

CominLabs Kharon

Android malware analysis

Valérie Viet Triem Tong

together with Jean-François Lalande – Thomas Genet

CominLabs days 2018

Inria CIDRE & CELTIQUE

CentraleSupélec – Inria – Insa CVL - Université de Rennes 1

Inria



CentraleSupélec



CominLabs Kharon project

Cominlabs project 2015-2018 fouding for 1 year engineer, 1 phd student

Automatic dissection of Android malware

- How a malware contaminates the operating system ?

By information flow monitoring

- How to identify and trigger the malicious code ?

By static and dynamic analysis

- How to replay attacks and explore the malicious code ?

By highlighting all the experiments artifacts

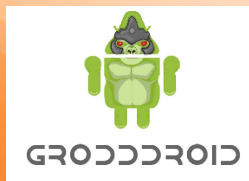
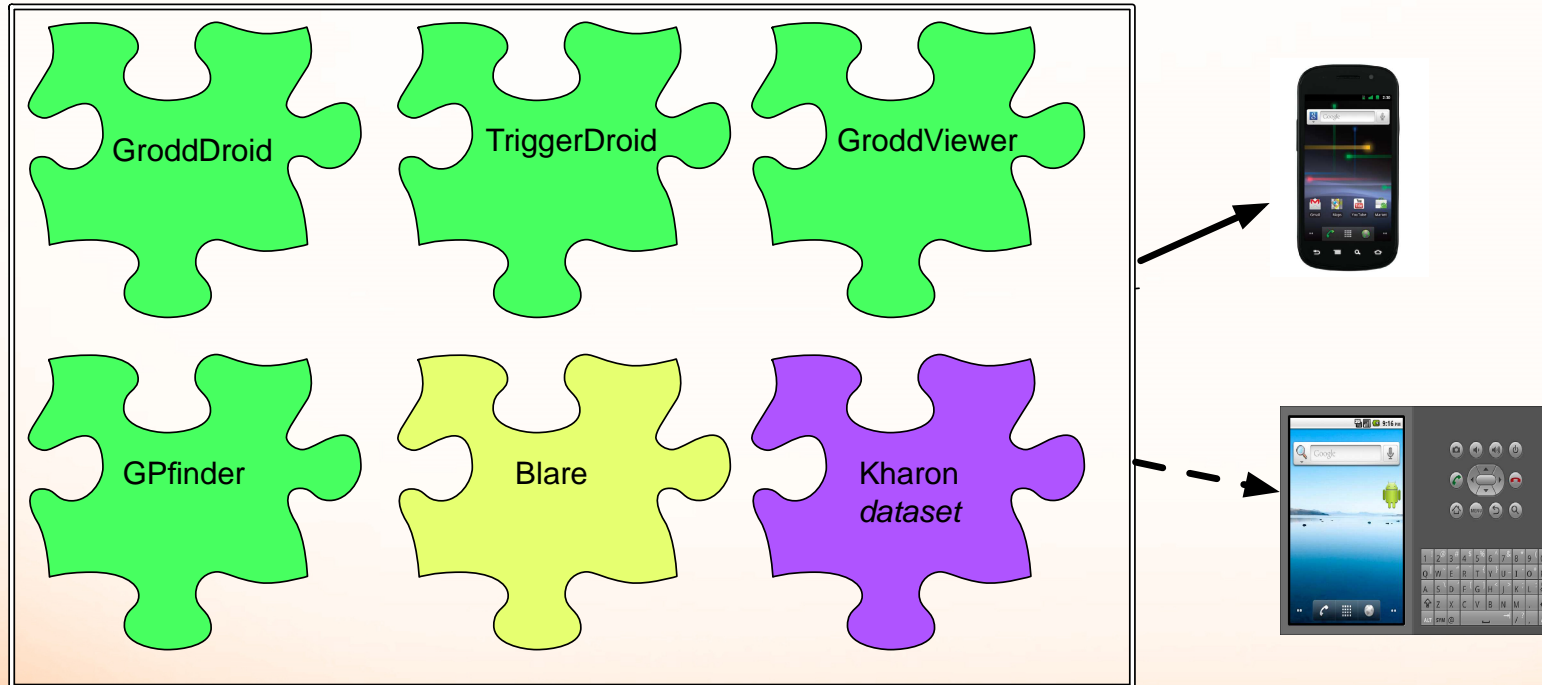
More than 23 people have worked for Kharon :

- 2 phd
- internship/projects

General overview of the Kharon platform @LHS



Analyse your Android Application in appropriate conditions



An online analysis platform

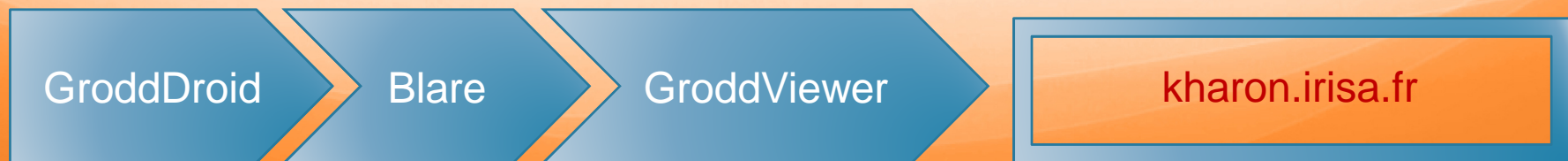
hosted by the High Security Laboratory
LHS @ Inria Rennes

Android Malware

- Send messages to premium numbers
- Install ads
- Take the control of the phone
- Ransom the user
- Mine cryptocurrency

With smart techniques to evade static and dynamic analysis

**An important scientific challenge :
being able to trigger a malware *on demand***



04:23

Current state information

Your personal documents and files on this device have just been crypted. The original files have been deleted and will only be recovered by following the steps described below. The encryption was done with a unique generated encryption key (using AES-256).

Data will be lost after	Number of encrypted files	The cost of the key for decryption
23h	14	0.0130 BTC

Important information

Your personal files are encrypted!

To decrypt files you need to obtain the private key. This means the encrypted files are of no use until they get decrypted using a private key stored on a server. The server will destroy the private key after a time specified in this window. After that, nobody and never will be able to restore original files.

To obtain the private key which will decrypt files, you need to pay the amount you see at the top of the screen. Without this key, you will never be able to get your original files back.

Also you can easily delete this software, but know that without it, you will never be able to get your original files back. Whenever possible then disable your antivirus app to prevent the removal of this software.

How can I pay?

Payment is accepted in Bitcoin only. For more information, click 'Where to get Bitcoin'.

Payment information

Please make payment to this Bitcoin address or you can scan QR-code to get Bitcoin-address easily. The operation is complete if there are 3 confirmations.

Android Malware

- Send messages to premium numbers
- Install ads
- Take the control of the phone
- Ransom the user
- Mine cryptocurrency



With smart techniques to evade static and dynamic analysis



**An important scientific challenge :
being able to trigger a malware *on demand***

GroddDroid

Blare

GroddViewer

kharon.irisa.fr

GroddDroid

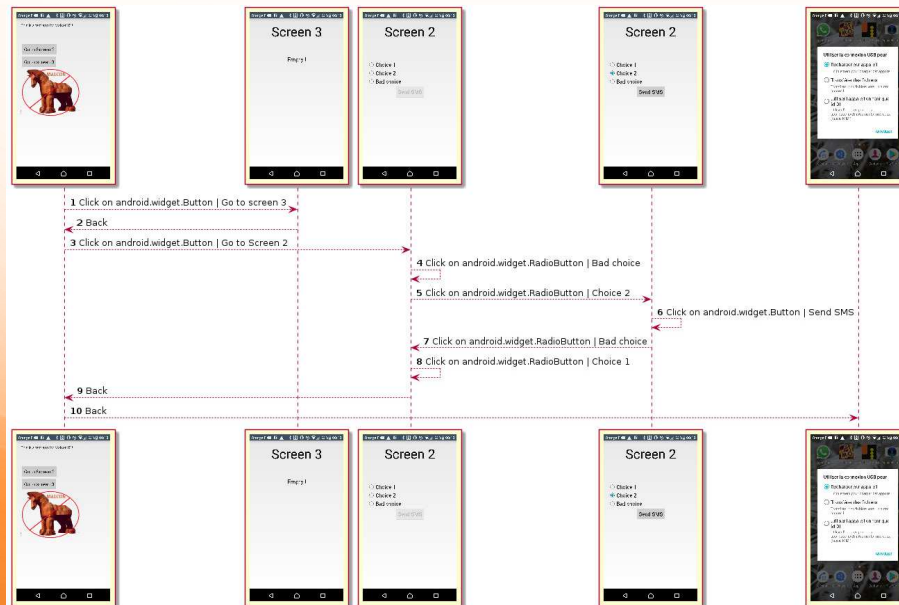
Blare

GroddViewer

kharon.irisa.fr

GroddDroid

- Explores the different screens
- Locates the suspicious code
- Forces suspicious code
- Executes, observes, visualizes



A. Abraham (internship 2015)
 Mourad Leslous (Phd 2015 – 201-)

with the help of students@CentraleSupélec

Best paper Malcon'15
Malcon'17

GroddDroid

Blare

GroddViewer

kharon.irisa.fr

GroddDroid relies on a prior static analysis

- 1 Computes the inter-procedural control flow graph with implicit flows
 - 2 Locates suspicious basic blocks
 - 3 Exhibits an execution path from an entry point towards suspicious code
- 1 Can force the execution paths

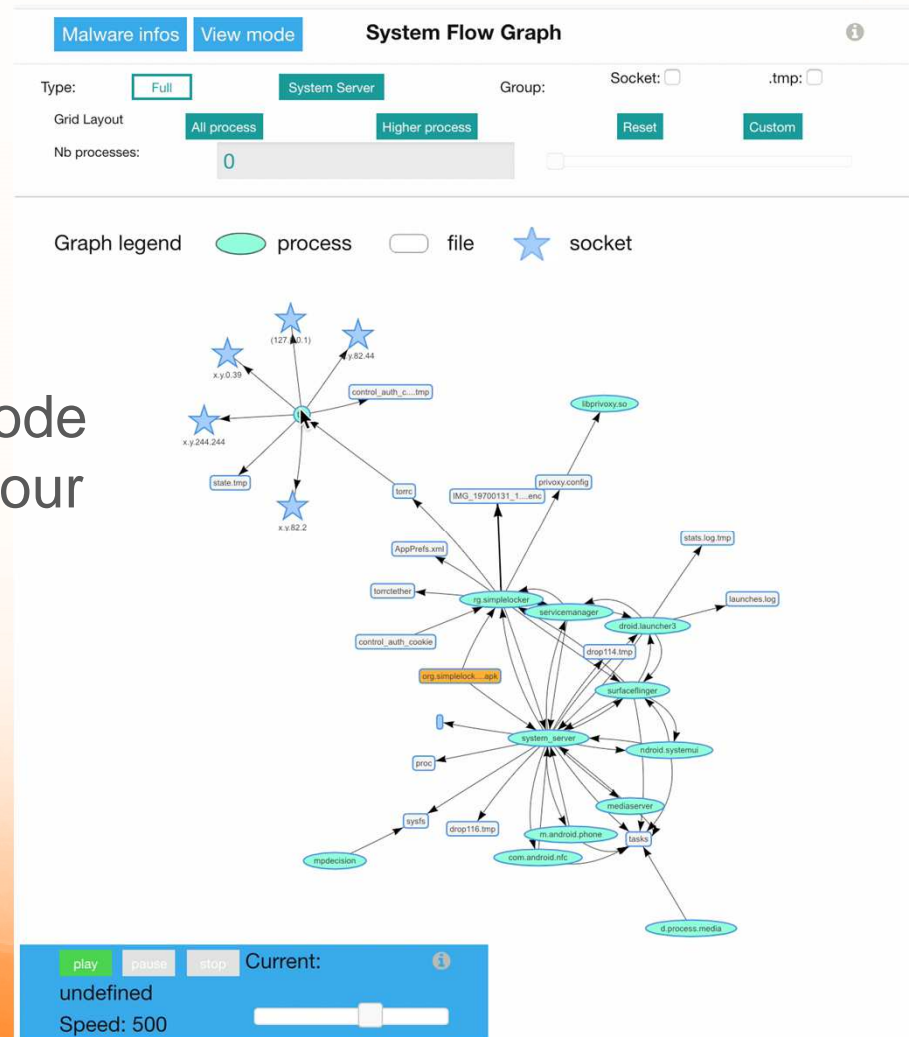


42% of malware are hidden behind implicit paths
95% of them have no alternative explicit paths



kharon.irisa.fr

- Visualizes together code and behaviour



- Allows to replay an attacks, explores the code

The Kharon platform at kharon.irisa.fr

with the help of S. Campion SED Inria



The screenshot shows a web browser window with the title "Kharon - Mozilla Firefox". The address bar contains "kharon.irisa.fr". The main heading of the page is "Kharon - Android Malware Analysis". Below the heading, there are three navigation tabs: "Experiments", "Work in progress", and "Devices". The main content area features a large blue button labeled "Parcourir..." with the text "Aucun fichier sélectionné." next to it. Below this is a smaller blue button labeled "Upload". Underneath, the text "API:" is followed by "HTTP POST analysis is available on this server, here is a curl example :". A code block contains the following command:

```
curl -X POST -F file=@/some/file -F scenario=@/some/optional/scenario -F 'model=optional_mobile_model_name' -H "Accept: application/json" 'http://kharon.irisa.fr' -u username
```

 At the bottom of the page, there is a dark, rectangular area that appears to be a placeholder or a redacted image. The browser's status bar at the very bottom shows system information: "me 2Pw | 162.2 GiB | W: (75% at jwifl-interne) 131.254.65.253 | E: down | SAT 18.85% 06:17:58 | 8-49 | 2018-05-28 11:25:55".

Issues from the Kharon project



Software and public dataset

- The Kharon dataset of fully reversed and documented malware
- The Kharon platform hosted by the High Security Laboratory kharon.irisa.fr
- GroddDroid, GroddView, GPFinder ,TriggerDroid a collection of tools

Publications

- **Best paper** MALCON 15, CSCLOUD 16, LASER 16, MALCON 17, SECRIPT 17, RESSI 18

European cooperation

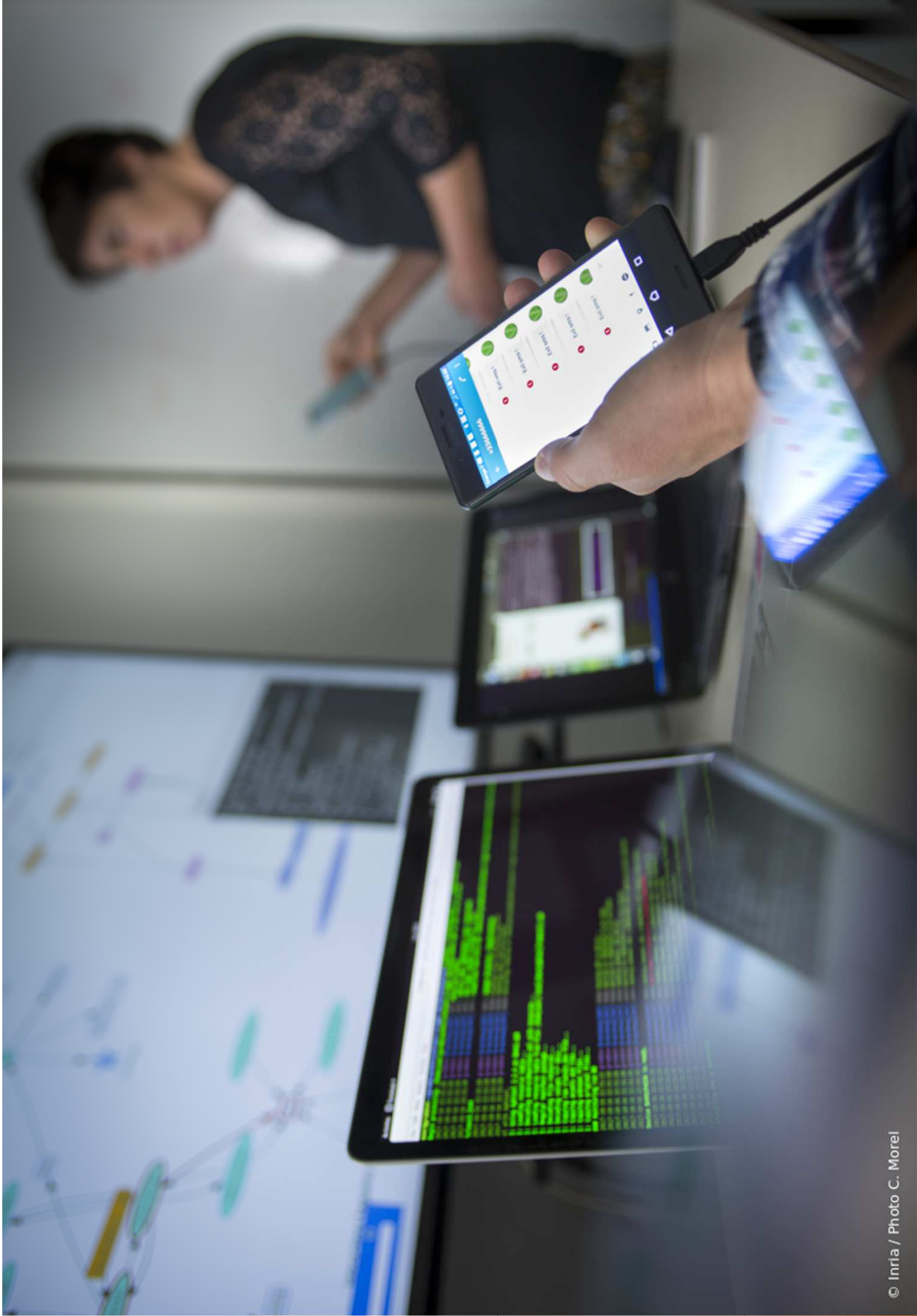
Alexander Prestchner - TU Munich and Lorenzo Cavallaro - Royal Holloway Univ.London

Dissemination

- Educational: Summer school Cyber In Britain 16, Cyber In Berry 17, Online courses
- Popularization: article in Interstices, « Fete de la Science », demo @LHS @FIC

In the future ?

- **An engineer will be recruited to maintain the platform**
- **We start a cooperation with Airbus**



© Inria / Photo C. Morel



KHARON PLATFORM - GRODDROID SOFTWARE

