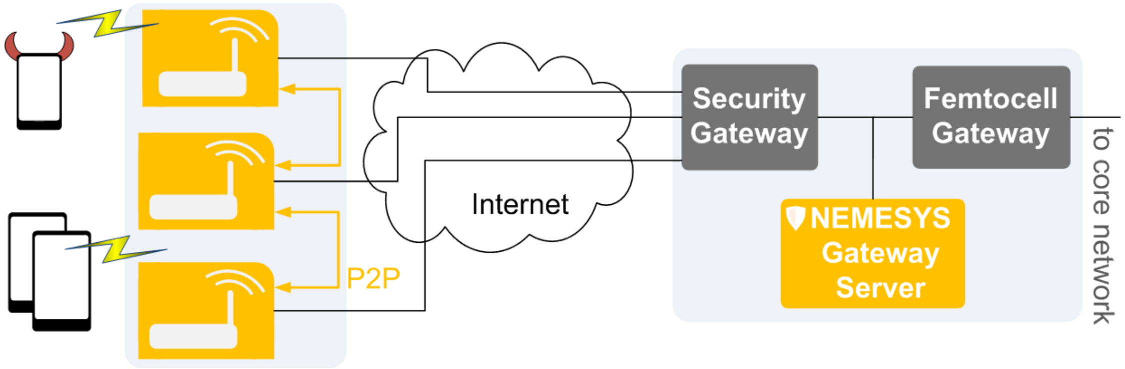
- Algorithms developed for identifying different types of anomalies in HLR
  - HLR/HSS: Critical components holding the details of millions mobile subscribers





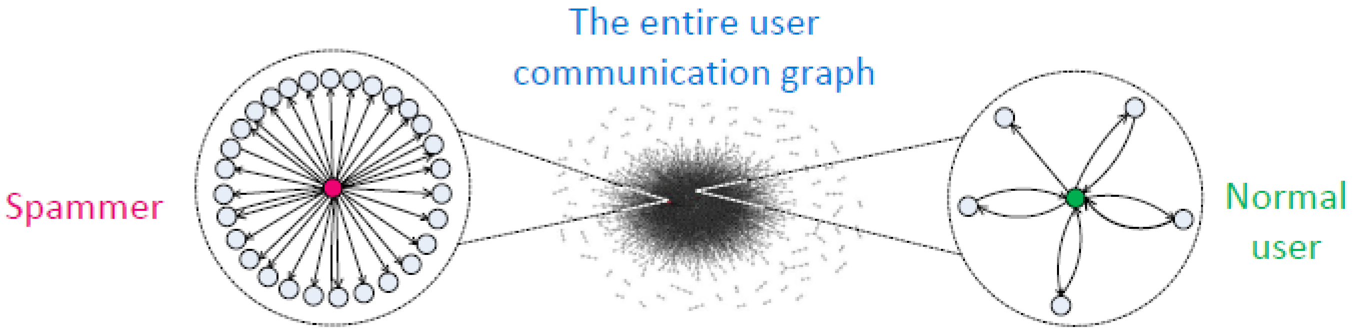
Security architecture for femtocells

- A compromised femtocell can be used to launch attacks against both the users and the mobile core network
- Femtocell devices
  - no end-to-end encryption
  - run outdated versions of open source software
  - have a web based configuration environment
  - their components are insufficiently isolated from one another



Visual Analytics for the Mobile Network Operator

- NEMESYS visualisation tools help the security analyst identify complex attack phenomena through hypothesis formulation and testing, attack attribution, and correlation analysis

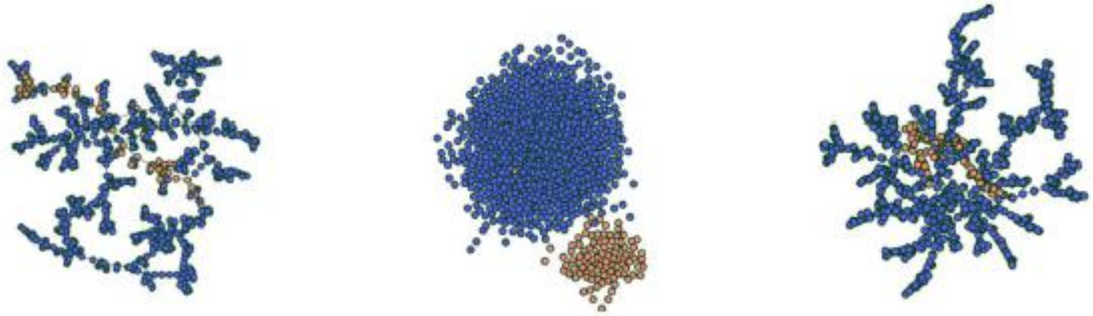


The entire user communication graph

Spammer

Normal user

Clustering of subscribers' common behaviours



Benefits for the Mobile Network Operator

Benefits for the MNO

- Rapidly identify traffic involved in malicious attacks | Reduce time between infection and mitigation
- Warn its customers early enough, prevent intrusions against their mobile devices and save them from bill shocks, thus reducing churn and achieving wider market share
- Differentiate from competition and promote the company’s brand/ reputation by protecting its customers from security risks, misuse and fraud while offering high service experience
- Save huge effort and expenditures that would have been required for security “repairs” and downtimes
- Generate new revenues by addressing new markets, such as selling security packages and security sensitive applications (m-banking / m-commerce / m-payments)

Conclusions

Conclusions

- The NEMESYS solution addresses the main MNO requirements
- Security solutions currently available by the major equipment vendors are not considered as holistic ones yet
- There are still issues to be investigated before the commercial exploitation of the solution
  - Terminal-related: battery drainage and performance degradation, applicability to various devices/OSs, rooting, real-time notifications, additional functionality (e.g., no SMS when screen is off), etc.
  - Integration into a “live network” to verify e2e proper operation | multi-vendor support.

Thank you for your attention!

Imperial College London

INFORMATION TECHNOLOGIES INSTITUTE
centre for research & technology - hellas

TELECOM ITALIA
INFORMATION TECHNOLOGY

TU berlin

HISPASEC

COSMOTE