CominLabs Kharon

Android malware analysis

Valérie Viet Triem Tong

together with Jean-François Lalande – Thomas Genet

ComінLabs days 2018

Inria CIDRE & CELTIQUE

CentraleSupélec – Inria – Insa CVL - Université de Rennes 1

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

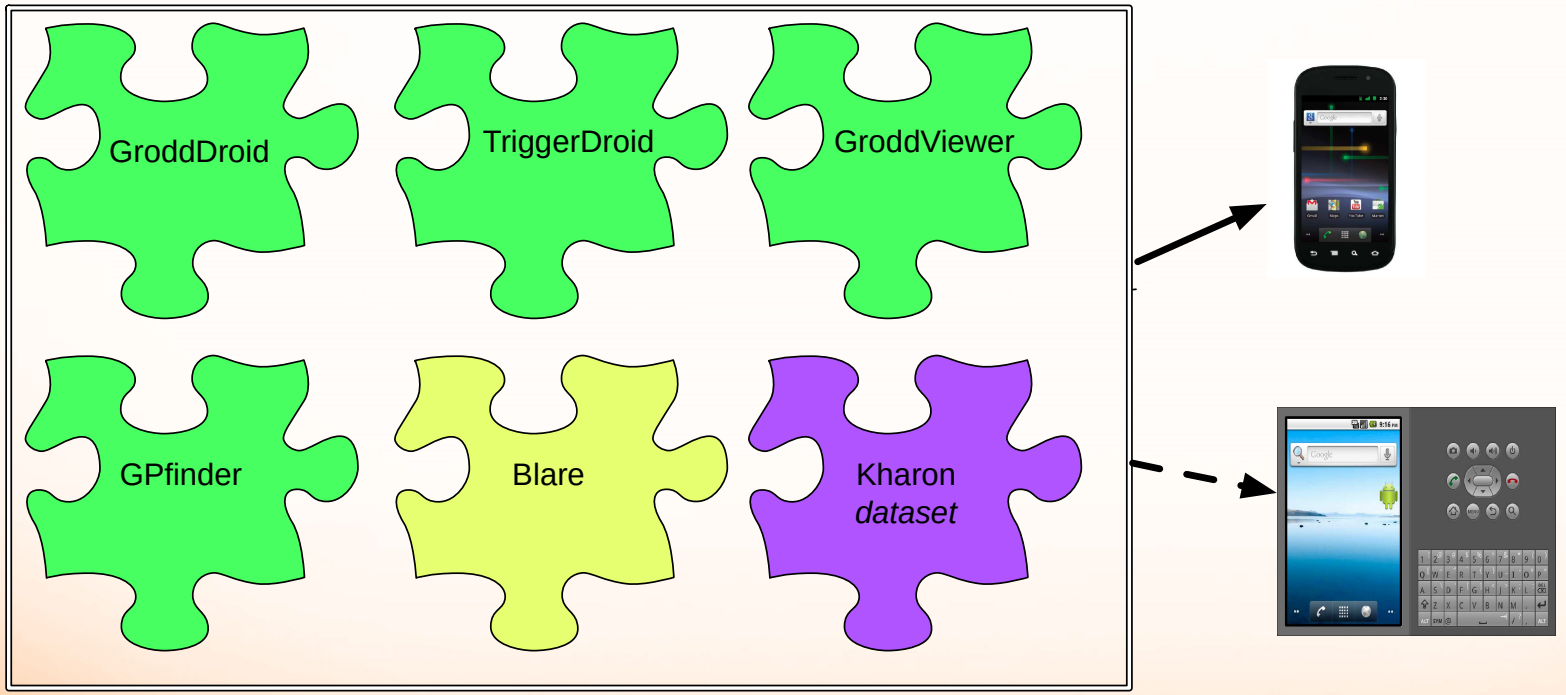
More than 23 people have worked for Kharon :

- 2 phd
- internship/projects

General overview of the Kharon platform @LHS

CominLabs

Analyse your Android Application in appropriate conditions



GRODDDROID

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*

GroddDroid → Blare → GroddViewer → kharon.irisa.fr

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*

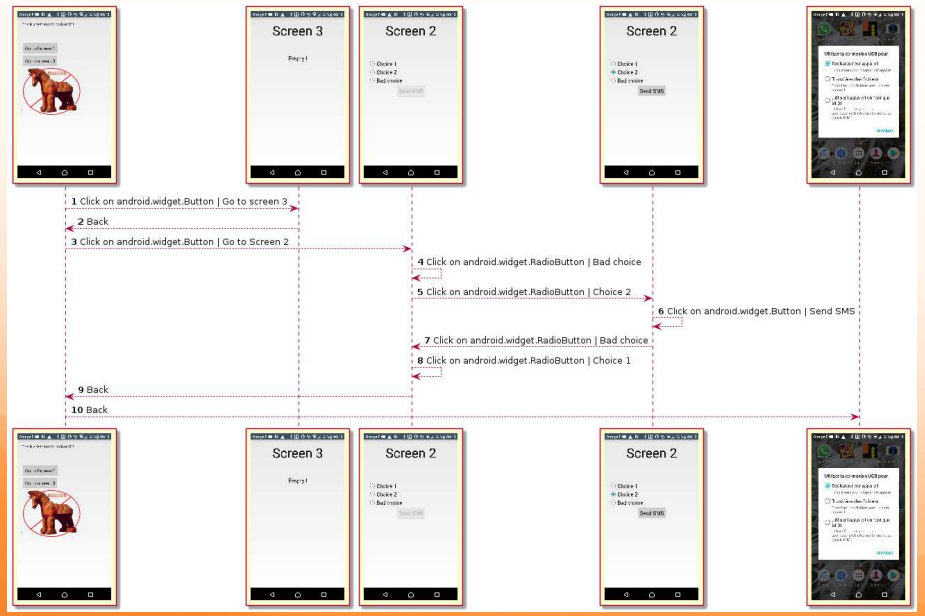
GroddDroid → Blare → GroddViewer → kharon.irisa.fr

ComInLabs

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@CentraleSupelec

Best paper Malcon'15
Malcon'17

ComInLabs

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

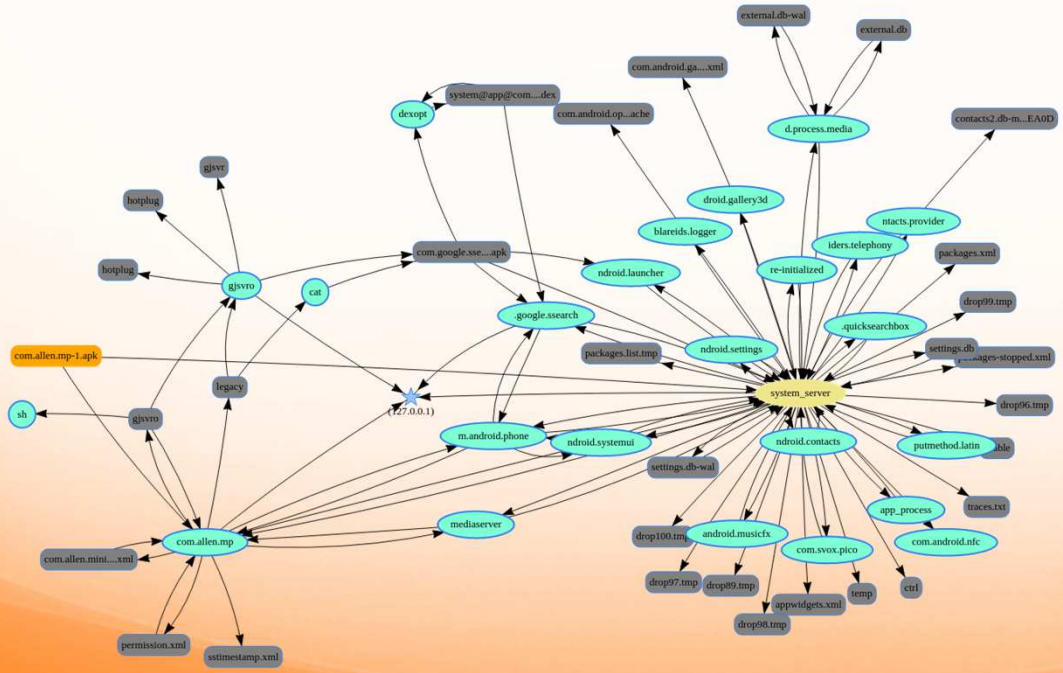
42% of malware are hidden behind implicit paths
95% of them have no alternative explicit paths

GroddDroid → **Blare** → GroddViewer

kharon.irisa.fr

Blare:

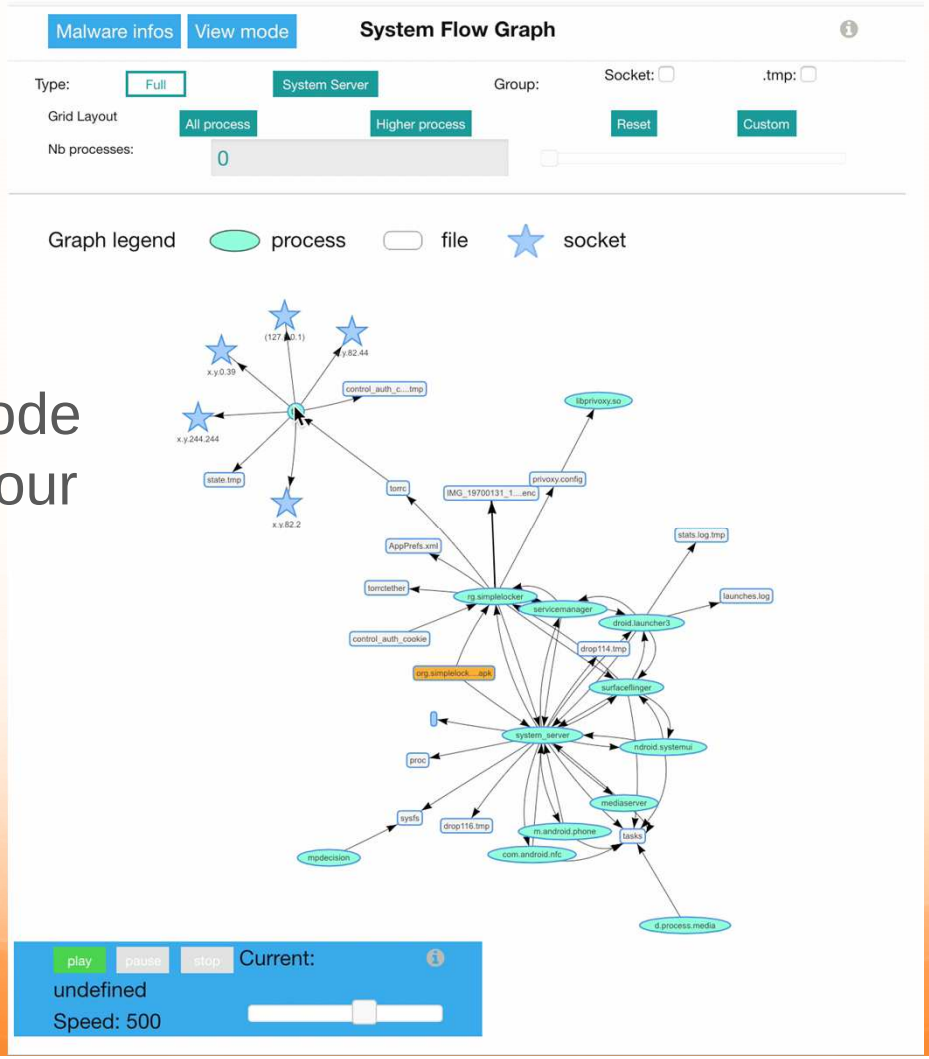
- Marks the initial file containing the malware (.apk)
- Observes information flows at the OS level



- Graphs as behavioral signatures **CS Cloud'16**
- Model of normal graphs **SECRYPT'17**

ComInLabs

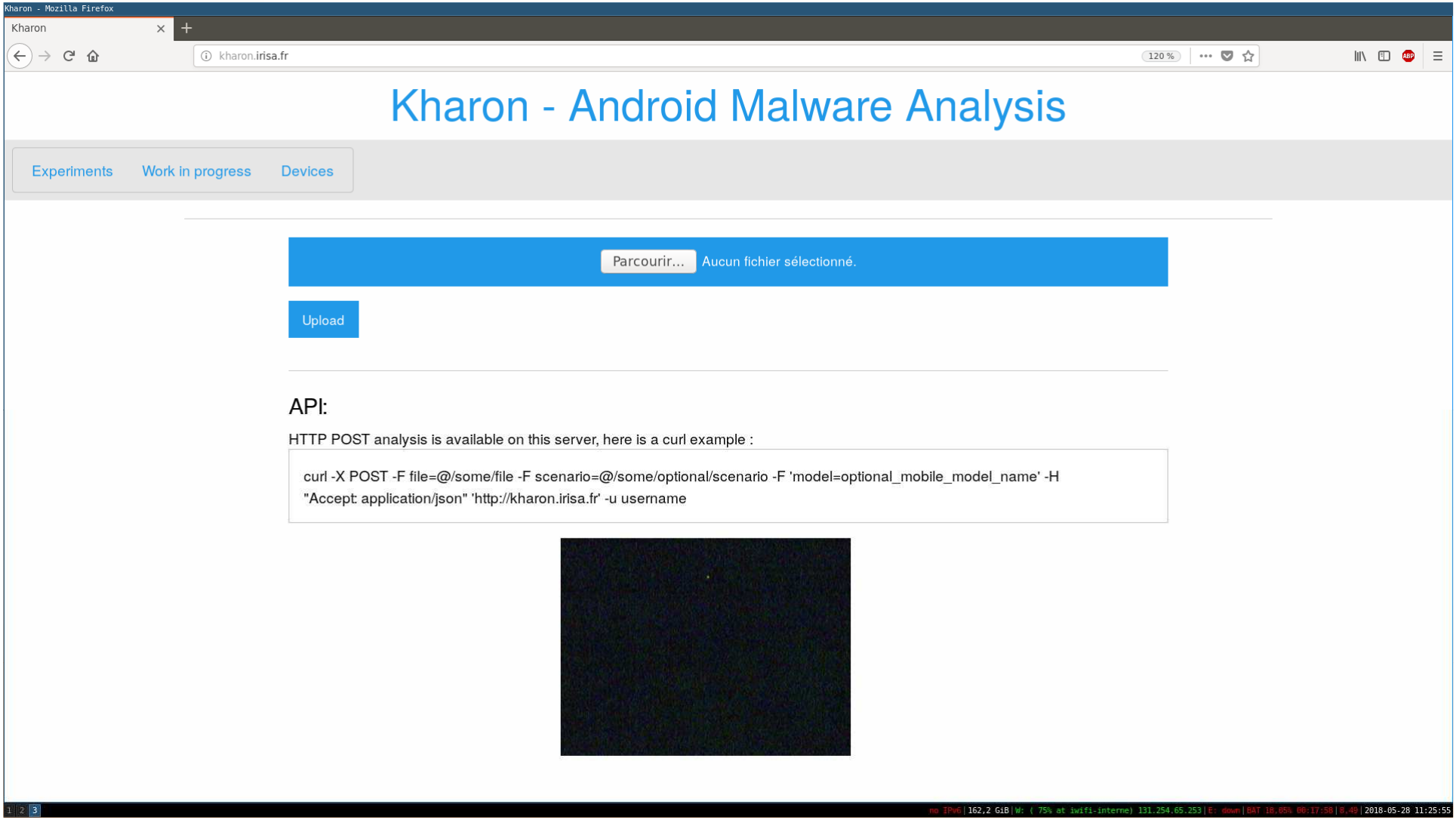
GroddDroid → Blare → GroddViewer → kharon.irisa.fr



- 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



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, SECRYPT 17, RESSI 18

European cooperation

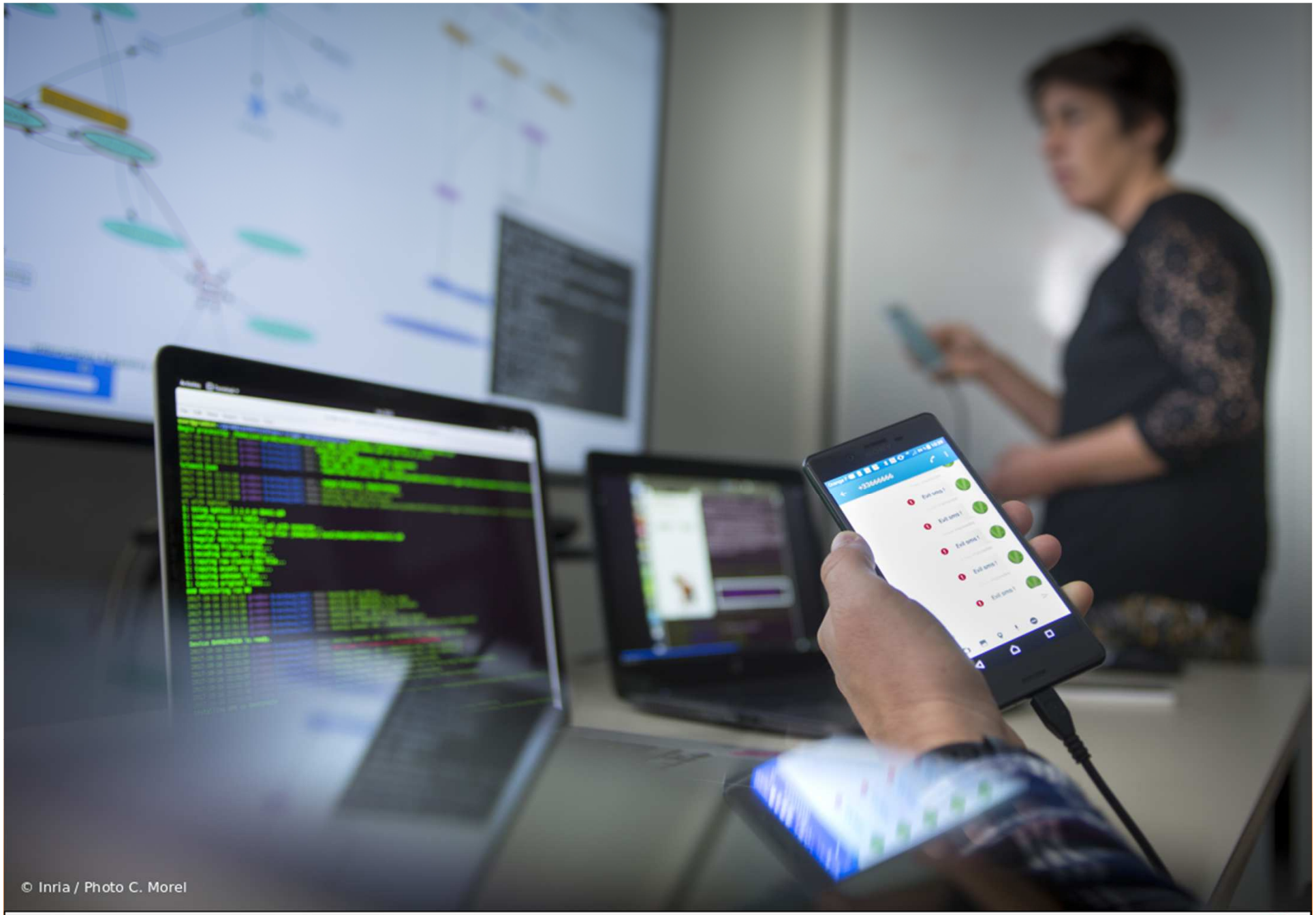
Alexander Prestchner - TU Munich and Lorenzo Cavallaro - Royal Holloway Univ.London

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 ComInLabs KHARON PLATFORM - GRODDDROID SOFTWARE CentraleSupélec UNIVERSITÉ DE RENNES 1 INSA