CominLabs Kharon project - final report
Coping with Android Malware

Valérie Viet Triem Tong
(Scientific leader)
Associate Professor at CentraleSupelec EPC CIDRE
CentraleSupelec/INRIA/CNRS/Université de Rennes 1
Rennes, France

valerie.viettriemtong@centralesupelec.fr

Jean François Lalande
Associate Professor at CentraleSupelec previously at Insa Centre-Val de Loire
EPC CIDRE
CentraleSupelec/INRIA/CNRS/Université de Rennes 1
Rennes, France

jean-francois.lalande@centralesupelec.fr

Thomas Genet
Associate Professor at Université de Rennes 1
EPC CELTIQUE
INRIA/CNRS/Université de Rennes 1
Rennes, France

thomas.genet@irisa.fr

Google Play offers more than three millions of applications (apps), and this number increases every day. Google play users have performed more than 25 billion app downloads. These applications vary from games to music, video, books, tools ... Unfortunately, each of these app is an attack vector on their Android devices. The number of applications considered malicious or risky found in the wild is constantly increasing. In this context, we have proposed the Kharon project to the Cominlabs Labex. This project has started in spring 2015.

At this moment, we had already studied Android malware, through their information flows in the operating system. We had highlighted that information flows at this level of observation, offer a promising manner to represent an attack and effects of an attack. This point of view was little studied in the literature.

The project was composed of members of the Cidre and Celtique Inria projects. Members of Celtique are experts on static analysis and have particularly studied static analysis of programs written in Java; members of Cidre have expertise in operating system security.

Goal of the project *an Online Automatic Malware Detection Platform*

The main practical outcome targeted by the Kharon project was an online platform where users can drop android applications and immediately get an understandable information flow digest, a report on detected malicious behaviors and a security policy to apply on the application to prevent such unwanted behaviors.

To reach this goal we had identified the following contributions to achieve:

1. automate the complete malware detection process,
2. propose a detection approach to classify malware and benign application with regards to what they do and not what they look like,
3. compute a compact and accurate representation of *what they do*.

Besides travel and hardware efforts, Cominlabs has granted a Phd thesis and a research engineer during one year on this project.

We have presented the final results of the Kharon project during *CominLabs Days* which was held at Inria-Rennes, from May 28th to May 30th, 2018. More than twenty people including PdD thesis with external sources of funding, master students and project students have contributed to the project. From our point of view, the Kharon project was a successful project. The project had academic, practical and educational outcomes as it is detailed in the following parts of this document. The main outcomes of the project are described on kharon.gforge.inria.fr

Scientific steps in the Kharon project

Automate the triggering of Android malware

The Kharon platform performs dynamic analysis on Android malware. These analysis are relevant only when the attacks are indeed observed during the time of the analysis. Unfortunately, malware authors can evade dynamic analysis easily, for example by delaying the attack. As a consequence, a dynamic analysis of an Android application has few chance to succeed because the attacker can implement logic bombs or hide its code in callbacks associated to events. Thus, starting the application on the smartphone would not execute the malware. For solving this problem, in the Kharon project, we have explored two directions:

- (Contribution 1) Automate the interactions with an Android application to mimic a real user.
- (Contribution 2) Automatically trigger the execution of Android malware payload, using intensive inspection of the code of the application and minimal modifications of its code for the runtime analysis.

Contribution 1 We have developed GroddDroid [1] a tool that manipulates a graphical interface of an Android application. GroddDroid recognizes buttons, check boxes, text boxes. GroddDroid is able to trigger these graphical elements to run methodically explore the activities of an Android application. GroddDroid was developed by Adrien Brunelat and Adrien Abraham (master students hired on the project with external sources of funding (CentraleSupelec).

Contribution 2 Mourad Leslous was the Phd student founded by the project (Phd 2015-2018). His main research topic was the automatic triggering of Android malware payload. He has exposed the hidden suspicious behaviors of Android application at runtime despite the static and dynamic evasion techniques that Android malware tends to use. His main contributions are:

- Design and implementation of GPFinder [2] that takes an Android application (possibly malicious) as input, generates an interprocedural control flow graph taking into consideration the Android framework properties, and finds all execution paths that lead from entry points (the methods that may start the code of the application) to suspicious code locations (the place where the attacker puts the payload).
- Design and implementation of TriggerDroid (the article will be submitted in early 2019) that triggers the suspicious code locations and can reveal malicious behaviors of the application.

Visualizes the analysis results

From a general point of view, an analysis takes as input an apk file and outputs a huge number of logs. These logs describe the executions paths, the interactions with the application, the effects of the attack on the operating system. We developed tools which build comprehensible and synthetic presentations for these logs. Our tools help human expert to understand and exploit the logs while analyzing a malware sample.

Contribution 3 In the Kharon project, we put efforts to produce synthetic and comprehensible representations of these logs to give usable tools to the human expert. A typical example of an analysis is available on kharon.gforge.inria.fr/dataset/malware_SimpLocker.html At this time all the efforts on visualization have led to the tool GroddViewer which is still under development. GroddViewer has been developed with the help of students of INSA Centre Val de Loire.

Automate the complete malware analysis process

Radoniaina Andriatsimandefitra has joint the Kharon project as research engineer during one year[1]. He has built an architecture to perform analysis on collections of malware. The first version of the deployed platform was relying on the customizable platform Irma from Quarsklab. The second version has been implemented with the help of SED services from Inria (Sébastien Campion), independently from Irma.

Contribution 4 The Kharon platform is hosted by the High Security Laboratory at Inria Rennes. It is available on kharon.irisa.fr. For now, access to the platform is restricted to authorized members but in the future, we plan to enhance the platform and widen the access. An analysis of an application performed on the Kharon platform involves:

1. Preparation of a real smartphone to offer a clean execution context (restauration of a fresh Android image), installation of (Andro)Blare the information flow monitor.
2. Static analysis of the application to locate the suspicious code and highlight execution paths towards the suspicious code.
3. Dynamic analysis on real Android device driven by GroddDroid.
4. Dynamic analysis on real Android device driven by TriggerDroid if necessary.
5. Visualization of the results of an analysis.

Lead sound experiments

During the project we need to verify or tests some of our hypothesis on real Android malware. If some hypothesis are easy to verify, some others need a important effort of reverse-engineering. During the project, we spent a long time to reverse and document samples in order to constitute a representative malware dataset. This dataset contains for instance spyware, an aggressive adware, two ransomware samples, a data-eraser, a rootkit, a remote access tool and will soon contain a cryptominer. We have presented this dataset on a publication at the Learning from Authoritative Security Experiment Results (LASER) workshop co-located with the Symposium on Security and Privacy (S&P) [3]. The documentation and analysis of the malware are available on kharon.gforge.inria.fr/dataset/index.html

[1] Radoniaina Andriatsimandefitra is now working at Sekoia as technical expert in cybersecurity.

Academic outcomes

Results obtained in this project were presented in

- **International Conferences**
  - **Keynotes**
    - Jean-François Lalande was invited to give a talk on *Android Security, examples of malware* at the third edition of the International symposium on information system security (CISSI 2015) [4]
    - Valérie Viet Triem Tong was invited to give a talk on *Behavioral Signatures of Malware using System Flow Graph* at the third edition of the International symposium on information system security (CISSI 2015)
    - Jean-François Lalande was invited to give a talk on *Challenges for Reliable and Large Scale Evaluation of Android Malware Analysis* at the International Workshop on Security and High Performance Computing Systems, Orleans in 2018. [5]
    - Jean-François Lalande was invited as a keynote speaker at the conference SecITC (International Conference on Information Technology and Communications Security). He gave a talk untitled "Android Malware Analysis: from technical difficulties to scientific challenges" [6]
  - **Articles**
    - The first version of automatic triggering (GroddDroid software) has received the *Best paper award* at the 10th International Conference on Malicious and Unwanted Software [1]
    - A detection of malware based of information flows was published at the second IEEE International Conference on Cyber Security and Cloud Computing [7]
    - A model of normal information flows for Android applications was presented at the 4th International Conference on Security and Cryptography [8]
    - A study of implicit execution calls used by Android malware was published at the 12th International Conference on Malicious and Unwanted Software [2]
  - **Posters** We have presented results of the Kharon project through posters in International Conference
    - DIMVA 2015 [9]
    - S&P 2016 [10]
- **National Conferences**
  - RESSI 2015 [11], RESSI 2018 [12]
- **International Workshops**

  We have shared our results in a malware dataset that was published in the *Learning from Authoritative Security Experiment Results (LASER)* workshop [3].
- **Magazine**

  We had an article in ERCIM News [13].

1 Educational outcomes

Scientific results obtained in this project have served to create lectures and to enhance existing lectures in the following institutions:

- CentraleSupelec: Labs about Android malware, master degree.

- University of Rennes 1: Course about Android malware, master degree.
- University of Orléans: Labs about Android malware, master degree.
- INSA Centre Val de Loire: Labs about Android malware, engineering degree.
- ENS Lyon: Labs about Android malware, master degree.

We gave also courses in the following conferences and summer schools:

- CISSI 2015
- CISSI 2016: http://kharon.gforge.inria.fr/tutorial/cissi-16/
- Cyber in Bretagne: http://kharon.gforge.inria.fr/tutorial/cyber-bretagne-16/
- Cyber in Berry: http://kharon.gforge.inria.fr/tutorial/cyber-berry-17/

We also add a publication at SIGCSE'19[2] **a ranked A conference for computer science education** [14]. This publication presents a global approach for learning security of mobile phone to students. The kharon project contributed for the learning part that is dedicated to malware.

2 Dissemination

Practical results issued from the Kharon project were presented by several *demos of our tools* during:

- *Forum International de la Cybersécurité* at Lille in 2016 and 2018
- *Fête de la science* at Inria in 2018
- *Fête de la science* at Bourges in 2016

These works also regularly presented during the visits of the *Laboratoire Haute Sécurité* in the Inria Rennes Bretagne Atlantique center.

We have disseminated our experience concerning Android malware to:

- Valérie Viet Triem Tong was invited by Fred Courant in the TV show *L'Esprit Sorcier* direct live at the *Fête de la Science, Cité des Sciences et de l'Industrie* 2017.
- Valérie Viet Triem Tong gives a talk at the *Séminaire Aristote de l'école Polytechnique* in 2016

Lastly, Valérie Viet Triem Tong is author of an article on malicious code in the french scientific popularization journal Inria Interstices 2016 [15]

3 Transfer

We have been invited by several industrial teams to present this work including Kereval, Morpho, Trusted Labs, Airbus, and DGA-MI. Airbus was very interested to include this work into Orion, its own platform of malicious code analysis. DGA-MI is also interested to acquire our platform for its operational teams. The negociations at this time are just beginning.

[2]Association for Computing Machinery's Special Interest Group on Computer Science Education

4 Future works

Jean François Lalande and Valérie Viet Triem Tong will continue research in this topic.

- Pierre Graux has started a phD thesis in october 2017, Pierre focuses on applications whose code on bytecode form is either corrupted, encrypted or intentionally missing but available in its binary form. This can appear when these applications have been protected by a packer or pre-installed in the device. Currently, as far as we know none of existing tools can analyze these applications.
- Souhir Laribi has just started a 2-years position of research engineer founded by Inria. Souhir has to enhance development of the Kharon platforms. She has also to contribute to the evolution of Blare, the information flows monitor.

The Kharon project has given the opportunity to interact with others French and European researchers working on malware analysis:

- Sébastien Bardin, researcher at theSoftware Safety & Security Lab of CEA
- Jean Yves Marion, Head of the computer science lab. of the University of Lorraine
- Guillaume Bonfante, maitre de conférence, Loria, École des Mines de Nancy
- Stéphano Zanero associated professor at Polytechnico di Milano
- Frédérico Maggi now at Trend Micro but previously associated professor at Polytechnico di Milano
- Jacques Klein and Yves Le Traon professors at University of Luxembourg
- Alexander Pretschner professor at TU Munich
- Lorenzo Cavallaro professor at Royal Holloway, University of London

Adrien Brunelat was master student in the Kharon project and has spent a year at Polytechnico di Milano with Frédérico Maggi and Stéphano Zanero. Mourad Leslous PhD in the Kharon project and has spent three months at Munich to work in the team of Alexander Pretschner and three months at London to work with Lorenzo Cavallaro.

We have already submitted two proposals to the French research agency (ANR). Those proposals are built upon the kharon project and integrate our colleagues from Loria and CEA.

References

[1] A. Abraham, R. Andriatsimandefitra, A. Brunelat, J.-F. Lalande, and V. Viet Triem Tong, "GroddDroid: a Gorilla for Triggering Malicious Behaviors," in *10th International Conference on Malicious and Unwanted Software*. Fajardo, Puerto Rico: IEEE Computer Society, Oct. 2015, pp. 119–127, best Paper Award. [Online]. Available: https://hal.inria.fr/hal-01201743

[2] M. Leslous, V. Viet Triem Tong, J.-F. Lalande, and T. Genet, "GPFinder: Tracking the Invisible in Android Malware," in *12th International Conference on Malicious and Unwanted Software*. Fajardo, Puerto Rico: IEEE Conputer Society, Oct. 2017, pp. 39–46. [Online]. Available: https://hal-centralesupelec.archives-ouvertes.fr/hal-01584989

[3] N. Kiss, J.-F. Lalande, M. Leslous, and V. Viet Triem Tong, "Kharon dataset: Android malware under a microscope," in *The Learning from Authoritative Security Experiment Results (LASER) workshop*. San Jose, United States: USENIX Association, May 2016, pp. 1–12. [Online]. Available: https://hal-centralesupelec.archives-ouvertes.fr/hal-01311917

[4] J.-F. Lalande, "Sécurité Android: exemples de malware," in *Colloque International sur la Sécurité des Systèmes d'Information*, Kénitra, Morocco, mar 2015.

[5] J.-F. Lalande, V. Viêt Triem Tong, M. Leslous, and P. Graux, "Challenges for Reliable and Large Scale Evaluation of Android Malware Analysis," in *SHPCS 2018 - International Workshop on Security and High Performance Computing Systems*. Orléans, France: IEEE Computer Society, Jul. 2018, pp. 1–3. [Online]. Available: https://hal-centralesupelec.archives-ouvertes.fr/hal-01844312

[6] J.-F. Lalande, "Android Malware Analysis: from technical difficulties to scientific challenges," in *International Conference on Information Technology and Communications Security*, Bucharest, 2018. [Online]. Available: https://hal-centralesupelec.archives-ouvertes.fr/hal-01906318/file/secitc-keynote.pdf

[7] R. Andriatsimandefitra and V. Viet Triem Tong, "Detection and Identification of Android Malware Based on Information Flow Monitoring," in *The 2nd IEEE International Conference on Cyber Security and Cloud Computing (CSCloud 2015)*, New York, United States, Nov. 2015. [Online]. Available: https://hal.inria.fr/hal-01191595

[8] V. Viet Triem Tong, A. Trulla, M. Leslous, and J.-F. Lalande, "Information flows at OS level unmask sophisticated Android malware," in *14th International Conference on Security and Cryptography*, vol. 6. Madrid, Spain: SciTePress, Jul. 2017, pp. 578–585. [Online]. Available: https://hal-centralesupelec.archives-ouvertes.fr/hal-01535678

[9] A. Abraham, R. Andriatsimandefitra Ratsisahanana, N. Kiss, J.-F. Lalande, and V. Viet Triem Tong, "Towards Automatic Triggering of Android Malware," 12th International Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Jul. 2015, poster. [Online]. Available: https://hal.inria.fr/hal-01168354

[10] M. Leslous, J.-F. Lalande, and V. Viet Triem Tong, "Using Implicit Calls to Improve Malware Dynamic Execution," 37th IEEE Symposium on Security and Privacy, May 2016, poster. [Online]. Available: https://hal.archives-ouvertes.fr/hal-01304326

[11] R. Andriatsimandefitra Ratsisahanana, T. Genet, L. Guillo, J.-F. Lalande, D. Pichardie, and V. Viet Triem Tong, "Kharon : Découvrir, comprendre et reconnaître des malware Android par suivi de flux d'information," in *Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*, Troyes, France, May 2015. [Online]. Available: https://hal.inria.fr/hal-01154368

[12] J.-F. Lalande and V. Viet Triem Tong, "Le projet CominLabs Kharon: aidons les malwares à s'exécuter," in *RESSI 2018 - Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information*, Nancy / La Bresse, France, May 2018, p. 1. [Online]. Available: https://hal-centralesupelec.archives-ouvertes.fr/hal-01794223

[13] V. Viet Triem Tong, J.-F. Lalande, and M. Leslous, "Challenges in Android Malware Analysis," *ERCIM News*, no. 106, pp. 42–43, Jul. 2016. [Online]. Available: https://hal-centralesupelec.archives-ouvertes.fr/hal-01355122

[14] J.-F. Lalande, V. Viet Triem Tong, P. Graux, G. Hiet, W. Mazurczyk, H. Chaoui, and P. Berthomé, "Teaching Android Mobile Security," in *SIGCSE'19*. Minneapolis, USA: ACM, 2019.

[15] V. Viet Triem Tong, "Lutter contre les codes malveillants," *Interstices*, Dec. 2016. [Online]. Available: https://hal.inria.fr/hal-01427326