Device Monitor for Android

Botnet hunting on Android mobile devices

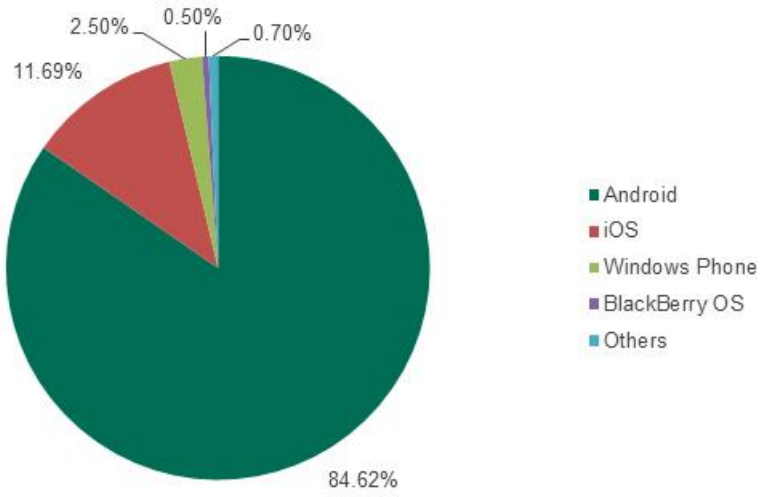
ales.cernivec@xlab.si, @alescernivec

ECSPI Awards: additional material to support the nomination

XLAB d.o.o. / Pot za Brdom 100 / SI-1000 Ljubljana / Slovenia
tel. +386 1 244 77 50 / fax +386 1 244 77 70 / e-mail: info@xlab.si
www.xlab.si

Cyber threat on mobile devices

- Trojan-SMSes
- Risky permissions / RiskTools
- Trojans / data leakage

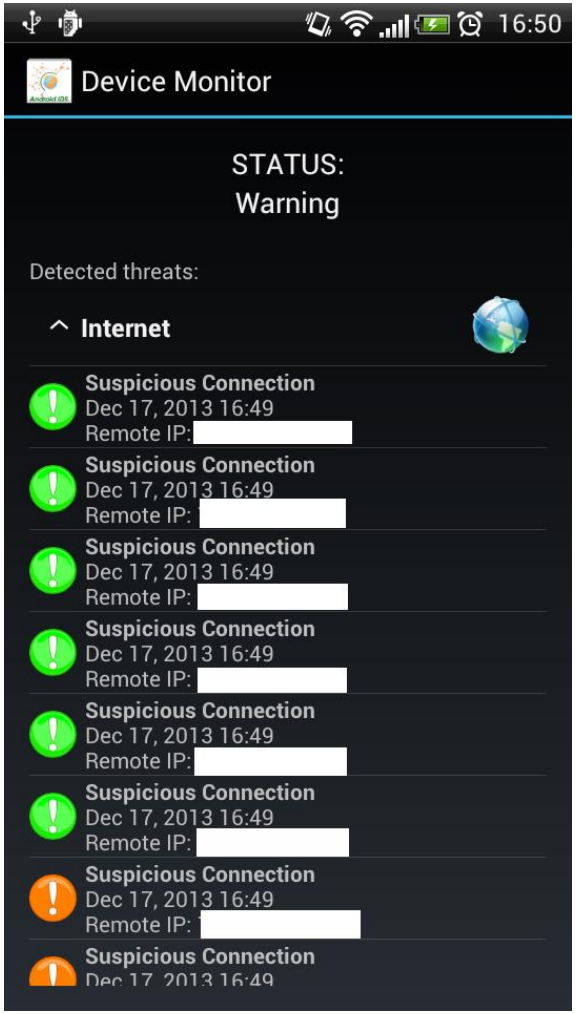


Distribution of mobile operating systems in Q2 2014. Source: IDC

We can save the world!

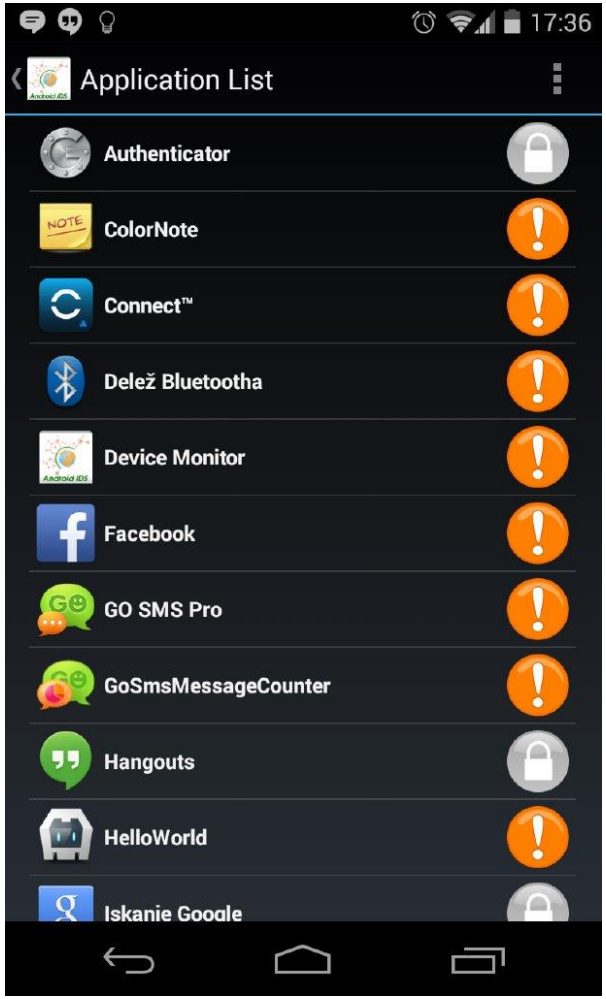
Phishing

- See when you stumble upon a suspicious URL
  - Prevention
  - Notification



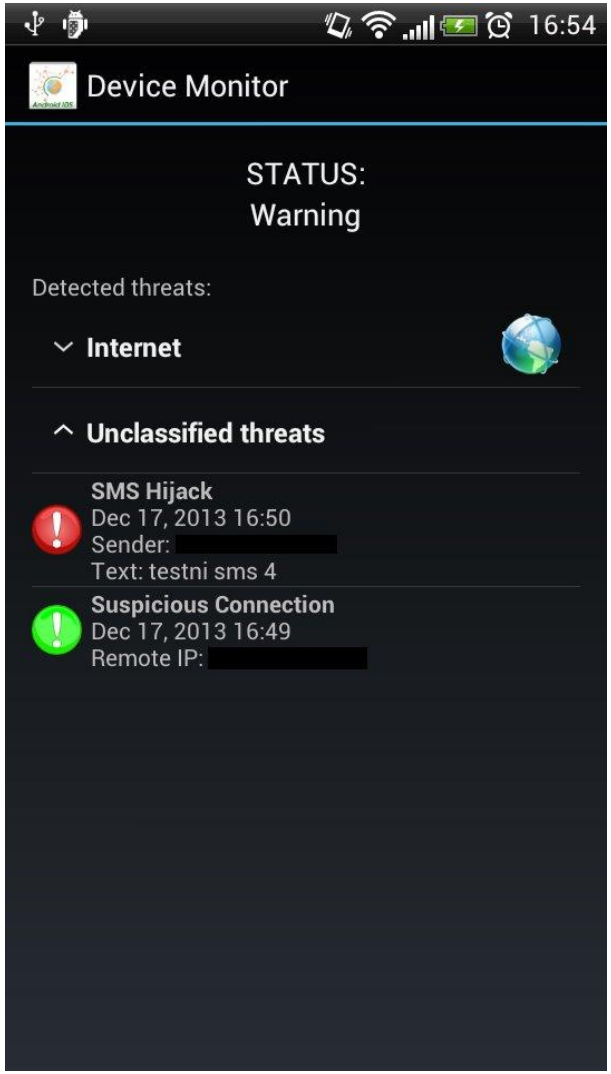
Malware

- Detection of malicious and suspicious applications
  - Notification



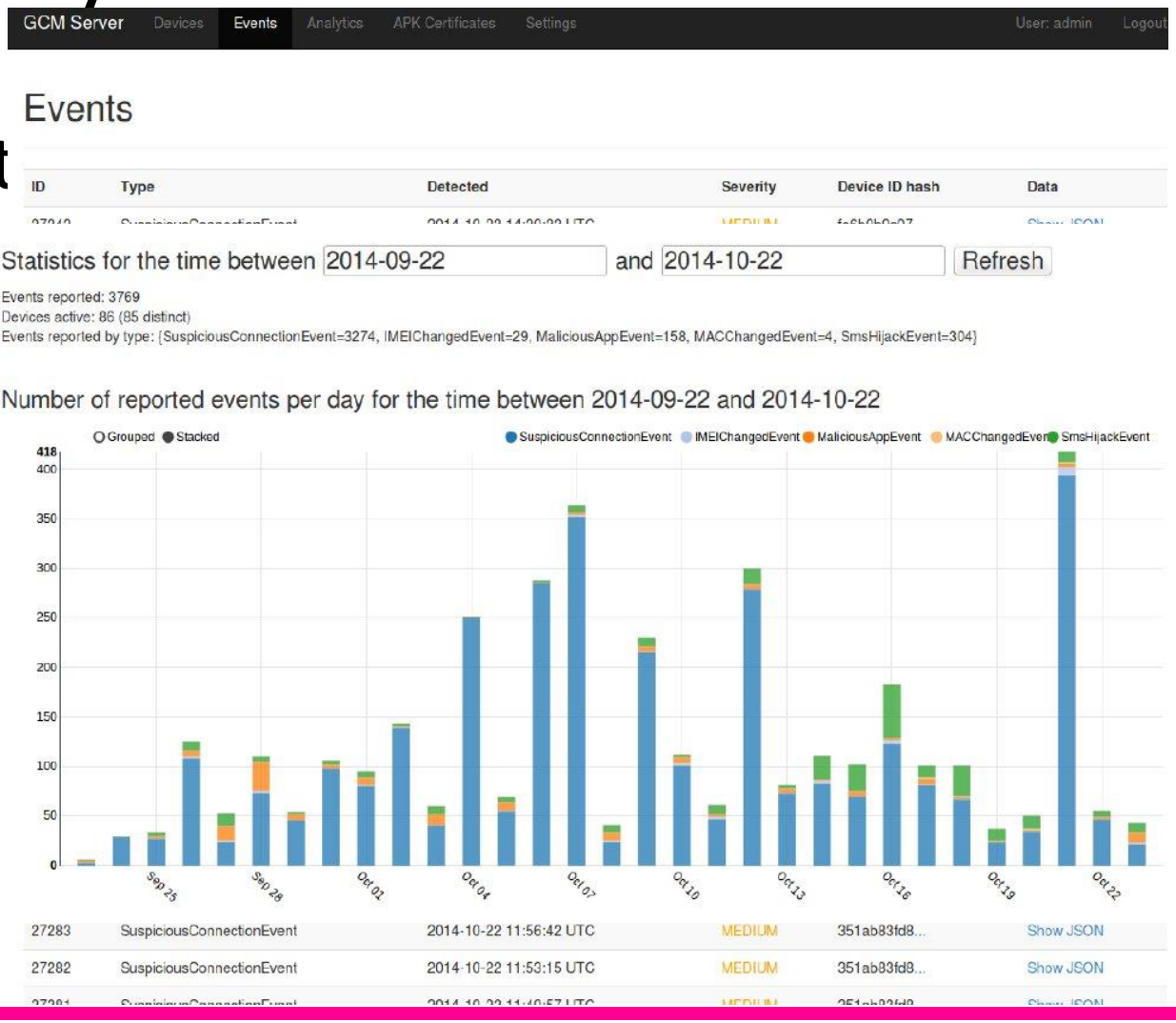
Spam

- SMS hijack detection
  - Notification



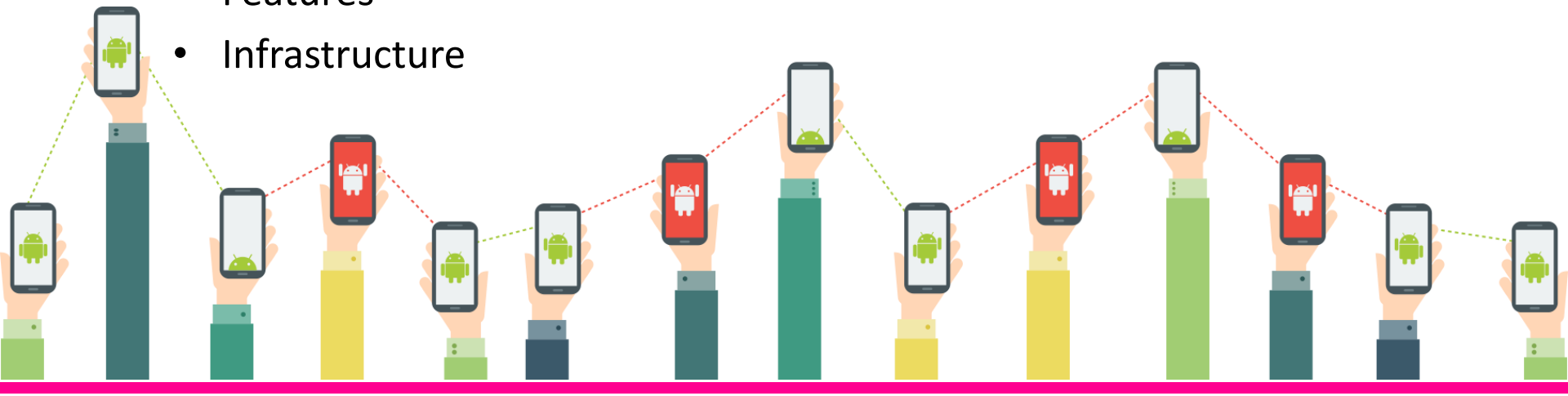
And your boss will know that!

- Wait
- Not



Content

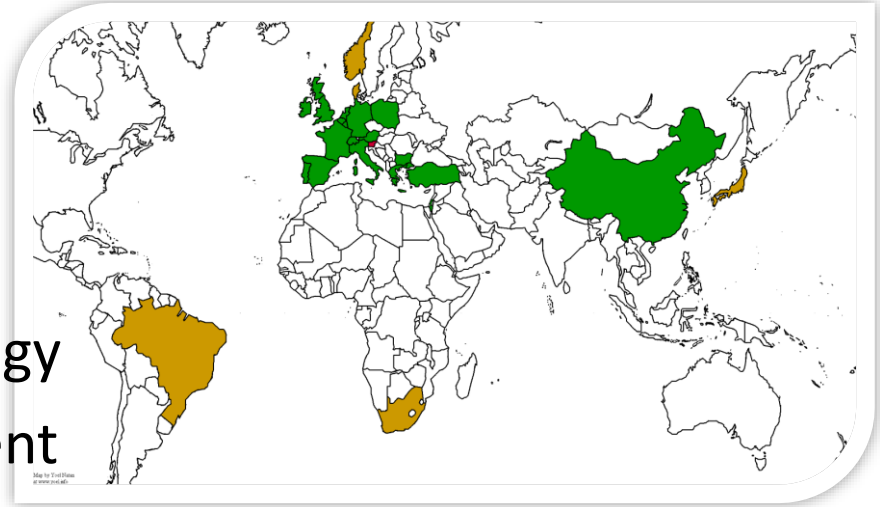
- Introduction
- Android malware
  - Building a botnet
  - Known exploits
- Device Monitor
  - Features
  - Infrastructure

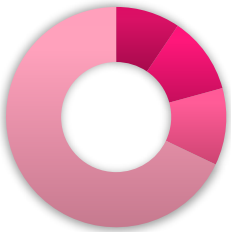


Introduction – about the company

XLAB

- Founded in 2001
- Strong research base
- Cloud services, cloud technology
- Mobile application development
- Application level security, best practices
- Security on mobile devices





PhD

MsC

Post graduate students

BsC

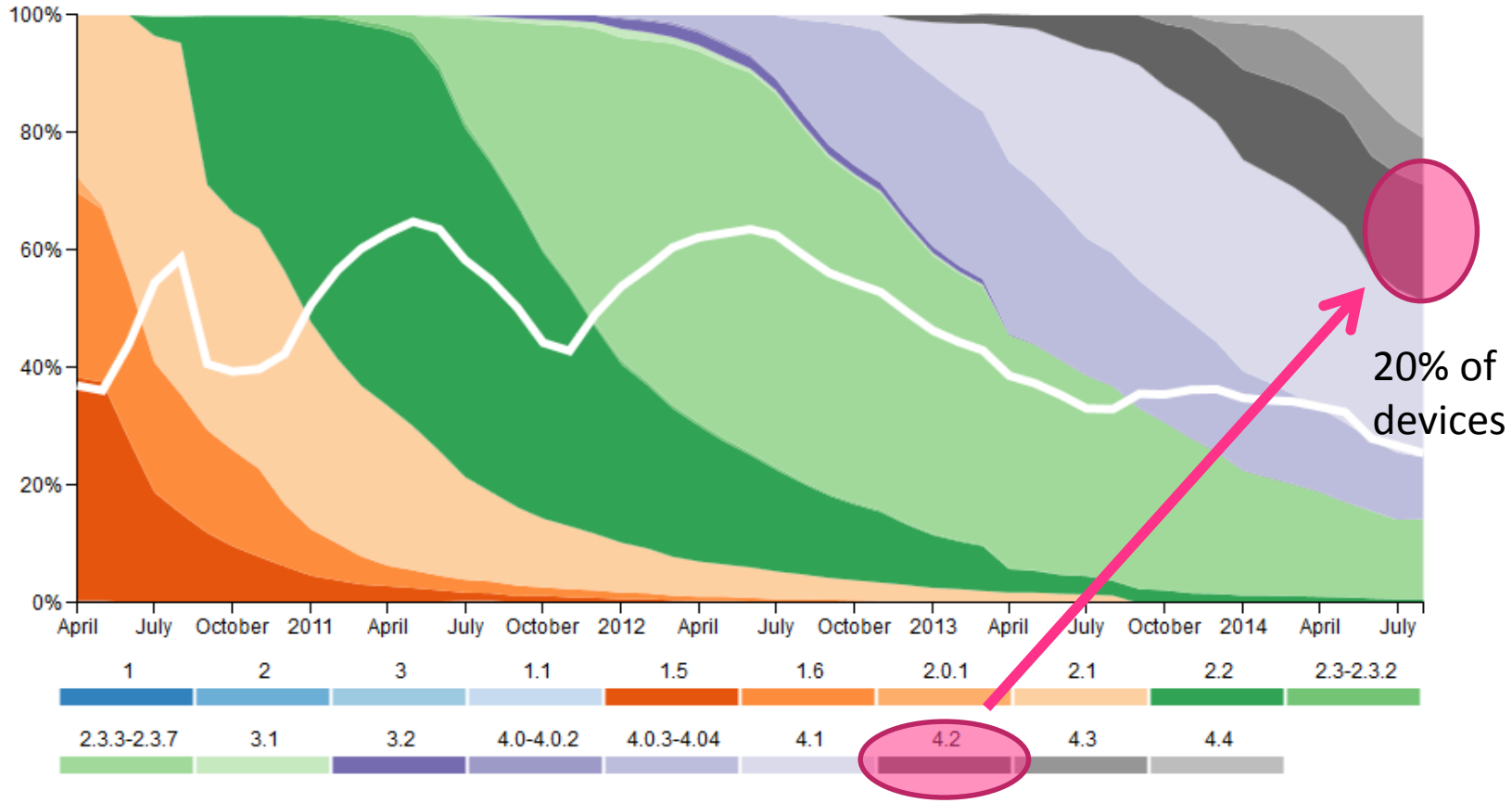
Univerza v Ljubljani

Institut "Jožef Stefan" Ljubljana, Slovenija

Building a mobile botnet

- Choose a device model, API version
  - 4.2
- Find weaknesses
  - Master-key, SMS hijack
- Use them to infiltrate the code
  - Drive-by-download
- Run the code „in stealth mode“
  - Commands
  - CC communication
- You could potentially control at least 20% of Android devices

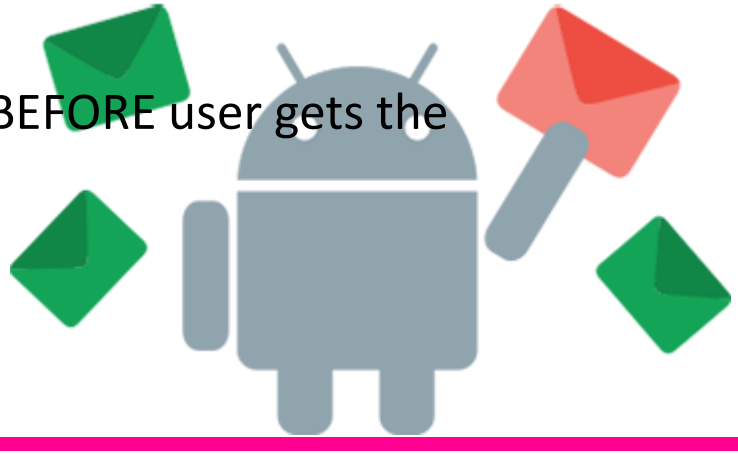
Android API fragmentation



By OpenSignal

Known exploits

- Master-key
  - Pretend to be A but installing the app as B
  - Repackage the application with different source
- Fake ID
  - A security hole within the OS‘ libraries
  - Internet browser‘s plugins
- SMS hijacks
  - app capable of discarding SMS messages BEFORE user gets the notification



Introduction – Device Monitor

- Mobile application - sensor
- Detection
  - Outgoing connections to malicious resources
  - Detection of SMS hijacking
- Application scanning
  - Classification based on app's permissions
  - Master-key, Fake ID
- Prevention to access known malicious resouces
  - Dedicated, corporate networks

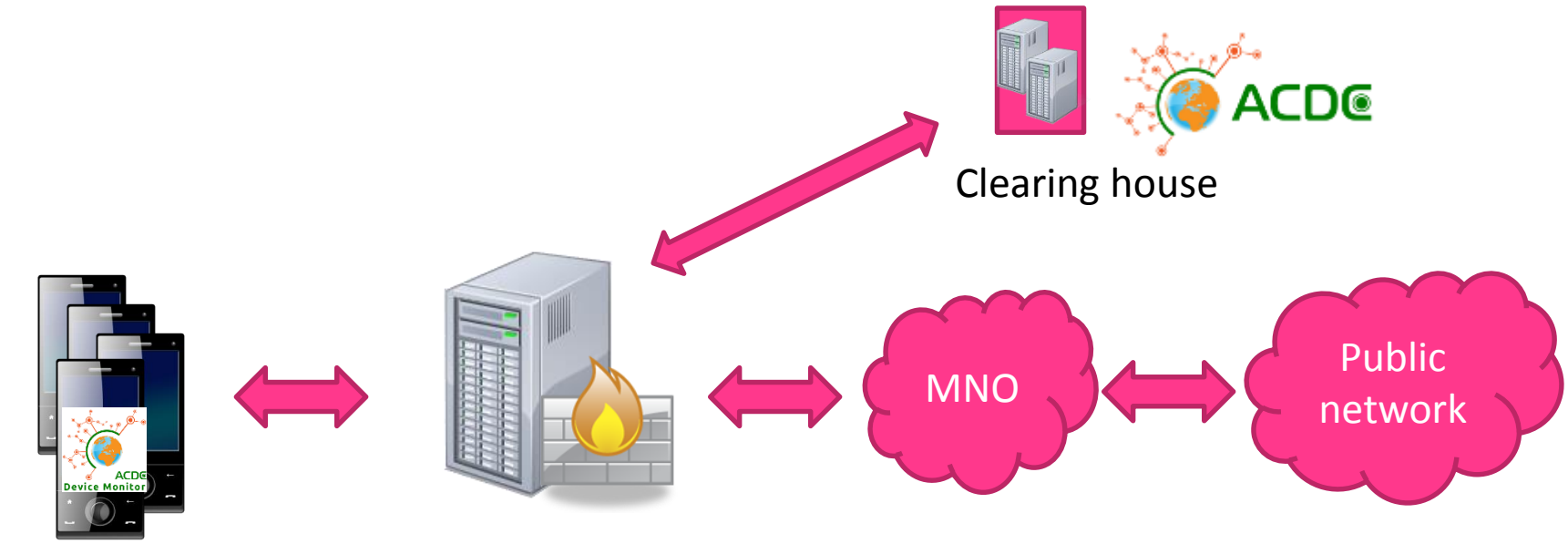
Device Monitor cont.

- Notifies the user and central server when
  - Detected malware is installed
  - Connecting to potential malicious end-points
- Dedicated infrastructure for data aggregation
- Notifies the user about suspicious events (logs)

Device Monitor features

- Network sensor on mobile device queries **the appliance** for
  - URL status
  - list of rogue IPs which is provided by the appliance
  - Sync detections
- On Wi-Fi networks:
  - Email clients:
    - ✓ rogue URLs **recognized, access prevented**
  - Other applications:
    - ✓ rogue destination IPs, **recognized** when connection is made
    - ✓ Connections dropped if so configured on the Suricata IDS
- On Mobile networks:
  - Email clients:
    - ✓ rogue URLs, **recognized**, **access prevented**
  - Other applications:
    - ⊗ rogue destination IPs **cannot be recognized nor access prevented** since MNO's proxy is visible as destination IP

Infrastructure

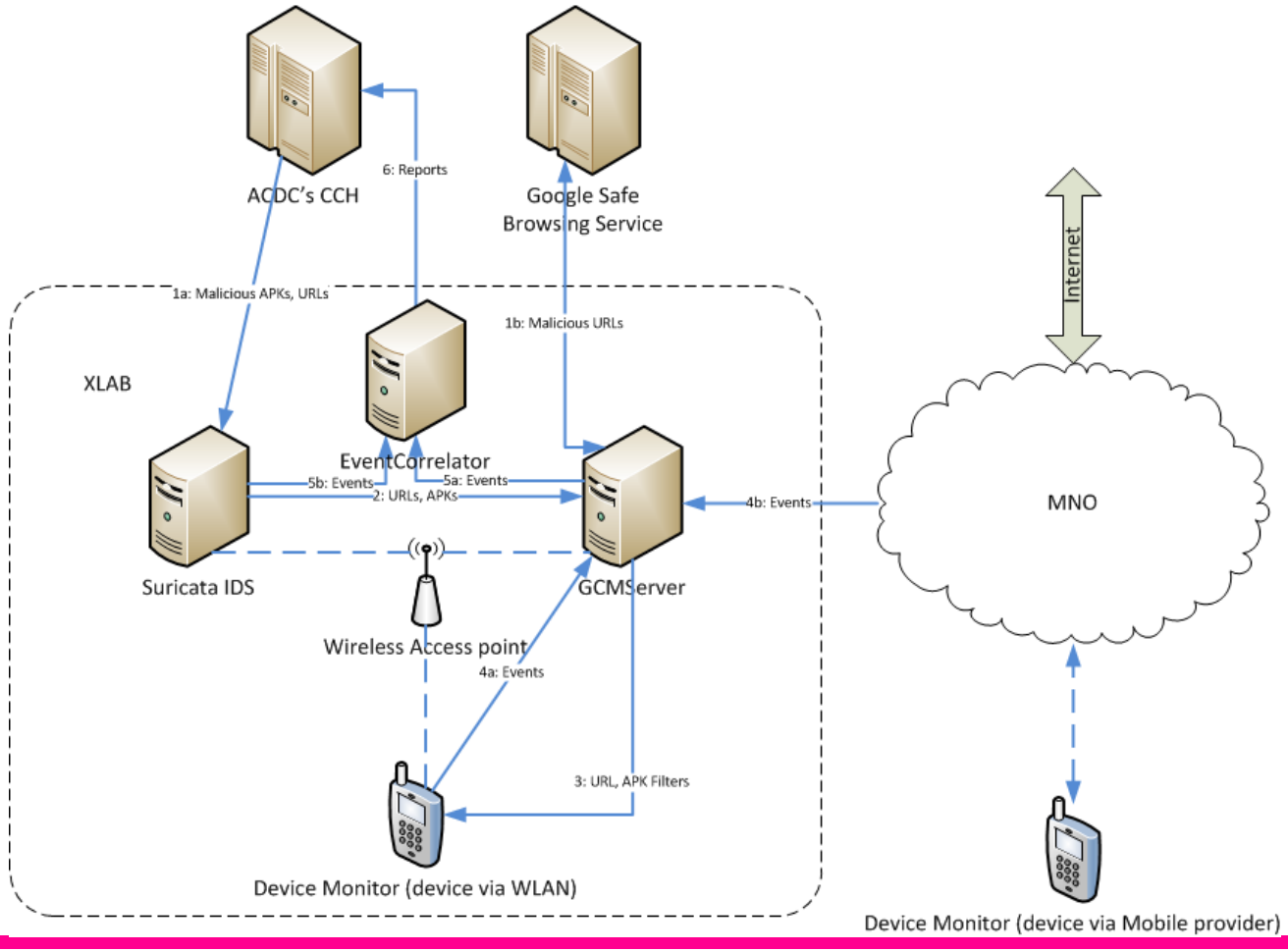


Infrastructure cont.

Solution consists of

- Mobile application
  - Device Monitor
- Appliance
  - IDS
  - EventCorrelator (analytics)
  - Message bus
  - GCMServer, RabbitMQ server

Infrastructure cont.



Device Monitor features recap

What can be detected within MNOs or dedicated network (AP) with Device Monitor?

	App classification	SMS hijack	Master-key	Fake ID	UrlBrowse	Suspicious connection	Prevention to access
MNO							
Wireless AP							

Available on Google Play Store

- https://play.google.com/store/apps/details?id=eu.acdc.xlab.devicemonitor
- Demo videos: http://x.k00.fr/zmprk