NEMESYS

COOPERATION

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

Ερευνητικό έργο NEMESYS: Καινοτόμες τεχνικές προστασίας συσκευών και δικτύων κινητών επικοινωνιών από κακόβουλες επιθέσεις

Dr. Konstantinos Filis
R&D Senior Engineer
cfilis@cosmote.gr
COSMOTE - Mobile Telecommunications S.A.

Infocom Security, April 2015, Athens

Imperial College London

berlin

INFORMATION TECHNOLOGIES INSTITUTE
centre for research & technology - hellas

HISPASEC

TELECOM ITALIA
INFORMATION TECHNOLOGY

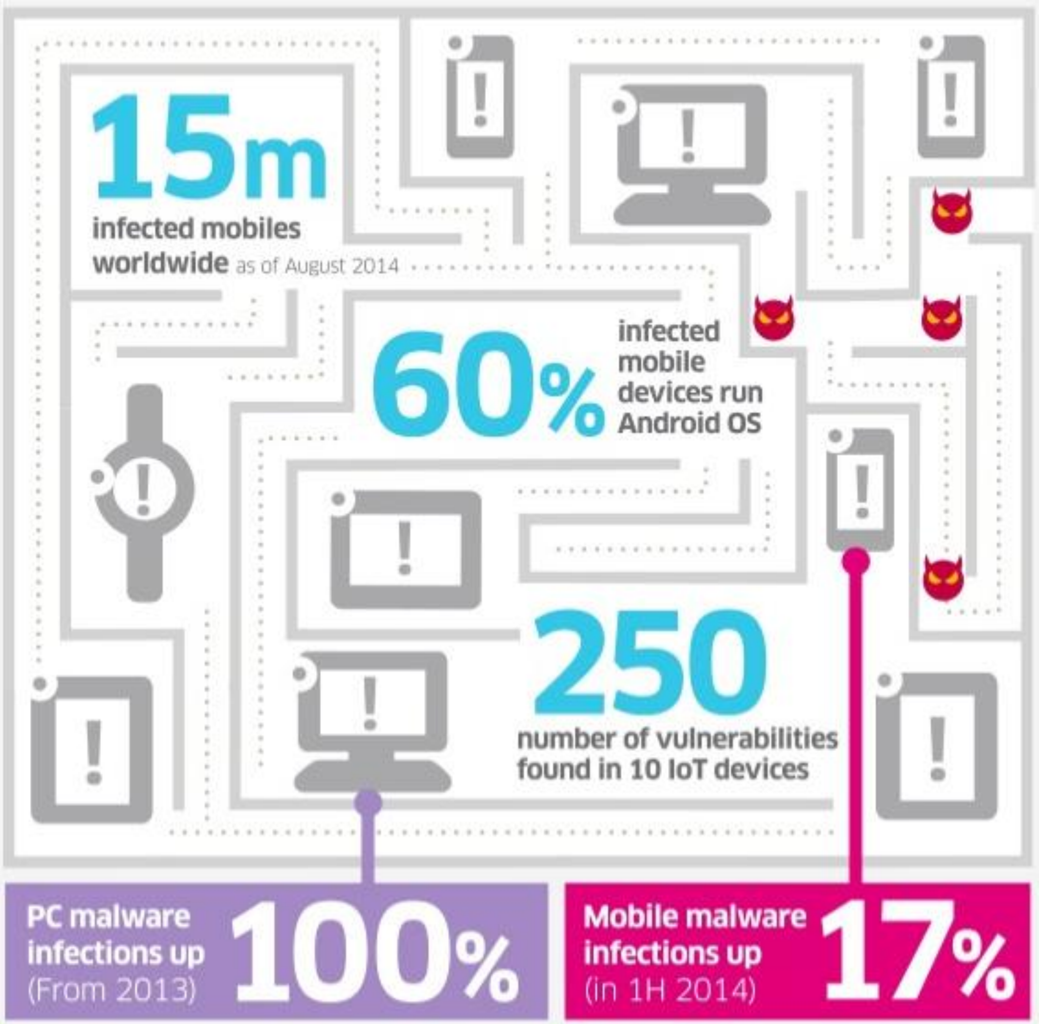
COSMOTE

www.nemesys-project.eu

The “Smart” Mobile Ecosystem

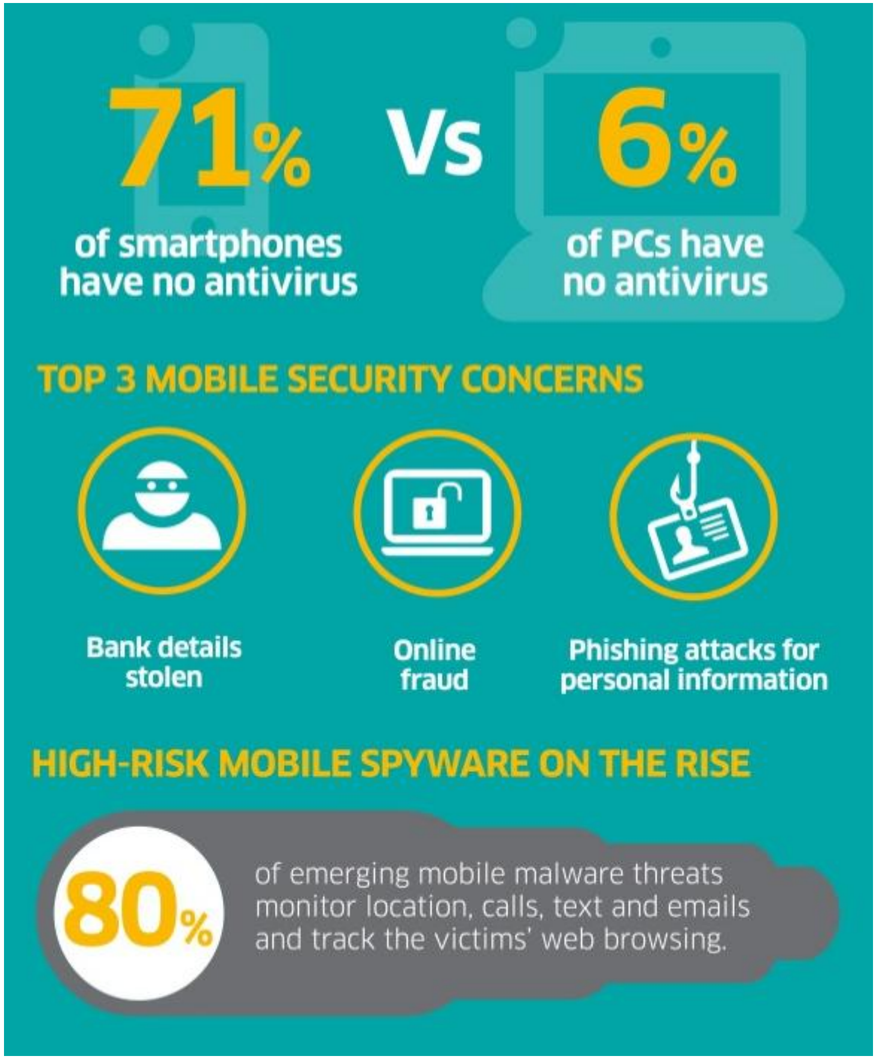
- Devices/Apps
  - Growing popularity of smart mobile devices and Applications
  - Different OSs
- Users
  - Increase in number, increase in usage (device/network)
- Communication Technologies
  - 2G/GPRS/EDGE, 3G/HSPA/HSPA+, LTE/4G, femtocells, Wi-Fi, NFC, BT, etc.
- Mobile threats
  - Growing mobile malware threat and new attack vectors against users (personal data, financial data, etc.) and the core mobile network (outage, billing data, etc.)
  - Low awareness (users)

Mobile malware is on the rise



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

Mobile devices are unprotected



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.

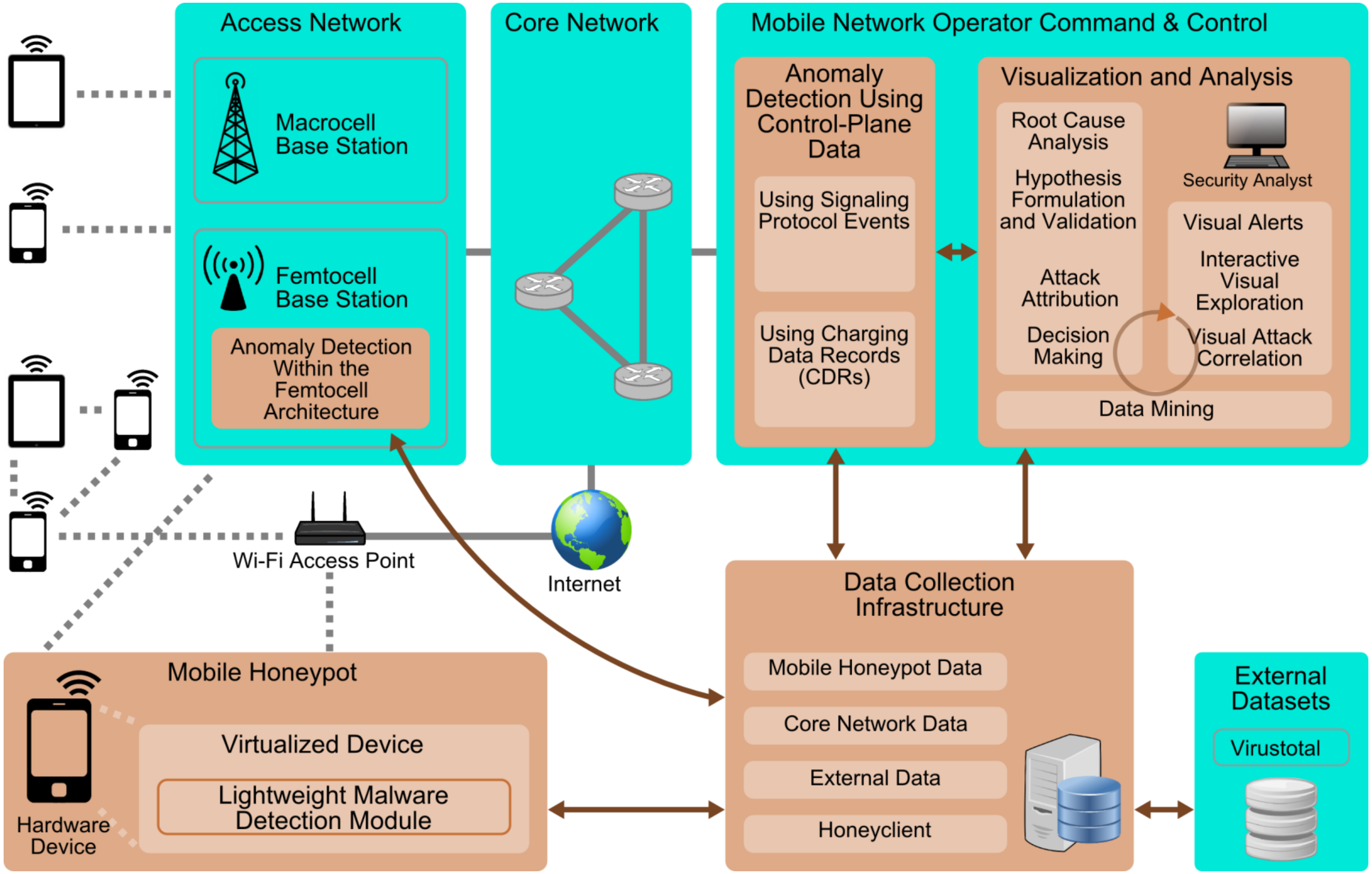
http://www.alcatel-lucent.com/solutions/security-guardian-infographic

Open issues in mobile security

- New threats due to mobile botnets
- Changing cyber-crime tactics
- Attack attribution and correlation
- Anomaly detection and analysis within large sets of heterogeneous data
- Different levels of security for different mobile OS
- Resource monitoring in the smartphone
- Device configuration surveillance for security vulnerabilities
- User awareness

The NEMESYS framework

A novel security framework to gather and analyze data about malicious 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
Virtualized Device
Lightweight Malware Detection Module
Hardware Device

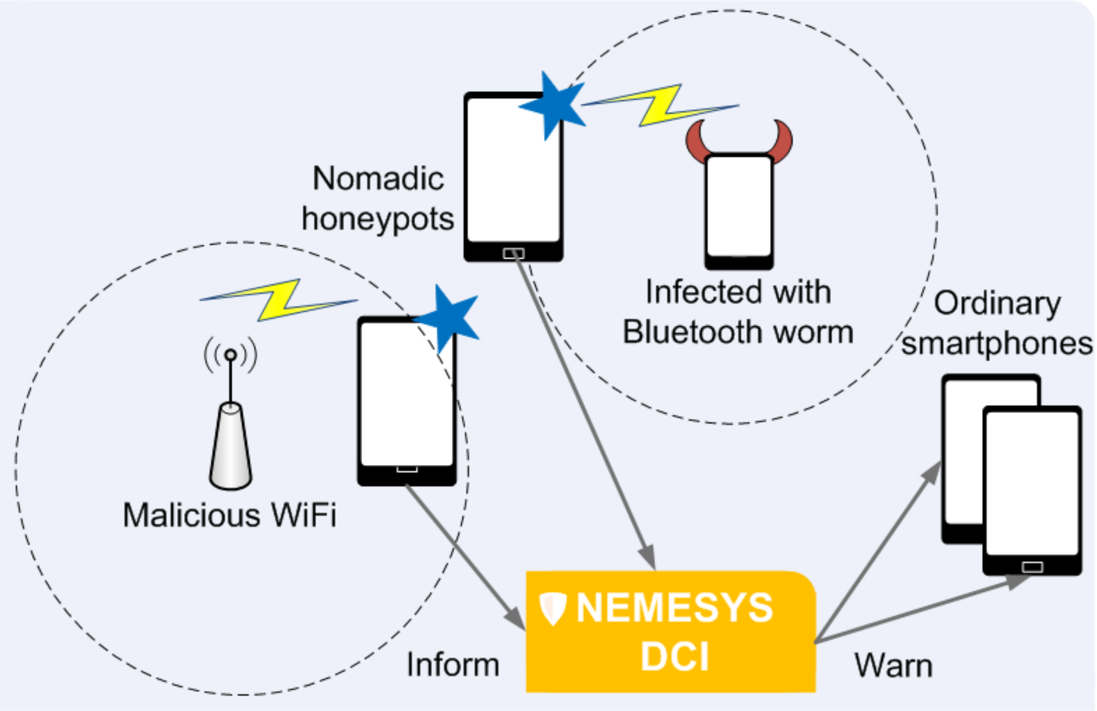
The NEMESYS project

Objectives

- Understand the mobile threat landscape
- Improve network security and services 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 and visualization and analysis tools for the security analyst
  - Provide early warning of emerging and existing threats

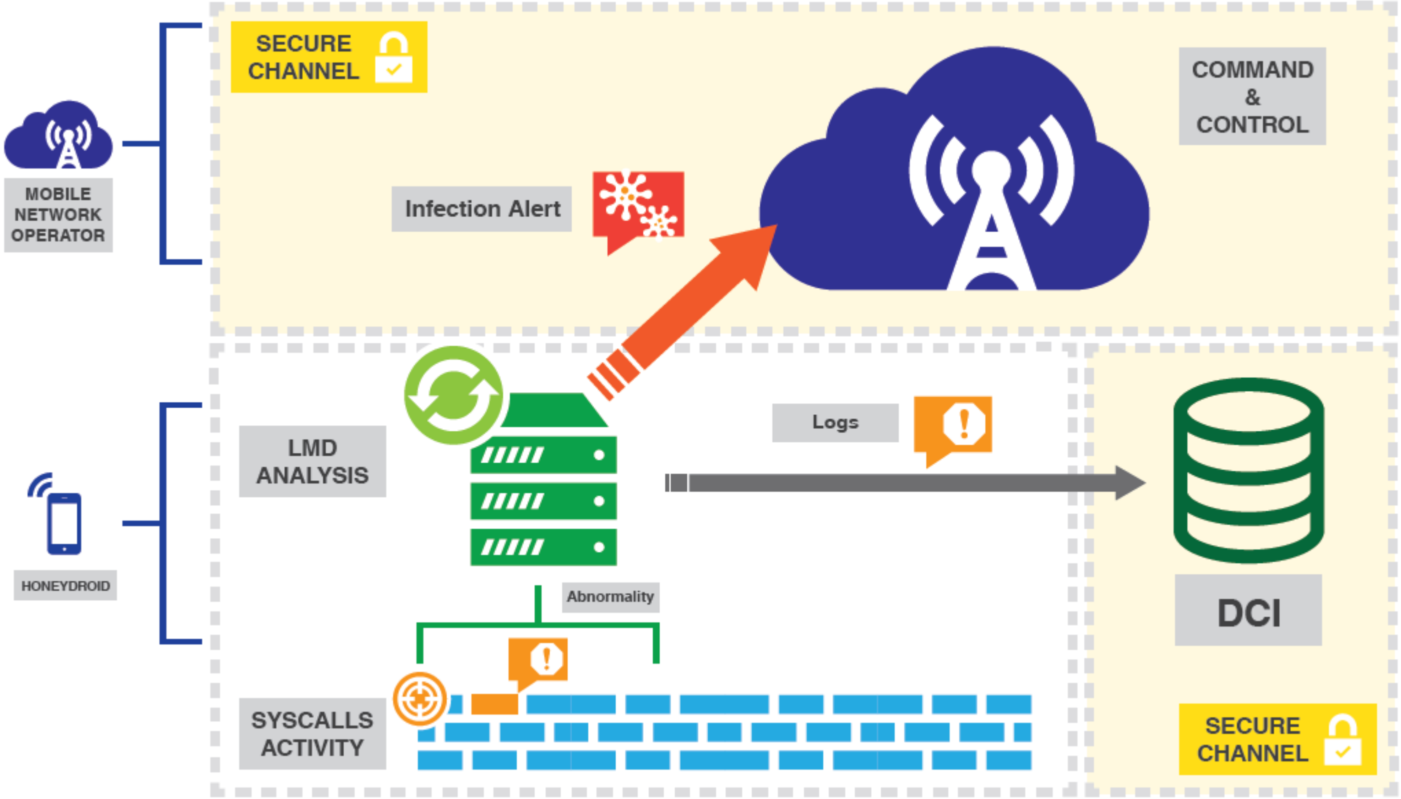
Mobile honeypot

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



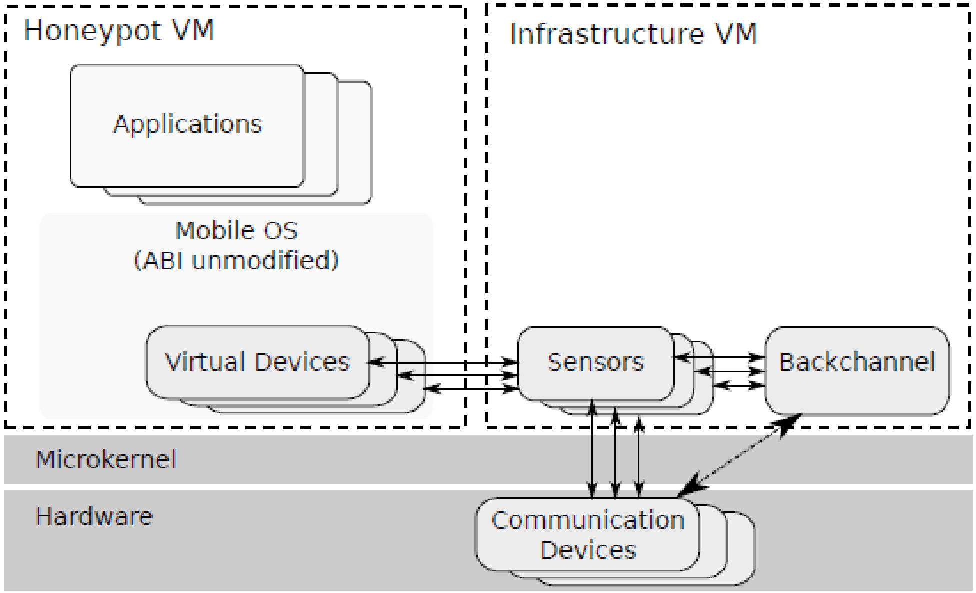
Lightweight Malware Detector (LMD)

- LMD collects several system calls in a regular period of time, analyses them and decides if the mobile device is infected or not.
- LMD stores the system calls in DCI to study and improve the algorithms



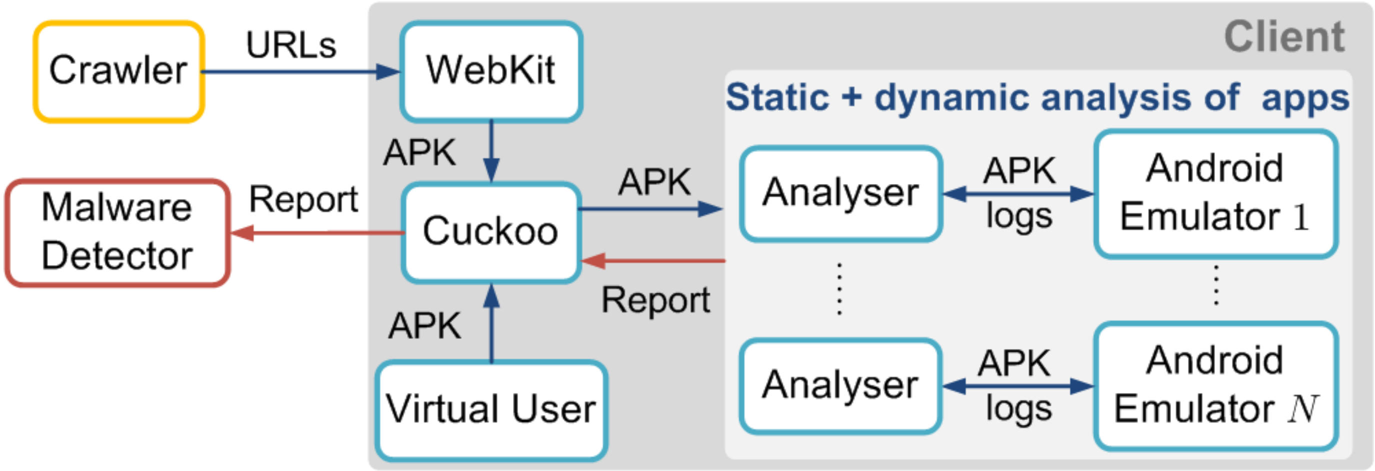
A prototype Samsung GSII honeydroid

- Honeydroid = Mobile honeypot + LMD
- Virtualised devices include: baseband modem, audio subsystem and display
- Pre-installed apps and third-party apps



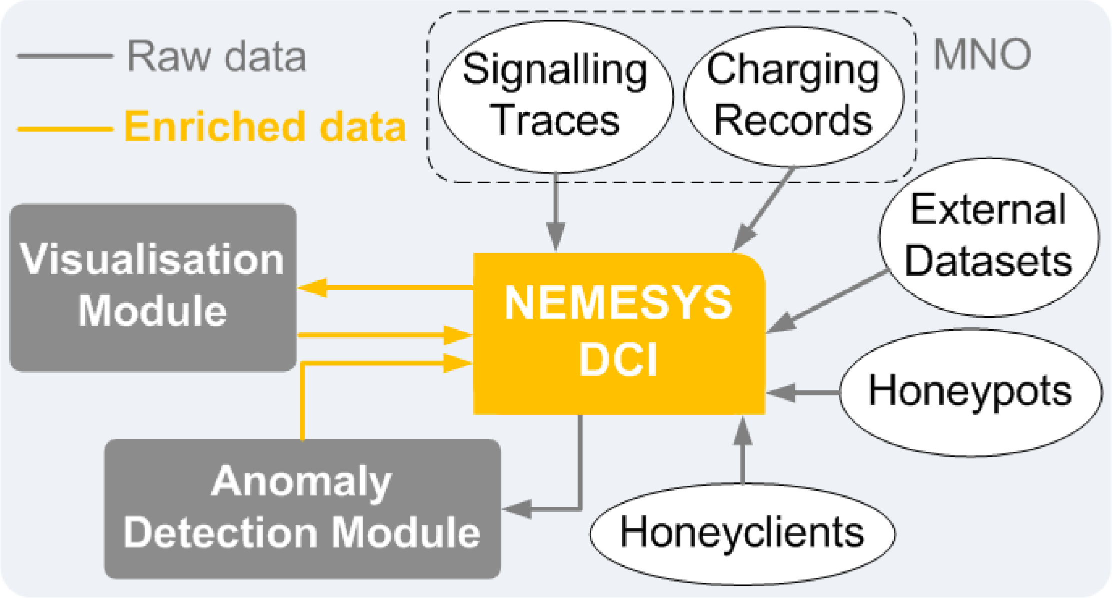
High interaction honeyclient

- 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



Data collection infrastructure (DCI)

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

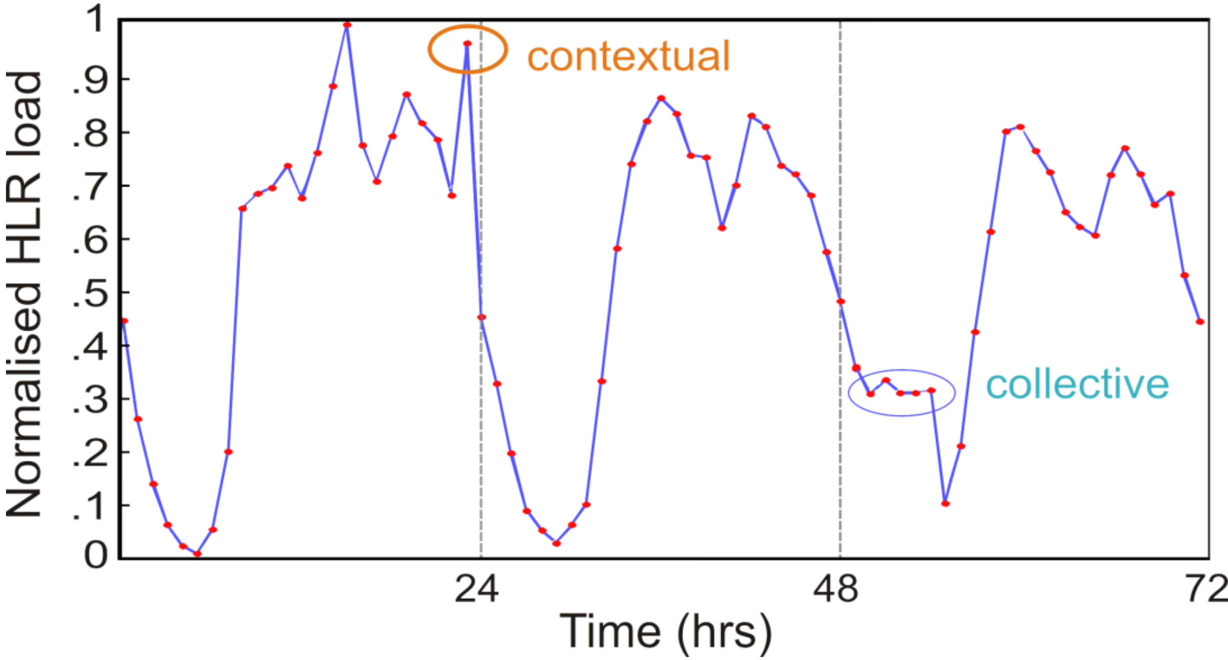


- Perform data enrichment via analysis and accessing external sources

Anomaly detection algorithms

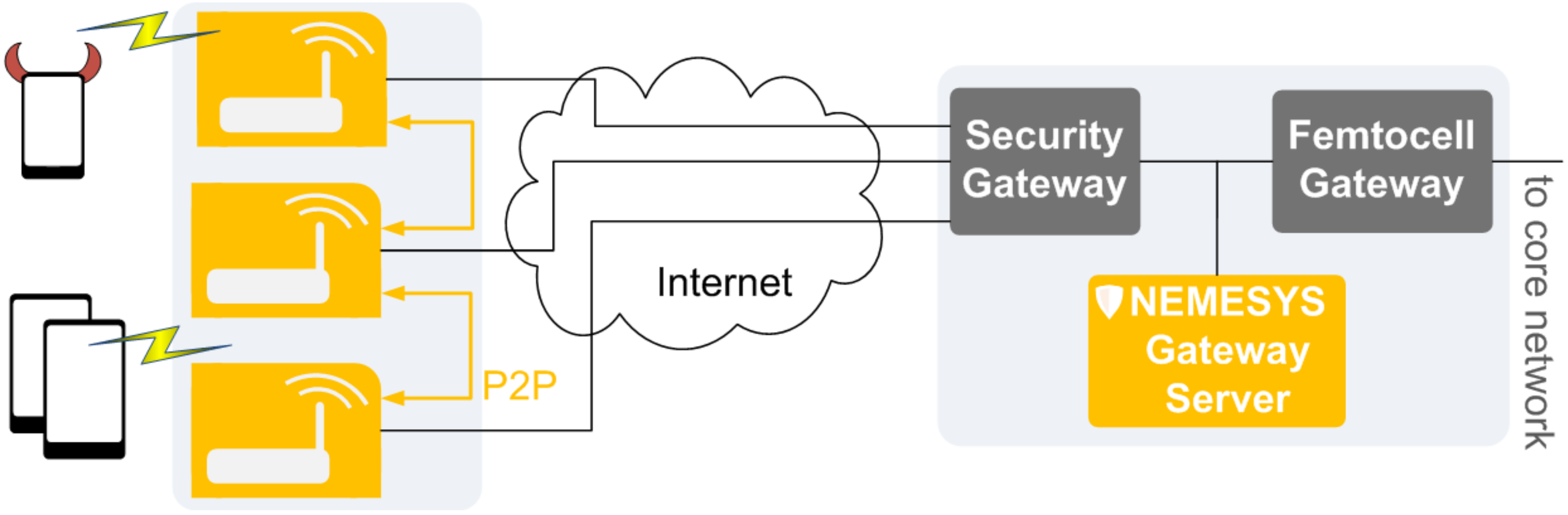
- Critical components include the HLR/HSS which hold the details of millions of mobile subscribers
- Mobile botnets and femtocell devices could be exploited to attack the core network

Algorithms for identifying different types of anomalies have been developed



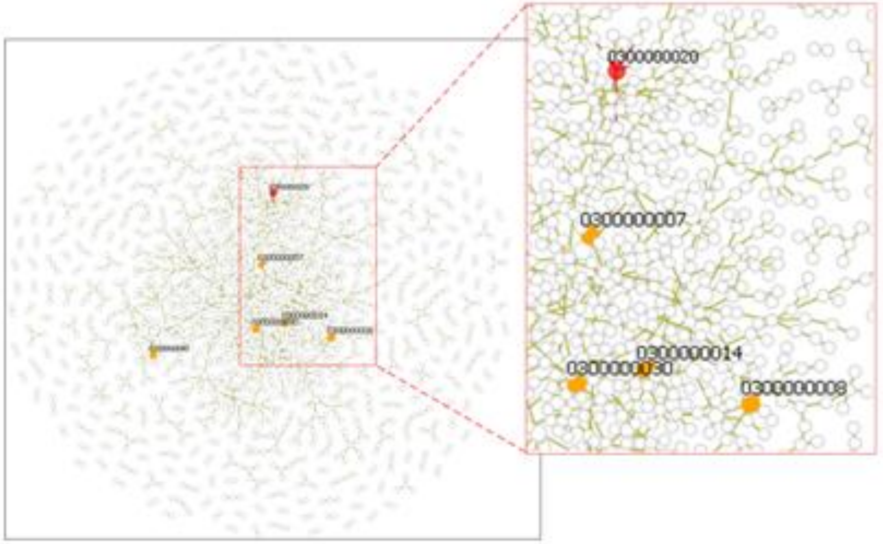
Security architecture for femtocells

- Form a peer-to-peer network of virtualised femtocell devices equipped with
  - Sensors for monitoring and anomaly detection
  - Filters for mitigation

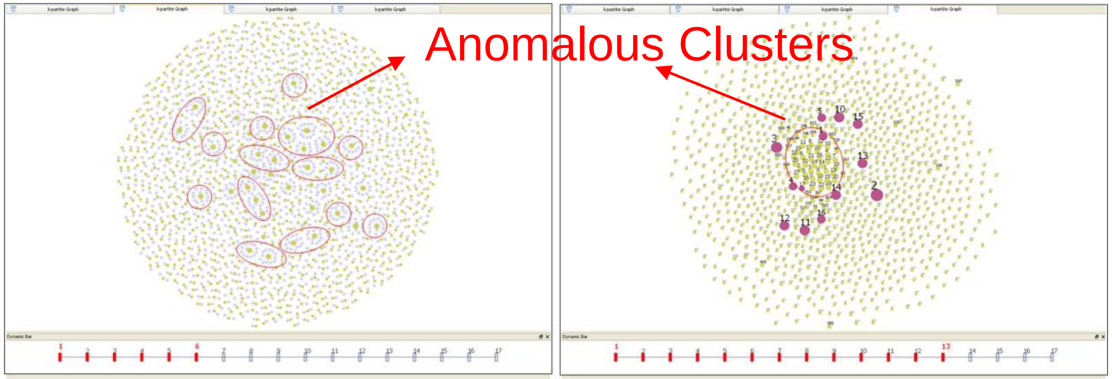


Visual Analytics for the Mobile Network Operator

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



- Multiple coordinated views facilitate the visual analytic exploration of multidimensional datasets, allowing a multifaceted perception and the discovery of any hidden attributes


Anomalous Clusters

Thank you for your attention!

Imperial College London

INFORMATION TECHNOLOGIES INSTITUTE
centre for research & technology - hellas

TELECOM ITALIA
INFORMATION TECHNOLOGY

TU berlin

HISPASEC

COSMOTE

NEMESYS

www.nemesys-projec.eu

COOPERATION