IN PARTNERSHIP WITH:
CNRS

CentraleSupélec

Université Rennes 1

Activity Report 2017

Project-Team CIDRE

Confidentialité, Intégrité, Disponibilité et Répartition

IN COLLABORATION WITH: Institut de recherche en informatique et systèmes aléatoires (IRISA)

RESEARCH CENTER
Rennes - Bretagne-Atlantique

THEME
Security and Confidentiality

Table of contents

Project-Team CIDRE

Creation of the Project-Team: 2011 July 01

Keywords:

Computer Science and Digital Science:

A1.2.8. - Network security
A1.3. - Distributed Systems
A3.3.1. - On-line analytical processing
A3.5.2. - Recommendation systems
A4.1.1. - Malware analysis
A4.1.2. - Hardware attacks
A4.4. - Security of equipment and software
A4.8. - Privacy-enhancing technologies
A4.9.1. - Intrusion detection
A4.9.2. - Alert correlation
A7.1. - Algorithms

Other Research Topics and Application Domains:

B6.5. - Information systems
B9.8. - Privacy

1. Personnel

Research Scientists

Emmanuelle Anceaume [CNRS, Researcher]
Michel Hurfin [Inria, Researcher, HDR]
Mohamed Kasraoui [Univ de Rennes I, Researcher, until Aug 2017]

Faculty Members

Christophe Bidan [Team leader, CentraleSupélec, Professor, HDR]
Gilles Guette [Univ de Rennes I, Associate Professor]
Guillaume Hiet [CentraleSupélec, Associate Professor]
Jean-François Lalande [CentraleSupélec, Associate Professor, from Sep 2017, HDR]
Ludovic Mé [CentraleSupélec, Professor, HDR]
Guillaume Piolle [CentraleSupélec, Associate Professor]
Eric Totel [CentraleSupélec, Professor, HDR]
Frédéric Tronel [CentraleSupélec, Associate Professor]
Valérie Viet Triem Tong [CentraleSupélec, Associate Professor, HDR]

PhD Students

Solenn Brunet [Orange Labs, until Oct 2017]
Vasile Cazacu [CNRS, from Feb 2017]
Ronny Chevalier [Hewlet Packard France]
Kun He [IMT Atlantique, until Sep 2017]
Deepak Subramanian [IMT Atlantique, until Sep 2017]
Damien Crémilleux [CentraleSupélec]
Aurélien Dupin [Thales]
Laurent Georget [Univ de Rennes I, until Sep 2017]

Florian Grandhomme [Univ de Rennes I, until Sep 2017]
Pierre Graux [Inria, from Oct 2017]
David Lanoé [Inria]
Laetitia Leichtnam [Ministère de la Défense]
Mourad Leslous [Inria]
Thomas Letan [ANSSI, until Sep 2017]
Pernelle Mensah [Bell Labs (Nokia)]
Mounir Nasr Allah [CentraleSupélec]
Aurélien Trulla [Inria]
Charles Arya Xosanavongsa [Thales]

Technical staff

Antoine Guellier [CNRS, from Jun 2017]
Christopher Humphries [Inria, until Aug 2017]

Interns

Minh Anh Dang [CNRS, from Jun 2017 until Aug 2017]
Boris Martin [from Mar 2017 until Oct 2017]
Leopold Ouairy [Univ de Rennes I, from Apr 2017 until Aug 2017]
Jianqiao Xu [CentraleSupélec, until Jan 2017]

Administrative Assistant

Lydie Mabil [Inria]

External Collaborators

Frédéric Majorczyk [DGA]
Sébastien Gambs [UQAM]

2. Overall Objectives

2.1. CIDRE in Brief

Our long term ambition is to contribute to the building of distributed systems that are trustworthy and respectful of privacy, even when some nodes in the system have been compromised.

With this objective in mind, the CIDRE team focuses mainly on the two following topics: Intrusion Detection and Privacy Protection.

3. Research Program

3.1. Our perspective

For many aspects of our everyday life, we heavily rely on information systems, many of which are based on massively networked devices that support a population of interacting and cooperating entities. While these information systems become increasingly open and complex, accidental and intentional failures get considerably more frequent and severe.

Two research communities traditionally address the concern of accidental and intentional failures: the distributed computing community and the security community. While both communities are interested in the construction of systems that are correct and secure, an ideological gap and a lack of communication exist between them that is often explained by the incompatibility of the assumptions each of them traditionally makes. Furthermore, in terms of objectives, the distributed computing community has favored systems availability while the security community has focused on integrity and confidentiality, and more recently on privacy.

Our long term ambition is to contribute to the building of distributed systems that are trustworthy and respectful of privacy, even when some nodes [1] in the system have been compromised. For that purpose, we are convinced that combining classical security approaches and distributed computing paradigms is an interesting way to enforce the security of large-scale distributed systems. More specifically, since a distributed system is composed of nodes, we assert that the security of large-scale distributed systems has to be addressed at three complementary levels:

- the level of each node: each standalone node has to enforce its own security;
- the level of an *identified* set of *trusted* nodes: the *trusted* nodes can *collaborate* to enforce together their security;
- the level of fully open large-scale distributed and dynamic systems: distributed computing paradigms such as consensus algorithms can be applied to cope with the possible presence of malicious nodes.

Notice that using a distributed architecture can also be an approach allowing the nodes to enforce their security without the need of a trusted third party.

The research activities of the CIDRE project-team focus mainly on the two following research axis:

- **Intrusion Detection System:** the objective is to detect any suspicious events with regard to the security by analyzing some data generated on the monitored system.
- **Privacy-preserving Services:** the objective is to ensure users' privacy even when this property seems incompatible with the provided services, like social networks or location-based services.

In all our studies, we consider a priori that the attacker is omnipotent. He can acts as he wants. Nevertheless, since our team is not specialized in cryptography, we consider that we can rely on strong unbroken crypto-systems.

3.2. Intrusion Detection / Security Events Monitoring and Management

Today, we have not yet fully entered into a world of "security by design". Security remains often a property that is considered a posteriori, when the system is deployed, which often results in applying patches when vulnerabilities are discovered (also called a "patch and pray" approach). Unfortunately, despite patching, the number of vulnerabilities remains high, as evidenced by the number of vulnerabilities published each year in the Common Vulnerabilities and Exposures (CVE) system. Thus, it is important to be able to early detect cyber-attacks, especially when they exploit vulnerabilities that are unknown. However, the efficiency of security events monitoring and management systems (including the IDS - Intrusion Detection Systems) is still an open issue today. Indeed, they are often unable to effectively deal with huge numbers of security events, and they usually produce too many false alarms yet missing some attacks. So one of the main research challenges in IT security remains the definition of efficient security events monitoring systems, i.e., that enable both to process a huge number of security events and to detect any attacks without flooding the security analysts with false alarms.

By exploiting vulnerabilities in operating systems, applications, or network services, an attacker can defeat preventive security mechanisms and violate the security policy of the whole system. The goal of an Intrusion Detection Systems (IDS) is to detect such violations by analyzing some *security events* generated on a monitored system. Ideally, the IDS should produce an alert for any violation (no *false negative*), and only for violations (no *false positive*).

To produce alerts, two detection techniques exist: the misuse based detection and the anomaly based detection. A misuse based detection is actually a signature based detection approach : it allows to detect only the attacks whose signature is available. From our point of view, while useful in practice, misuse detection is intrinsically limited. Indeed, it requires to update in real-time the database of signatures, similarly to what has to be done for antivirus tools. The CIDRE project-team follows the alternative approach, namely the anomaly approach, which consists in detecting a deviation from a referenced behavior. Our contributions on anomaly-based IDS follow three axis:

[1] The term node either refers to a device that hosts a network client or service or to the process that runs this client or service.

- **Illegal Information Flow Detection:** our goal is to detect information flows in the monitored system (either a node or a set of trusted nodes) that are allowed by the access control mechanism, but are illegal from the security policy point of view. This approach is particularly appealing to detect intrusions in a standalone node, such as a smartphone.
- **Anomaly-Based Detection in Distributed Applications:** our goal is to specify the normal behavior based on either a formal specification of the distributed application, or previous executions. This approach is particularly appealing to detect intrusions in industrial control systems since these systems exhibit well-defined behaviors at different levels: network level (network communication patterns, protocol specifications, etc.), control level (continue and discrete process control laws), or even the state of the local resources (memory or CPU).
- **Online data analytics:** our goal is to estimate on the fly different statistics or metrics on distributed input streams to detect abnormal behavior with respect to a well-defined criterion such as the distance between different streams, their correlation or their entropy.

Beside the anomaly-based IDS, we have also led research work on alert correlation and visualisation of security events. Indeed, in large systems, multiple (host and network) IDS and many sensors are deployed and they continuously and independently generate notifications (event's observations, warnings and alerts). To cope with this huge amount of collected data, we have studied two different approaches, each with specific goal:

- **Alert Correlation System:** the alerts of *low level* IDSes can be viewed as *security events* of a *high level* IDS whose goal is to correlate these alerts. An alert correlation system aims at exploiting the known relationships between some elements that appear in the flow of low level notifications to generate high semantic meta-alerts. The main goal is to reduce the number of alerts (and especially, false positive) returned to the security analysts and to allow a higher level analysis of the situation (situational awareness).
- **Visualization Tools:** a visualization tools aims at relying on the capacity of human beings to detect patterns and outliers in datasets when these datasets are properly visually represented. Human beings also know pieces of contextual information that are very difficult to formalize so as to make them usable by a computer. Visualization is therefore a very useful complementary tool to detect abnormal events in real time (monitoring), to search for malicious events in log files (data exploration and forensics) and to communicate results (reporting).

3.3. Privacy

In a world of ubiquitous technologies, each individual constantly leaves digital traces related to his activities and interests. The current business plan of many web services such as social networks, is based on the sale of these digital traces. Of course, this is usually done in a legal way, the license of use clearly stating that the user gives the right to the service provider for using his personal data. However, on the one hand, users generally do not read these licenses, and on the other hand, these licenses are usually very vague on the use of personal data [2]. In addition these digital traces can potentially be stolen and maliciously used, they must therefore be protected. In this context, users' privacy is now recognized as a fundamental individual right. Any new IT service should thus follow the *privacy-by-design* approach: privacy issues have to be studied from the earliest phase of a project by taking into account the multi-stakeholders and transdisciplinary aspects in order to ensure proper, end-to-end private data protection properties.

In the CIDRE project, we mainly focus on domains in which privacy issues collide with provided services. Here are some concrete examples of such domains:

- **Location-based services:** the challenge is to design services that depend on the user's location while preserving the privacy of his location;
- **Social networks:** the challenge is to demonstrate that it is possible to design social networks respectful of users' privacy;

[2] Besides, it has been shown that service providers do not necessarily comply with their own license.

- **Mobile services:** given that such services are based on user's identity, the challenge is to design mobile services while preserving the users' anonymity;
- **Ad-hoc netwoks:** in ad-hoc networks, any participant can potentially know the relative location of the other participants. Thus, the issue is to allow nodes to forward messages while preserving the privacy of the communications.

For all of these domains, we have proposed new Privacy-Enhancing Techniques (PETs) based on a mix of different foundations such as cryptographic techniques, security policies and access control mechanisms, just to name a few. More generally, we think that a major option to protect users' privacy consists in using a decentralized architecture that enables to transfer control and services from the service providers to the users.

The concept of IDS seems to be in contradiction with the users' privacy. Indeed, an IDS is a monitoring system that needs to collect and analyze information coming from different levels such as network, applications and OS, this information being able to include users' personal data. However, we are confident that IDS and privacy are not completely antagonist. In particular, integrating some privacy features inside an IDS to build a privacy-preserving IDS may allow to limit the amount of information that can leak if one of the nodes within the system is compromised. On the other hand, enabling IDS to detect attacks against privacy as well as security violations can extend the range of their applicability.

4. Application Domains

4.1. Security is Required Everywhere

With the infiltration of computers and software in almost all aspects of our modern life, security can nowadays be seen as an absolutely general concern. As such, the results of the research targeted by CIDRE apply to a wide range of domains. It is clear that critical systems, in which security (and safety) is a major concern, can benefit from ideas such as dynamic security policy monitoring. On the other hand, systems used by the general public (basically, the internet and services such as web or cloud services, social networks, location-based services, etc.) can also benefit from results obtained by CIDRE, in particular to solve some of the privacy issues raised by these systems that manipulate huge amount of personal data. In addition, systems are getting more and more complex, decentralized, distributed, or spontaneous. Cloud computing, in particular, brings many challenges that could benefit from ideas, approaches and solutions studied by CIDRE in the context of distributed systems.

Industrial Control Systems (ICS) and in particular Supervisory Control and Data Acquisition are also new application domains for intrusion detection. The Stuxnet attack has emphasized the vulnerability of such critical systems which are not totally isolated anymore. Securing ICS is challenging since modifications of the systems, for example to patch them, are often not possible. High availability requirements also often conflict with preventive approaches. In this case, security monitoring is appealing to protect such systems against malicious activities. Intrusion detection in ICS is not fundamentally different from traditional approaches. However, new hypotheses and constraints need to be taken into account, which also bring interesting new research challenges.

5. Highlights of the Year

5.1. Highlights

This year, the CIDRE team would like to emphasize the following publications that appeared in major academic venues:

- Formal verification of an information flow monitor, presented at SEFM'17 [11]. See below (5.1.1) for a more complete description of this work.

- Automated quantitative information flow analysis for imperative deterministic programs, presented at POPL'17 [8].
- Reconstruction of connectivity graph for cloud infrastructures, presented at NCA'2017 [17]
- Co-processor-based Behavior Monitoring: Application to the Detection of Attacks Against the SMM, presented at ACSAC'17 [10]

5.1.1. Awards

Laurent Georget, Mathieu Jaume (LIP6), Guillaume Piolle, Frédéric Tronel and Valérie Viet Triem Tong received the best paper award at the SEFM'17 conference , which is a well established conference focused on the link between software development and formal methods. This publication is based on the work realized by Laurent Georget during his PhD. It focuses on the automated verification of the correctness of an information flow monitor that operates at the kernel level (Linux kernel). This information flow monitor relies on the Linux Security Module (LSM hereafter) framework. This framework has been designed for mandatory access control. This work tries to answer the question of its correctness when used for information flow monitoring. The verification is operated by a GCC plugin during the compilation phase of a full Linux kernel. Based on an ad-hoc static analysis, it can determine if the LSM hooks are correctly placed with respect to a property of complete mediation of systems calls. Each system call that is known to generate an information flow during its execution (34 system calls on a grand total of 340) is analyzed to determine if the LSM framework through the hooks it provides can intercept each execution that potentially generates an information flow. We have demonstrated that for 4 system calls, the hooks are not well placed, and discovered that 4 systems calls are simply lacking LSM hooks. A patch has been produced to improve this situation.

BEST PAPER AWARD:

[11]
L. GEORGET, M. JAUME, G. PIOLLE, F. TRONEL, V. VIET TRIEM TONG. *Information Flow Tracking for Linux Handling Concurrent System Calls and Shared Memory*, in "15th International Conference on Software Engineering and Formal Methods (SEFM 2017)", Trento, Italy, A. CIMATTI, M. SIRJANI (editors), LNCS, Springer International Publishing, September 2017, pp. 1-16 [*DOI :* 10.1007/978-3-319-66197-1_1], http://hal.upmc.fr/hal-01535949

6. New Software and Platforms

6.1. Blare

To detect intrusion using information flows
KEYWORDS: Cybersecurity - Intrusion Detection Systems (IDS) - Data Leakage Protection
SCIENTIFIC DESCRIPTION: Blare implements our approach of illegal information flow detection for a single node (Android and Linux kernel, JVM) and a set of nodes (monitoring of flows between linux machines).
FUNCTIONAL DESCRIPTION: Blare IDS is a set of tools that implements our approach to illegal information flow detection for a single node and a set of nodes.

NEWS OF THE YEAR: During this year, Laurent Georget has modified the implementation of Blare in order to correctly monitor the kernel system calls with LSM hooks. He add also ported this new version of Blare to the Lollipop Android emulator.

- Partner: CentraleSupélec
- Contact: Frédéric Tronel
- Publications: Information Flow Tracking for Linux Handling Concurrent System Calls and Shared Memory - Verifying the Reliability of Operating System-Level Information Flow Control Systems in Linux - Monitoring both OS and program level information flows to detect intrusions against network servers - Experimenting a Policy-Based HIDS Based on an Information Flow Control Model - Introducing reference flow control for intrusion detection at the OS level - Blare Tools: A Policy-Based Intrusion Detection System Automatically Set by the Security Policy - Diagnosing intrusions in Android operating system using system flow graph - Intrusion detection in distributed systems, an approach based on taint marking - BSPL: A Language to Specify and Compose Fine-grained Information Flow Policies - Information Flow Policies vs Malware - A taint marking approach to confidentiality violation detection - Designing information flow policies for Android's operating system - Information Flow Control for Intrusion Detection derived from MAC Policy - Flow based interpretation of access control: Detection of illegal information flows - A taint marking approach to confidentiality violation detection
- URL: http://www.blare-ids.org/

6.2. GNG

Security Supervision by Alert Correlation
KEYWORDS: Intrusion Detection Systems (IDS) - SIEM
SCIENTIFIC DESCRIPTION: GNG is an intrusion detection system that correlates different sources (such as different logs) in order to identify attacks against the system. The attack scenarios are defined using the Attack Description Langage (ADeLe) proposed by our team, and are internally translated to attack recognition automatons. GNG intends to define time efficient algorithms based on these automatons to recognize complex attack scenarios.

- Partner: CentraleSupélec
- Contact: Eric Totel
- Publication: A Language Driven Intrusion Detection System for Events and Alerts Correlation
- URL: http://www.rennes.supelec.fr/ren/perso/etotel/GNG/index.html

6.3. GroddDroid

KEYWORDS: Android - Detection - Malware
SCIENTIFIC DESCRIPTION: GroddDroid automates the dynamic analysis of a malware. When a piece of suspicious code is detected, groddDroid interacts with the user interface and eventually forces the execution of the identified code. Using Blare (Information Flow Monitor), GroddDroid monitors how an execution contaminates the operating system. The output of GroddDroid can be visualized in an web browser. GroddDroid is used by the Kharon software.
FUNCTIONAL DESCRIPTION: GroddDroid 1 - locates suspicious code in Android application 2 - computes execution paths towards suspicious code 3 - forces executions of suspicious code 4 - automate the execution of a malware or a regular Android application

NEWS OF THE YEAR: In 2017, GroddDroid has integrated the work of Mourad Leslous, who have implemented GFinder. GPFinder improves the computation of control flow paths by taking into account the Android framework. The end of the year has been used to clean the code and to improves the graphical interface.

- Partners: CentraleSupélec - Insa Centre Val-de-Loire
- Contact: Valérie Viet Triem Tong
- Publications: Kharon dataset: Android malware under a microscope - GroddDroid: a Gorilla for Triggering Malicious Behaviors - GPFinder: Tracking the Invisible in Android Malware - Information flows at OS level unmask sophisticated Android malware
- URL: http://kharon.gforge.inria.fr/grodddroid.html

6.4. Kharon

KEYWORDS: Android - Malware - Dynamic Analysis
FUNCTIONAL DESCRIPTION: Kharon is a software for managing Android application analysis. Kharon uses the results of the GroddDroid software. The user can submit one or several applications to Kharon and get a graph of the innformation flows that occured at system level and that have been caused by the application.

Kharon is used in the Kharon platform for the analysis of malicious applications. This platform is deployed at the high security laboratory (LHS) of Rennes.

- Author: Sébastien Campion
- Partners: CentraleSupélec - Insa Centre Val-de-Loire
- Contact: Valérie Viet Triem Tong
- URL: http://kharon.gforge.inria.fr/

6.5. StarLord

KEYWORDS: Security - SIEM
FUNCTIONAL DESCRIPTION: In the domain of security event visualisation, we have developed a prototype called StarLord. Basically, this software is able to parse heterogeneous logs, and to extract from each line of logs a set of security objects. Moreover, some of these objects appears in several lines of different logs. These lines are thus linked by the sharing of one or more security objects. When we analyse the lines of logs, we are thus able to generate graphs that represents the links between the different objects discovered in the logs. These graphs are thus displayed in 3D in order for the administrator to investigate easily the relations between the logs and the relations between the logs and some particular indicators of compromission. The tool permits to discover visually the activity of an attacker on the supervised system.

- Authors: Ludovic Mé, Eric Totel, Nicolas Prigent and Laetitia Leichtnam
- Contact: Eric Totel
- Publication: STARLORD: Linked Security Data Exploration in a 3D Graph

6.6. SpecCert

KEYWORDS: Formal methods - Coq
FUNCTIONAL DESCRIPTION: SpecCert is a framework for specifying and verifying Hardware-based Security Enforcement (HSE) mechanisms against hardware architecture models. HSE mechanisms form a class of security enforcement mechanism such that a set of trusted software components relies on hardware functions to enforce a security policy.

- Participant: Thomas Letan
- Partners: ANSSI - CentraleSupélec
- Contact: Guillaume Hiet
- Publications: SpecCert: Specifying and Verifying Hardware-based Security Enforcement - SpecCert: Specifying and Verifying Hardware-based Software Enforcement
- URL: https://github.com/lethom/speccert

6.7. HardBlare

KEYWORDS: Intrusion Detection Systems (IDS) - FPGA - Static analysis
FUNCTIONAL DESCRIPTION: HardBlare is a hardware/software framework to implement hardware DIFC on Xilinx Zynq Platform. HardBlare consists of three components : 1) the VHDL code of the coprocessor, 2) a modified LLVM compiler to compute the static analysis, and 3) a dedicated Linux kernel. This last component is a specific version of the Blare monitor.

- Partners: CentraleSupélec - Lab-STICC
- Contact: Guillaume Hiet
- Publications: ARMHEx: A hardware extension for DIFT on ARM-based SoCs - ARMHEx: a framework for efficient DIFT in real-world SoCs - ARMHEx: embedded security through hardware-enhanced information flow tracking - HardBlare: a Hardware-Assisted Approach for Dynamic Information Flow Tracking - A portable approach for SoC-based Dynamic Information Flow Tracking implementations - Towards a hardware-assisted information flow tracking ecosystem for ARM processors - HardBlare: an efficient hardware-assisted DIFC for non-modified embedded processors

6.8. Conductor

KEYWORDS: Intrusion Detection Systems (IDS) - Static analysis - Instrumentation
FUNCTIONAL DESCRIPTION: Conductor contains three main components: a static analysis to extract the expected behavior of the target, an instrumentation module to add instructions to the target's code in order to send messages to the co-processor, and an intrusion detection engine executed on the co-processor. The latter processes the messages sent by the instrumented target, describing its current behavior. This behavior is then compared against the expected behavior previously extracted by the static analysis.

- Participants: Ronny Chevalier, Guillaume Hiet, Maugan Villatel and David Plaquin
- Partners: CentraleSupélec - HP Labs
- Contact: Ronny Chevalier
- Publication: Co-processor-based Behavior Monitoring: Application to the Detection of Attacks Against the System Management Mode

6.9. Platforms

6.9.1. Kharon platform

The Kharon platform is under development in the LHS of Rennes and should be ready to use in the beginning of 2018. This experimental platform aims to analyze Android malware using a set of software developed by the CIDRE team. Software that are involved are:

- The Blare IDS http://www.blare-ids.org/, and in particular the AndroBlare version, for tracking information flows of malware;
- The GroddDroid software http://kharon.gforge.inria.fr/grodddroid.html, for manipulating the malware statically and dynamically;
- The GPFinder software http://kharon.gforge.inria.fr/gpfinder.html, for computing paths in the malware's control flow;
- The kharon software that handles the orchestration of a bunch of malware, the server and a set of smartphones.

The Kharon platform will be used for analysing malware as soon as they appear in the wild. The analysis results will be stored for further experiments and statistics.

7. New Results

7.1. Intrusion Detection

7.1.1. Intrusion Detection in Distributed Systems

Alert Correlation: In large systems, multiple (host and network) Intrusion Detection Systems (IDS) and many sensors are usually deployed. They continuously and independently generate notifications (event's observations, warnings and alerts). To cope with this amount of collected data, alert correlation systems have to be designed. An alert correlation system aims at exploiting the known relationships between some elements that appear in the flow of low level notifications to generate high semantic meta-alerts. The main goal is to reduce the number of alerts returned to the security administrator and to allow a higher level analysis of the situation. However, producing correlation rules is a highly difficult operation, as it requires both the knowledge of an attacker, and the knowledge of the functionalities of all IDSes involved in the detection process. In the context of the PhD of Erwan Godefroy, we focus on the transformation process that allows to translate the description of a complex attack scenario into correlation rules and its assessment. We show that, once a human expert has provided an action tree derived from an attack tree, a fully automated transformation process can generate exhaustive correlation rules that would be tedious and error prone to enumerate by hand. This is a top-down approach to correlation rule generation. With the PhD of Charles Xosanavongsa, we tackle the problem of a bottom-up approach that consists in discovering automatically the events or alerts that have been produced by the attacker activity. The objective is to classify automatically all suspicious entries in heterogeneous logs relative to a given attack. This requires to exhibit all log entries that are causally linked, and permits to produce a correlation rule that could detect later a new occurence of the attack.

Intrusion Detection in Cloud Infrastructure: Prior to detecting intrusion, it can be useful to know how the supervised system is vulnerable to attacks. Such result is obtained during a risk analysis phase in usual systems. In the PhD thesis of Pernelle Mensah, we try to automate the generation of the description of all possible attacks against a Cloud infrastructure. This work is divided in two separate steps: (1) We first discover the topology of the virtual machines executing in the cloud infrastructure [16], [17] and (2) Build in a second phase a topological attack graph that represents all possible known attacks on the virtual infrastructure. This graph will be later used either to adapt counter-measures to known attacks, or to generate automatically correlation rules to detect the described attacks.

Inferring the normal behavior of an application: We propose an approach to detect intrusions that affect the behavior of distributed applications. To determine whether an observed behavior is normal or not (occurence of an attack), we rely on a model of normal behavior. This model has been built during an initial training phase (machine learning approach). During this preliminary phase, the application is executed several times in a safe environment. The gathered traces (sequences of actions) are used to generate an automaton that characterizes all these acceptable behaviors. To reduce the size of the automaton and to be able to accept more general behaviors that are close to the observed traces, the automaton is transformed. These transformations may lead to introduce unacceptable behaviors. Our current work solves this problem by characterizing the acceptable behaviors with invariant properties that they must verify. During the PhD thesis of David Lanoe, we enhanced the model building. Moreover, we assess this solution, by applying it to a distributed file system called XtreemFS. We show that it is possible to build the model of this given application, and to detect attack against XtreemFS, without producing too much false positives.

This approach is particularly appealing to detect intrusions in industrial control systems since these systems exhibit well-defined behaviors at different levels: network level (network communication patterns, protocol specifications, etc.), control level (continue and discrete process control laws), or even the state of the local resources (memory or CPU). Industrial control systems (ICS) can be subject to highly sophisticated attacks which may lead the process towards critical states. Due to the particular context of ICS, protection mechanisms are not always practical, nor sufficient. On the other hand, developing a process-aware intrusion detection solution with satisfactory alert characterization remains an open problem. Sophisticated process-aware attacks targeting industrial control systems require adequate detection measures taking into account the physical

process. We propose an approach relying on automatically mined process specifications to detect attacks on sequential control systems. The specifications are synthesized as monitors that read the execution traces and report violations to the operator. In contrast to other approaches, a central aspect of our method consists in reducing the number of mined specifications suffering from redundancies. We evaluate our approach on a hardware-in-the-loop testbed with a complex physical process model and discuss our approach's mining efficiency and attack detection capabilities. This work has been submitted to the Safeprocess'18 conference.

7.1.2. Illegal Information Flow Detection

Our research work on intrusion detection based on information flow has been initiated in 2002. This research work has resulted in Blare, a framework for Intrusion Detection Systems [3], including KBlare, an implementation as a Linux Security Module (LSM), JBlare, an implementation for the Java Virtual Machine (JVM), and AndroBlare, for Android applications.

Information Leaks: Qualitative information flow aims at detecting information leaks, whereas the emerging quantitative techniques target the estimation of information leaks. Quantifying information flow in the presence of low inputs is challenging, since the traditional techniques of approximating and counting the reachable states of a program no longer suffice. We propose an automated quantitative information flow analysis for imperative deterministic programs with low inputs. The approach relies on a novel abstract domain, the cardinal abstraction, in order to compute a precise upper-bound over the maximum leakage of batch-job programs. We prove the soundness of the cardinal abstract domain by relying on the framework of abstract interpretation. We also prove its precision with respect to a flow-sensitive type system for the two-point security lattice. This approach has been published in POPL'17 [8].

Correct information flow monitoring by design: As mentionned previously, our research team is developing an information monitor called Blare. Like most of its competitors (e.g. Laminar or Weir) our solution is based on the Linux Security Module (LSM) framework. However, this framework was initially designed with access control in mind. A natural question arises from this matter of fact: does the LSM framework can be used to correctly track information flow (at the operating system level) ? In the context of his PhD thesis, Laurent Georget has studied this very same question.

To tackle this problem, Laurent Georget has designed an ad hoc static analysis that run as a GCC plugin during the Linux kernel compilation. This analysis can prove (or disprove) the fact that LSM hooks within a chosen set of system calls (known to realize information flows between operating systems containers like files, sockets or pipe) are placed at correct locations so as to intercept these possible information flows. The experiments conducted by Laurent Georget have revealed that on an initial set of 38 system calls, 28 were correctly instrumented by LSM, 4 of them were equipped with a LSM hook that could miss some information flow (under certain circumstances), 3 were simply lacking a LSM hook, and 3 false positives had to be manually analyzed and requalified. Laurent Georget was able to produce a kernel patch to remove all missing and misplaced hooks. This patch can be prove to be correct using the same tool. This contribution was published at FormaliSE 2017 [12].

We had detected for a long time a subtle bug in our information flow monitor implementation (Blare) that we were able to track down to a race condition between two concurrent system calls reading and writing into the same pipe. Laurent Georget has proposed during its PhD an elegant solution to this complex problem: he proposed to divide each information flow into three stages: the activation, the execution and the deactivation. Only the activation and deactivation can be observed by the monitor using LSM hooks placed at the beginning and the exit of a system call. This way, it becomes possible to track causal dependencies between concurrent system calls within the LSM framework. Laurent Georget has proved (using the Coq proof assistant) that his approach is correct and computes the smallest possible over-approximation, in the sense that for any concurrent execution where multiple system calls are used there exists a linearization of this execution that produces the information flow computed by his algorithm. Laurent Georget has implemented his algorithm in the Linux kernel. This contribution was publish at Software Engineering & Formal Methods (2017) where it was granted the best paper award [11]. Laurent Georget has defended his PhD thesis in September 2017 .

[3] http://www.blare-ids.org/

Advanced Persistent Threats: Long lived attack campaigns known as Advanced Persistent Threats (APTs) have emerged as a serious security risk. These attack campaigns are customised for their target and performed step by step during months on end. The major difficulty in detecting an APT is keeping track of the different steps logged over months of monitoring and linking them. In [29], we described TerminAPTor, an APT detector which highlights links between the traces left by attackers in the monitored system during the different stages of an attack campaign. TerminAPTor tackles this challenge by resorting to Information Flow Tracking (IFT). TerminAPTor was presented last year and we have pursue our effort in this area. More precisely, we have focus on the evaluation of this solution and thus we face to the lack of public datasets of attacks. We develop Moirai a framework dedicated to attacks scenario sharing [22] .

Characterizing Android Malware: Android has become the world's most popular mobile operating system, and consequently the most popular target for unscrupulous developers. These developers seek to make money by taking advantage of Android users who customize their devices with various applications, which are the main malware infection vector. Indeed, the most likely way a user executes a repackaged application is by downloading a seemingly harmless application from a store and executing it. Such an application may have been modified by an attacker in order to add malicious pieces of code.

To fight repackaged applications containing malicious code, most official application marketplaces have implemented security analysis tools that try to detect and remove malware. Countermeasures adopted by the attackers to bypass these new controls can be divided into two main approaches: avoiding static analysis and avoiding dynamic analysis. A static analysis of an application consists of analysing its code and its resources without executing it. Conversely, dynamic analysis stands for any kind of analysis that requires executing the application in order to observe its actions.

The Kharon project [30] goes a step further from classical dynamic analysis of malware [4]. Funded by the Labex CominLabs and involving partners of CentraleSupélec, Inria and INSA Centre Val de Loire, this project aims to capture a compact and comprehensive representation of malware. To achieve such a goal we have developed tools to monitor operating systems' information flows induced by the execution of a marked application. We support the idea that the best way to understand malware impact is to observe it in its normal execution environment i.e., a real smartphone. Additionally, the main challenge is to be able to trigger malicious behaviors even when the malware tries to escape dynamic analysis.

In this context, we have developed an original solution whose main purpose is a relavant dynamic analysis of the malicious code. We develop the GroddDroid software, that mainly consists of 'helping the malware to execute'. To reach this goal, GroddDroid relies on a previous static analysis that evidence all the execution paths leading to the malicious code. We compute a global control flow graph (CFG) that exhibits execution paths to reach specific parts of code, even if these paths use callbacks that are handled in the Android framework itself [15]. Finally, GroddDroid slightly modifies the bytecode of the infected application in order to defeat the protection against dynamic analysis and executes the suspicious code in its most favorable execution conditions. Thus, GroddDroid helps to understanding malware's objectives and the consequences on the health of a user's device.

GroddDroid can also be used for classifying applications between goodware and malware. We show in [19] that benign applications have a System Flow Graph (a graph that represent flows at operating system level) that can be anticipated. Malware that perform complex operations such as installing backdoor or launching a Tor client, have a CFG that differ enough to be classified easily.

Our main research direction and challenges in this area are to continue to enhance these technologies in order to reach a sufficient level of software maturity to deploy a permanent platform of malware analysis in the LHS (Laboratory of High Security) and to create new opportunities with industrial partners.

7.1.3. Intrusion Detection in Low-Level Software Components

In order to protect the IDS itself, we have initiated different research activities in the domain of hardware security. Our goal is to use co-design software/hardware approaches against traditional software attacks. In a

[4] http://kharon.gforge.inria.fr

bilateral research project with HP Inc Research Labs, we investigate how dedicated hardware could be used to monitor the whole software stack (from the firmware to the user-mode applications). In the CominLabs HardBlare project, we study the use of a dedicated co-processor to enforce Information Flow Control (IFC) on the main CPU. Finally, in the context of the PhD thesis of Thomas Letan (ANSSI), we investigate the use of formal methods to evaluate the security guarantees provided by hardware platforms, which combine different CPUs, chipsets and memories.

Highly privileged software, such as firmware, is an attractive target for an attacker. Thus, BIOS vendors use cryptographic signatures to ensure firmware integrity at boot time. Nevertheless, such boot time protection does not prevent an attacker from exploiting vulnerabilities at runtime. To detect such runtime attacks, we proposed an event-based monitoring approach that relies on an isolated co-processor [10]. We instrument the code executed on the main CPU to send information about its behavior to the monitor. In this work, we focus on the detection of attacks targeting the System Management Mode (SMM), a highly privileged x86 execution mode executing firmware code at runtime. We use the control flow of the code as a model of its behavior. We evaluate our approach with two open-source implementations: EDK II and coreboot. We evaluate its ability to detect state-of-the-art attacks and its runtime execution overhead by simulating an x86 system coupled with an ARM Cortex A5 co-processor. The results show that our solution detects intrusions from the state of the art while remaining acceptable in terms of performance overhead in the context of the SMM. This work has been done in collaboration with HP Inc Research Labs, in the context of the PhD of Ronny Chevalier.

Over time, hardware designs have constantly grown in complexity and modern platforms involve multiple interconnected hardware components. During the last decade, several vulnerability disclosures have proven that trust in hardware can be misplaced. The approach we developed with Thomas Letan rely on a formal definition of Hardware-based Security Enforcement (HSE) mechanisms, a class of security enforcement mechanisms such that a software component relies on the underlying hardware platform to enforce a security policy. We then model a subset of a x86-based hardware platform specifications and we prove the soundness of a realistic HSE mechanism within this model using Coq, a proof assistant system.

The HardBlare project proposes a software/hardware co-design methodology to ensure that security properties are preserved all along the execution of the system but also during files storage. It is based on the Dynamic Information Flow Tracking (DIFT) that generally consists in attaching tags to denote the type of information that are saved or generated within the system. These tags are then propagated when the system evolves and information flow control is performed in order to guarantee the safe execution and storage within the system monitored by security policies. We proposed ARMHEx [20], a practical solution targeting DIFT on ARM-based SoCs (e.g. Xilinx Zynq). Current DIFT implementations suffer from two major drawbacks. First, recovering required information for DIFT is generally based on software instrumentation leading to high time overheads. ARMHEx takes profit of ARM CoreSight debug components and static analysis to drastically reduce instrumentation time overhead (up to 90% compared to existing works). Then, security of the DIFT hardware extension itself is not considered in related works. In this work, we tackle this issue by proposing a solution based on ARM Trustzone. This work has been done in the context of the PhD of Muhammad Abdul Wahab and Mounir Nasr Allah.

7.1.4. Vizualization

When using Intrusion Detection Systems (IDS), the large quantities of alerts generated are difficult to handle by security experts. To help solving this problem, we have proposed VEGAS, an alerts visualization and classification tool that allows primary visions based on their principal component analysis (PCA) representation. Following this, we have studied the context of collaboration between the various security actors. We have then proposed an extension to VEGAS that allows to help the actors to collaborate. We have developped an interface that permits the front-end operator to quickly understand the security events, and group them to organize incidents and send them to dedicated analysts. Conversely, once the incidents have been analysed, the analysts can send information to the front-line operators to help them understanding the futur security events.

We also developed another tool called STARLORD [14] that permits to an administrator the explore in a 3D graph representing the links between the heterogeneous entries in various logs produced either by the system, applications or IDSes. To emphasize the important relations between the lines of logs that can potentially be part of an attack activity, we classify these links in order to present only the part of the graph that is linked to an indicators of compromission.

Our previous research on visualization of security events has lead to two proofs-of-concept (See ELVIS and CORGI softwares). We are currently pursuing business opportunities on this topic. Indeed SplitSec is a soon to be founded startup developing tools to help security experts to better manage and understand security data. Scalable analysis solutions and data visualisations adapted for security are combined into powerful tools for incident response. Until June 2017, Christopher Humphries has been hired by Inria as a technology transfer engineer to build these tools based on promising research prototypes.

7.2. Privacy

7.2.1. Image Encryption

More and more users prefer to share their photos through image-sharing platforms of social networks than using e-mail or personal webpages. Since the provider of the image-sharing platform can clearly know the contents of any published images, the users have to trust the provider to respect their privacy or has to encrypt their images. In the context of the PhD of Kun He, we have proposed an IND-CPA image encryption algorithm that preserve the image format after encryption, and we have shown that our encryption algorithm can be used on several widely used image-sharing platforms such as Flickr, Pinterest, Google+ and Twitter. Kun He has completed her PhD thesis in September 2017 [5].

7.3. Security of Communicating and Distributed Systems

7.3.1. Routing Protocol for Tactical Mobile Ad Hoc Networks

In the context of the PhD thesis of Florian Grandhomme, we propose new secure and efficient algorithms and protocols to provide inter-domain routing in the context of tactical mobile ad hoc network. The proposed protocol has to handle context modification due to the mobility of Mobile Ad hoc NETwork (MANET), that is to say split of a MANET, merge of two or more MANET, and also handle heterogeneity of technology and infrastructure. The solution has to be independent from the underlying intra-domain routing protocol and from the infrastructure: wired or wireless, fixed or mobile. This work is done in cooperation with DGA-MI.

New generation military equipment, soldiers and vehicles, use wireless technology to communicate on the battlefield. During missions, they form a MANET. Since the battlefield includes coalition, each group may communicate with another group, and inter-MANET communication may be established. Inter-MANET (or inter-domain MANET) communication should allow communication, but maintain a control on the exchanged information. Several protocols have been proposed in order to handle inter-domain routing for tactical MANETs. During the thesis we have shown that simulator (NS3) or emulator (CORE) do not handle correctly ad hoc network behavior and then that solution in the state of the art are more complex than needed. Based on this analysis, we propose some preconizations to design Inter-domain protocols for MANET and we propose the ITMAN (Inter Tactical Mobile Ad hoc Network) protocol that allows also to handle simple routing policy (merge, link and deny). We evaluate this new protocol through experimentation and we show that our proposition is quite efficient. On going work on this protocol is the definition and implementation of more subtle routing policy that allow announce filtering of giving prefix for example.

7.3.2. Decentralized Cryptocurrency Systems

Distributed Ledgers (e.g. Bitcoin) occupy currently the first lines of the economical and political media and many speculations are done with respect to their level of coherence and their computability power. Interestingly, there is no consensus on the properties and abstractions that fully capture the behaviour of distributed ledgers. The interest in formalising the behaviour of distributed ledgers is twofold. Firstly, it helps

to prove the correctness of the algorithms that implement existing distributed ledgers and explore their limits with respect to an unfriendly environment and target applications. Secondly, it facilitates the identification of the minimal building blocks necessary to implement the distributed ledger in a specific environment. Even though the behaviour of distributed ledgers is similar to abstractions that have been deeply studied for decades in distributed systems no abstraction is sufficiently powerful to capture the distributed ledger behaviour. We have defined the Distributed Ledger Register, a register that mimics the behaviour of one of the most popular distributed ledger, i.e. the Bitcoin ledger. The aim of our work is to provide formal guarantees on the coherent evolution of Bitcoin. We furthermore showed that the Bitcoin blockchain maintenance algorithm verifies the distributed ledger register properties under strict conditions. Moreover, we proved that the Distributed Ledger Register verifies the regularity register specification. It follows that the strongest coherency implemented by Bitcoin is regularity under strong assumptions (i.e. partial synchronous systems and sparse reads). In [7] we proposed a study that contradicts the common belief that Bitcoin implements strong coherency criteria in a totally asynchronous system. To the best of our knowledge, our work is the first one that makes the connection between the distributed ledgers and the classical theory of distributed shared registers.

Double spending and blockchain forks are two main issues that the Bitcoin crypto-system is confronted with. The former refers to an adversary's ability to use the very same coin more than once while the latter reflects the occurrence of transient inconsistencies in the history of the blockchain distributed data structure. We present a new approach to tackle these issues: it consists in adding some local synchronization constraints on Bitcoin's validation operations, and in making these constraints independent from the native blockchain protocol. Synchronization constraints are handled by nodes which are randomly and dynamically chosen in the Bitcoin system. In [13] we show that with such an approach, content of the blockchain is consistent with all validated transactions and blocks which guarantees the absence of both double-spending attacks and blockchain forks.

7.3.3. Large Scale Systems

Population Protocol: the computational model of population protocols is a formalism that allows the analysis of properties emerging from simple and pairwise interactions among a very large number of anonymous finite-state agents. Significant work has been done so far to determine which problems are solvable in this model and at which cost in terms of states used by the protocols and time needed to converge. The problem tackled in is the population proportion problem: each agent starts independently from each other in one of two states, say A or B, and the objective is for each agent to determine the proportion of agents that initially started in state A, assuming that each agent only uses a finite set of state, and does not know the number n of agents. In [18], we show that for any $\delta \in (0, 1)$, the number of interactions needed per node to converge is $O(ln(n/\delta))$ with probability at least $1 - \delta$. We also prove that each node can determine, with any high probability, the proportion of nodes that initially started in a given state without knowing the number of nodes in the system. This work provides a precise analysis of the convergence bounds, and shows that using the 4-norm is very effective to derive useful bounds.

Distributed Stream Processing Systems: shuffle grouping is a technique used by stream processing frameworks to share input load among parallel instances of stateless operators. With shuffle grouping each tuple of a stream can be assigned to any available operator instance, independently from any previous assignment. A common approach to implement shuffle grouping is to adopt a Round-Robin policy, a simple solution that fares well as long as the tuple execution time is almost the same for all the tuples. However, such an assumption rarely holds in real cases where execution time strongly depends on tuple content. As a consequence, parallel stateless operators within stream processing applications may experience unpredictable unbalance that, in the end, causes undesirable increase in tuple completion times. In [25] we propose Online Shuffle Grouping (OSG), a novel approach to shuffle grouping aimed at reducing the overall tuple completion time. OSG estimates the execution time of each tuple, enabling a proactive and online scheduling of input load to the target operator instances. Sketches are used to efficiently store the otherwise large amount of information required to schedule incoming load. We provide a probabilistic analysis and illustrate, through both simulations and a running prototype, its impact on stream processing applications.

The real time analysis of massive data streams is of utmost importance in data intensive applications that need to detect as fast as possible and as efficiently as possible (in terms of computation and memory space) any correlation between its inputs or any deviance from some expected nominal behavior. The IoT infrastructure can be used for monitoring any events or changes in structural conditions that can compromise safety and increase risk. It is thus a recurrent and crucial issue to determine whether huge data streams, received at monitored devices, are correlated or not as it may reveal the presence of attacks. We propose a metric, called codeviation, that allows to evaluate the correlation between distributed massive streams. This metric is inspired from classical metric in statistics and probability theory, and as such enables to understand how observed quantities change together, and in which proportion. In [6], we propose to estimate the codeviation in the data stream model. In this model, functions are estimated on a huge sequence of data items, in an online fashion, and with a very small amount of memory with respect to both the size of the input stream and the values domain from which data items are drawn. We then generalize our approach by presenting a new metric, the Sketch-metric, which allows us to define a distance between updatable summaries of large data streams. An important feature of the Sketch-metric is that, given a measure on the entire initial data streams, the Sketch-metric preserves the axioms of the latter measure on the sketch. We finally conducted extensive experiments on both synthetic traces and real data sets allowing us to validate the robustness and accuracy of our metrics.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- **HP (2013-2019): Embedded Systems Security** We aim at researching and prototyping low-level intrusion detection mechanisms in embedded system software. This involves mechanisms in continuation of previous work realized by our team as well as investigating new techniques more directly tied to specific HP device architectures. Our main objective is to monitor low-level software (firmware, OS kernels, hypervisors) thanks to a dedicated external co-processor. Ronny Chevalier is doing is PhD in the context of this project. Being under NDA, details about this research program cannot be provided.

8.2. Bilateral Grants with Industry

- **Orange Labs: Privacy-preserving location-based services** Solenn Brunet has completed her PhD thesis in November 2017 within the context of a CIFRE contract with Orange Labs Caen. Her PhD subject was about privacy-preserving services that are able to provide the service to the user while preserving his privacy. In particular, Solenn Brunet has designed new cryptographic primitives to build anonymous accreditation and she has used these primitives to provide data anonymization mechanisms in the context of e-voting and e-cash.
- **DGA: BGP-like Inter Domain routing protocol for tactical mobile ad hoc networks: feasibility, performances and quality of service** Florian Grandhomme has completed his PhD thesis in September 2017 in cooperation with DGA-MI. The subject of the PhD was to propose new secure and efficient algorithms and protocols to provide inter-domain routing in the context of tactical mobile ad hoc network. The proposed protocol handles context modification due to the mobility of MANET, that is to say split of a MANET, merge of two or more MANET, and also handles heterogeneity of technology and infrastructure. The solution is independent from the underlying intra-domain routing protocol and from the infrastructure: wired or wireles, fixed or mobile.
- **DGA: Visualization for security events monitoring** Damien Crémilleux has started his PhD thesis in October 2015 in the context of a cooperation with DGA-MI. The subject of the PhD is to define relevant representations to allow front-line security operators to monitors systems from a security perspective. A first proposal was made that led to a tool, VEGAS, that allows to monitor large quantities of alerts in real time and to dispatch these alerts in a relevant way to security analysts.

- **DGA: Intrusion Detection in Distributed Applications** David Lanoé has started his PhD thesis in October 2016 in the context of a cooperation with DGA-MI. His work is focussing on the construction of behavioral models (during a learning phase) and their use to detect intrusions during an execution of the modelled distributed application.
- **Nokia: Risk-aware security policies adaptation in modern communication infrastructures** Pernelle Mensah was hired in January 2016 on this CIFRE funding in order to work on unexplored aspects of information security, and in particular response strategies to complex attacks, in the context of cloud computing architectures. The use case proposed by our industrial partner is a multi-tenant cloud computing platform involving software-defined networking in order to provide further flexibility and responsiveness in architecture management. The topic of the thesis is to adapt and improve the current risk-aware reactive response tools, based on attack graphs and adaptive security policies, to this specific environment, taking into account the heterogeneity of actors, platforms, policies and remediation options.
- **Thales: Privacy and Secure Multi-party Computation** Aurélien Dupin has started his PhD thesis in January 2016 within the context of a CIFRE contract with Thales. His PhD subject concerns secure multi-party computation. Secure two-party computation provides a way for two parties to compute a function, that depends on the two parties' inputs, while keeping them private. Known since the 1980s, Yao's garbled circuits appear to be a general solution to this problem, in the semi-honest model. Decades of optimizations have made this tool a very practical solution. However, it is well known that a malicious adversary could modify a garbled circuit before submitting it. Many protocols, mostly based on cut-&-choose, have been proposed to secure Yao's garbled circuits in the presence of malicious adversaries. Nevertheless, how much an adversary can modify a circuit and make it still executable have not been studied. In the context of his PhD, Aurélien Dupin is interested by such a question.
- **Thales: Combining Attack Specification and Dynamic Learning from traces for correlation rule generation** Charles Xosanavongsa has started his PhD thesis in December 2016 in the context of a CIFRE with Thales. His work will focus on the construction of correlation rules. In previous work on correlation rule generation, the usual approach is static. It always relies on the description of the supervised system using a knowledge base of the system. The use of correlation trees is an appealing solution because it allows to have a precise description of the attacks and can handle any kind of IDS. But in practice, the behavior of each IDS is quite difficult to predict, in particular for anomaly based IDS. To manage automatically the correlation rules (and adapt them if necessary), we plan to analyze synthetic traces containing both anomaly based and misused based IDS alerts resulting from an attack.
- **Ministry of Defence: Visualisation for the characterization of security events** Laetitia Leichtnam has started his PhD thesis in November 2016 in the context of a contract between CentraleSupelec and the French Ministry of Defence. His work consists in presenting events appearing in heterogeneous logs as a dependency graph between the lines of logs. This permits to the administrator to investigate easily the logs to discover the different steps that has performed an attack in the supervised system.
- **ANSSI: Security of Low-level Components** Thomas Letan has started his PhD thesis in the context of a contract between CentraleSupelec and the French National Computer Security Agency (ANSSI). His work consists in using formal methods to specify hardware/software security mechanisms and to verify that they correctly enforce some security policies.

9. Partnerships and Cooperations

9.1. Regional Initiatives

- **Region Bretagne ARED Grant :** the PhD of Mourad Leslous on malicious codes in Android applications is supported by a grant from the Région Bretagne.
- **Labex COMINLABS contract (2014-2017): "Kharon-Security" - http://kharon.gforge.inria.fr**

  Google Play offers more than 800'000 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, etc. Unfortunately, each of these application is an attack vector on Android. The number of malicious applications (pieces of malware) discovered during the first six months of 2013 exceeds the number of pieces of malware discovered during the 2010 to 2012 period, more than 700 thousand malicious and risky applications were found in the wild. In this context, we propose the Kharon-Security project to stem the progression of Android pieces of malware. We propose to combine static and dynamic monitoring to compute a behavioral signature of Android malware. Behavioral signatures are helpful to understand how malware infect the devices and how they spread information in the Android operating system. Static analysis is essential to understand which particular event or callback triggers malware payload.

  In the project we have already developed GroddDroid a tool dedicated to automatic identification and execution of suspicious code. We have also built a dataset of Android malware. In this dataset, all malware are entirely manually reverse and documented. We have also developed an analysis platform. This platform is been deployed at the High Research Laboratory.
- **Labex COMINLABS contract (2015-2018): "HardBlare-Security" - http://www.hardblare.cominlabs.ueb.eu/**

  The general context of the HardBlare project is to address Dynamic Information Flow Tracking (DIFT) that generally consists in attaching marks to denote the type of information that is saved or generated within the system. These marks are then propagated when the system evolves and information flow control is performed in order to guarantee a safe execution and storage within the system. Existing solutions imply a large overhead induced by the monitoring process. Some attempts rely on a hardware-software approach where DIFT operations are delegated to a coprocessor. Nevertheless, such approaches are based on modified processors. Beyond the fact hardware-assisted DIFT is hardly adopted, existing works do not take care of coprocessor security and multicore/multiprocessor embedded systems.

  We plan to implement DIFT mechanisms on boards including a non-modified ARM processor and a FPGA such as those based on the Xilinx Zynq family. The HardBlare project is a multidisciplinary project between CentraleSupélec IETR SCEE research team, CentraleSupélec Inria CIDRE research team and UBS Lab-STICC laboratory. Mounir Nasr Allah is doing his PhD in the context of this project. The main objective of this PhD is to study how hybrid analysis could improve hardware assisted DIFT using static analysis performed at compile-time. Another objective is to manage labels for persistent memory (i.e., files) using a modified OS kernel.
- **Labex COMINLABS contract (2016-2019): "BigClin" - http://www.bigclin.cominlabs.ueb.eu/**

  Health Big Data (HBD) is more than just a very large amount of data or a large number of data sources. The data collected or produced during the clinical care process can be exploited at different levels and across different domains, especially concerning questions related to clinical and translational research. To leverage these big, heterogeneous, sensitive and multi-domain clinical data, new infrastructures are arising in most of the academic hospitals, which are intended to integrate, reuse and share data for research.

  Yet, a well-known challenge for secondary use of HBD is that much of detailed patient information is embedded in narrative text, mostly stored as unstructured data. The lack of efficient Natural Language Processing (NLP) resources dedicated to clinical narratives, especially for French, leads to the development of ad-hoc NLP tools with limited targeted purposes. Moreover, the scalability and real-time issues are rarely taken into account for these possibly costly NLP tools, which make them

inappropriate in real-world scenarios. Some other today's challenges when reusing Health data are still not resolved: data quality assessment for research purposes, scalability issues when integrating heterogeneous HBD or patient data privacy and data protection. These barriers are completely interwoven with unstructured data reuse and thus constitute an overall issue which must be addressed globally.

In this project, we plan to develop distributed methods to ensure both the scalability and the online processing of these NLP/IR and data mining techniques; In a second step, we will evaluate the added value of these methods in several real clinical data and on real use-cases, including epidemilology and pharmaco-vigilance, clinical practice assessment and health care quality research, clinical trials.

9.2. National Initiatives

9.2.1. ANR

- **ANR INFRA Project: SOCIOPLUG (2013-2017) - http://socioplug.univ-nantes.fr/index.php/SocioPlug_Project**

  SocioPlug is a collaborative ANR project involving Inria (ASAP and CIDRE teams), the Nantes University, and LIRIS (INSA Lyon and Université Claude Bernard Lyon). The project emerges from the observation that the features offered by the Web 2.0 or by social media do not come for free. Rather they bring the implicit cost of privacy. Users are more of less consciously selling personal data for services. SocioPlug aims to provide an alternative for this model by proposing a novel architecture for large-scale, user centric applications. Instead of concentrating information of cloud platforms owned by a few economic players, we envision services made possible by cheap low-end plug computers available in every home or workplace. This will make it possible to provide a high amount of transparency to users, who will be able to decide their own optimal balance between data sharing and privacy.

- **ANR Project: PAMELA (2016-2020) - https://project.inria.fr/pamela/**

  PAMELA is a collaborative ANR project involving Rennes 1 university (ASAP and CIDRE teams in Rennes), Inria Lille (MAGNET team), LIP6 (MLIA team) and two start-ups, Mediego and Snips. It aims at developing machine learning theories and algorithms in order to learn local and personalized models from data distributed over networked infrastructures. The project seeks to provide first answers to modern information systems built by interconnecting many personal devices holding private user data in the search of personalized suggestions and recommendations. More precisely, we will focus on learning in a collaborative way with the help of neighbors in a network. We aim to lay the first blocks of a scientific foundation for these new types of systems, in effect moving from graphs of data to graphs of data and learned models. CIDRE's contribution in this project involves the design of adversary models and privacy metrics suitable to the privacy-related issues of this distributed learning paradigm.

9.3. International Initiatives

9.3.1. Inria International Partners

9.3.1.1. Informal International Partners

Emmanuelle Anceaume is actively working with Leonardo Querzoni from the University La Sapienza, Italy, on data streams algorithms and engines. Their cooperation gave rise to one publication in Algotel 2017 [25].

Valérie Viet Triem Tong has shortly visited Prof Alexander Pretchner at TU Munchen in june 2017. She has participated to a workshop about Android Malware analysis.

9.4. International Research Visitors

9.4.1. Research Stays Abroad

In the context of the project with HP Inc Labs, Ronny Chevalier and Guillaume Hiet collaborate with the security team of HP Labs in Bristol. They are working more specifically with David Plaquin and Maugan Villatel, who are co-authors of the article published at ASCAC. Ronny Chevalier has spent 3 monts to HP Labs at Bristol.

Mounir Nasr Allah is currently visiting ARM R&D labs at Cambridge for 6 months in the context of the HardBlare project. This visit has been funded by the EIT Digital Doctoral School Program. He is working with Alastair Reid on the use of formal methods to prove that some hardware security mechanisms of ARM embedded processors effectively enforce information flow policies.

Mourad Leslous did an international mobility of three months at the Technical University of Munich, in the team of Professor Alexander Pretschner. This mobility was part of the program of EIT Digital Doctoral School, a European institute that promotes entrepreneurship and innovation among PhD students. During this mobility, he worked on control flow and data flow dependencies in order to detect the malicious code inside Android applications.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

Emmanuelle Anceaume co-chair with Maria Potop Butucaru, Christian Cachin and Shlomi Dolev the Workshop on Blockchain Technology and Theory 2017, co-located with DISC 2017.

10.1.1.2. Member of the Organizing Committees

Christophe Bidan served as a member of the organization committee of C&ESAR 2017 (24rd Computers & Electronics Security Applications Rendez-vous), November 2017, Rennes, France.

Frédéric Tronel served as a member of the organization committee of SSTIC 2017 (Symposium sur la sécurité des technologies de l'information et des communications) that took place in Rennes, France from 7th to 9th of June, where it gathered 600 participants.

10.1.2. Scientific Events Selection

10.1.2.1. Member of the Conference Program Committees

Emmanuelle Anceaume served as a member of the following program committees:

- Algotel 2017 (19èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications), May 2017, Quiberon, France.
- ICDCS 2017 (37th IEEE International Conference on Distributed Computing Systems), Atlanta, USA, 2017
- DEBS 2017 (11th ACM International Conference on Distributed and Event-based Systems), Barcelona, Spain 2017
- NCA 2017 (16th International Symposium on Network Computing and Applications), October 2017, Cambridge, MA, USA.
- PECS 2017 (3rd International Conference on Pervasive and Embedded Computing), Porto, Portugal, 2017
- ADSN2017 (6th International Workshop on Assurance in Distributed Systems and Networks, Atlanta, USA, 2017

Christophe Bidan served as a member of the following program committees:

- CRiSIS 2017 (12th International Conference on Risks and Security of Internet and Systems), September 2017, Dinard, France.
- C&ESAR 2017 (24rd Computers & Electronics Security Applications Rendez-vous), November 2017, Rennes, France.

Frédéric Majorczyck served as a member of the program committee of VizSec 2017 (IEEE Symposium on Visualization for Cyber Security), October 2017, Phoeniz, Arizona, USA.

Guillaume Piolle served as a member of the program committee of APVP 2017 (Atelier sur la Protection de la Vie Privée), June 2017, Autrans, France.

Eric Totel served as a member of the program committee of RESSI 2017 (Les Rendez-vous de la recherche et de l'enseignement en sécurité des systèmes d'information).

Frédéric Tronel served as a member of the program committee of SSTIC 2017 (Symposium sur la sécurité des technologies de l'information et des communications) June 2017, Rennes, France.

Gilles guette served as a member of the following program committees:

- ICISSP 2017 (International Conference on Information System Security and Privacy), February 2017, Porto, Portugal.

10.1.2.2. Reviewer

- Gilles Guette - IEEE ISNCC 2017 (IEEE International Symposium on Networks, Computers and Communications).
- Michel Hurfin - NCA 2017 (16th International Symposium on Network Computing and Applications).
- Jean-François Lalande - ICISSP 2017 (3rd International Conference on Information Systems Security and Privacy).

10.1.3. Journal

10.1.3.1. Member of the Editorial Boards

Michel Hurfin belongs to the editorial board of the Springer open access journal of Internet Services and Applications.

10.1.3.2. Reviewer - Reviewing Activities

- Emmanuelle Anceaume - Elsevier JPDC (Journal of Parallel and Distributed Computing), Performance Evaluation, IEEE TDSC (Transactions on Dependable and Secure Computing), and IEEE TPDS (Transactions on Parallel and Distributed Systems).
- Michel Hurfin - Springer JISA (Journal of Internet Services and Applications) and Springer TOCS (Theory of Computing Systems).
- Jean-François Lalande - IARIA IJAS (International Journal on Advances in Security), and Elsevier Computer Communications (International Journal for the Computer and Telecommunications Industry).
- Guillaume Piolle - ACM TOIT (Transactions on Internet Technologies).
- Eric Totel - IEEE Transactions on Reliability.

10.1.4. Invited Talks

Emmanuelle Anceaume was invited to give

- a keynote at Algotel 2017, May 2017, entitled "Bitcoin and its distributed ledger"
- a keynote at WIFS 2017, December 2017, entitled: "A primer on blockchain technology and the bitcoin cryptocurrency"

10.1.5. Leadership within the Scientific Community

Ludovic Mé serves the Scientific Council of the LIRIMA (Laboratoire International de Recherche en Informatique et Mathématiques Appliquées).

Ludovic Mé chairs the steering Committee of the annual French conference RESSI (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information). He is a member of the Steering Committee of the annual international conference RAID (International Symposium on Research in Attacks, Intrusions and Defenses).

10.1.6. Research Administration

Emmanuelle Anceaume has participated in various juries (Post-doctoral grants, delegation Inria, PEDR Inria). As a member of the CE Inria, Emmanuelle Anceaume has participated to the hiring committee CR2/CR1 of Rennes and Sophia Antipolis.

Michel Hurfin is the local representative of the "mission jeunes chercheurs" in Rennes. He is a member of the "Commission personnel" and is in charge of the PhD student recruitment campaign of Inria Rennes Bretagne Atlantique. He is a member of the councils of the doctoral school Matisse. He is a member of the advisory board of the doctoral training center of EIT Digital in Rennes.

Ludovic Mé acts as Scientific Officer for the Rennes - Bretagne Atlantic Inria Research Center. As such, he is also a member of the Evaluation Commission and of the Internal Scientific Council of Inria.

Ludovic Mé leads the expert group dedicated to the evaluation of the French laboratories working in the "computing and telecom" domain, relatively to the way they protect their scientific and technical patrimony (PPST French regulation).

Valérie Viet Triem Tong has participated in the scientific evaluation comity *Global Security and Cybersecurity* (CES 39) of the French Research Agency (ANR). Valérie Viet Triem Tong has also participated in the Inria post-doctoral grant.

10.2. Teaching - Supervision - Juries

10.2.1. Certification

The master degree program "Mastère Spécialisé en Cybersécurité" has received the SecNum*edu* label. This label testifies that this program meets the requirements of a charter that has been jointly established by ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information) and various actors (administrations, companies, ...) of the domain. This label was awarded during the annual Forum International de la Cybersécurité (FIC) in January 2017 at Lille.

10.2.2. Teaching

- Master: Emmanuelle Anceaume, *Research in Computer Science - Distributed Algorithms*, 20 hours of lecture, M2; Université Rennes 1, France;
- Licence: Christophe Bidan, *Algorithms and Data Structures*, 36 hours of lecture including 7.5 hours of lectures, L3 - first year of the engineering degree, CentraleSupélec, France;
- Licence: Christophe Bidan, *Software Engineering*, 12 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Licence: Christophe Bidan, *Supervision of student project*, 1 project, L3 - first year of the engineer degree, CentraleSupélec, France;
- Master: Christophe Bidan is responsible for the module *Secured information systems*, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Christophe Bidan, *Applied cryptography*, 6 hours of lecture, M2 - master 2 degree, University of Rennes 1, France;

- Master: Christophe Bidan, *Applied cryptography*, 15 hours including 6 hours of lecture, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master : Christophe Bidan, *Cryptographic Protocols*, 6 hours of lecture, mastère CS (Cyber Security), CentraleSupélec, France;
- Master: Christophe Bidan, *Information systems*, 4.5 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Christophe Bidan, *Supervision of student project*, 2 projects, M1 - second year of the engineer degree, CentraleSupélec, France;
- Licence: Gilles Guette, *Algorith and Complexity*, 28 hours, L1 - Licence, ISTIC/University of Rennes, France;
- Licence: Gilles Guette, *Network Initiation*, 57.5 hours, L3 - Licence, ISTIC/University of Rennes, France;
- Licence: Gilles Guette, *Network Initiation*, 41.5 hours, L3 - first year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Network Routing*, 32 hours, M1 - second year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Mobile Network Routing*, 5 hours, M1 - second year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Advanced Network Services*, 10 hours, M1 - second year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Network Project*, 24 hours, M1 - second year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Security*, 28 hours, M1 - second year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Network and System Security*, 12 hours, M2 - third year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Network Modeling*, 18 hours, M2 - third year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Sensors Network*, 30 hours, M2 - Master, ISTIC/University of Rennes, France;
- Master: Gilles Guette, *Supervision of student*, Contrat de professionnalisation, M2 - third year of the engineer degree, ESIR, France;
- Master: Gilles Guette, *Supervision of student internship*, M2 - ISTIC/University of Rennes, France;
- Licence: Guillaume Hiet, *Algorithms and Data Structures*, 12.5 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Computer security and privacy for the engineer*, 8 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Buffer overflow vulnerabilities*, 16 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Buffer overflow vulnerabilities*, 16 hours, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;
- Master: Guillaume Hiet, *Pentest*, 19 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Pentest*, 3 hours, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;
- Master: Guillaume Hiet, *Introduction to Linux*, 3 hours, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;

- Master: Guillaume Hiet, *Java Security*, 4.5 hours, M2 - Mastère Spécialisé CS, CentraleSupélec, France;
- Master: Guillaume Hiet, *Linux Security*, 18 hours, M2 - Mastère Spécialisé CS , CentraleSupélec, France;
- Master: Guillaume Hiet, *Linux Security*, 7.5 hours, third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *LDAP*, 7.5 hours, third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Intrusion Detection*, 15 hours, M2 - Mastère Spécialisé CS, CentraleSupélec, France;
- Master: Guillaume Hiet, *Intrusion Detection*, 13.5 hours, M2 - third year of the engineer degree, M2 research degree of University of Rennes 1, CentraleSupélec, France;
- Master: Guillaume Hiet, *Security Monitoring*, 3 hours, M2, cycle "Sécurité Numérique", INHESJ, France;
- Master: Guillaume Hiet, *Computer Security*, 31.5 hours, M2, Mastère Spécialisé Architecte des Systèmes d'Information, CentraleSupélec, France;
- Master: Guillaume Hiet, *Intrusion Detection*, 16 hours, M2, University of Rennes 1, France;
- Master: Guillaume Hiet, *Intrusion Detection*, 10 hours, M2 - third year of the engineer degree, ESIR, France;
- Master: Guillaume Hiet, *Intrusion Detection*, 9 hours, M2, Université of Limoges, France;
- Master: Guillaume Hiet, *Firewall*, 6 hours, M2, University of Rennes 1, France;
- Master: Guillaume Hiet, *Supervision of student project*, 4 projects, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Supervision of student project*, 2 projects, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Hiet, *Supervision of student project*, 2 projects, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;
- Master:Jean-François Lalande, *Legal aspects of information security*, 3.5 hours, M2 - master CyberSecurity, CentraleSupélec, France;
- Master: Guillaume Hiet, *Android Malware*, 3.5 hours, M2, Mastère Spécialisé CS (Cyber Security), France;
- Master: Jean-François Lalande, *Supervision of student project*, 2 projects, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Jean-François Lalande, *Supervision of student project*, 2 projects, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Jean-François Lalande, *Supervision of student project*, 1 projects, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France;
- Licence : Ludovic Mé, *Software Engineering*, 18 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Licence : Ludovic Mé, *Software Engineering tutorials*, 6 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Licence : Ludovic Mé, *Software Engineering and Java development*, 18 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Master : Ludovic Mé, *Information systems tutorials*, 6 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

- Master : Ludovic Mé, *Supervision of student project*, 1 project, 38 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Licence: Guillaume Piolle, *Software engineering*, 1.5 hours, L3 - first year of the engineering degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Modelling, Algorithms and Programming*, 22 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Computer security and privacy*, 5 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Software project*, 3.5 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Relational databases*, 6 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Computer networks*, 30 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Security Policies*, 4.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Java programming*, 4.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Computer networks*, 9 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Software engineering*, 12 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Network Access Control*, 9 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Web development*, 32 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Privacy protection*, 18 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Computing project*, 60 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Guillaume Piolle, *Legal aspects of information security*, 4.5 hours, M2 - master CyberSecurity, CentraleSupélec, France;
- Licence : Eric Totel, *Foundations of computer science, data structures and algorithms*, 9 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Licence : Eric Totel, *Software Modeling*, 15 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Master : Eric Totel, *Operating Systems*, 30 hours, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master : Eric Totel, *C language*, 24 hours including 6 hours of lecture, M2 - master CS (Cyber Security), CentraleSupélec, France;
- Master : Eric Totel, *C language and C++ language*, 12 hours including 6 hours of lecture, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master : Eric Totel, *Dependability* , 9 hours including 7.5 hours of lecture, M2 - third year of the engineer degree and master research, CentraleSupélec, France;
- Master : Eric Totel, *Dependability*, 3 hours of lecture, M2 - third year of the engineer degree (ingénierie des systèmes automatisés), CentraleSupelec, France;

- Master : Eric Totel, *Dependability*, 4.5 hours of lecture, M2 - post-graduate training (master Architecture des Réseaux de Communication), CentraleSupélec, France;
- Master : Eric Totel, *Intrusion Detection*, 6 hours of lecture, M2 - M2 - master CS (Cyber Security), CentraleSupélec, France;
- Master : Eric Totel, *Intrusion Detection*, 9 hours of lecture, M2 - master 2 degree, University of Rennes 1, France;
- Master : Eric Totel, *Supervision of student project*, 4 projects, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master : Eric Totel, *Supervision of student project,* 1 project, M2 - third year of the engineer degree, CentraleSupélec, France;
- Licence: Frédéric Tronel, *Software engineering*, 40 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Licence: Frédéric Tronel, *Operating Systems*, 12 hours, L3 - first year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel is responsible of the M2 degree in *CyberSecurity* (mastère spécialisé), organized jointly by CentraleSupélec and Institut Mines Télécom (IMT) Atlantique, France;
- Master: Frédéric Tronel, *Operating systems*, 21 hours hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Compilers*, 18 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Automatic reasoning*, 4.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Assembly Language*, 6 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Buffer overflow vulnerabilities (theory and practice)*, 20.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Firewall*, 15 hours, M2 - third year of the engineer degree, CentraleSupélec, France;
- Master: Frédéric Tronel, *Calculability in distributed systems*, 6 hours, M2, jointly with University of Rennes 1 and CentraleSupélec, France;
- Master: Frédéric Tronel, *Computer network*, 8 hours, M2, jointly with University of Rennes 1 and CentraleSupélec, France;
- Licence : Valérie Viet Triem Tong, *Algorithms and Data Structures*, 36 hours of lecture including 7 hours of lectures, L3 - first year of the engineering degree, CentraleSupélec, France;
- Licence : Valérie Viet Triem Tong, *Supervision of student project*, 6 projects of 2nd year of the engineer degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Games Theory*, 18 hours, M1 - second year of the engineering degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Formal Methods*, 9 hours, M2 - third year of the engineering degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Intrusion detection using information flow control*, 9 hours, M2 / third year of the engineering degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Programming in Java*, 12 hours, M1 - international students (NplusI) second year of the engineering degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Small elements of decidability*, 7.5 hours, M2 - third year of the engineering degree, CentraleSupélec, France;

- Master : Valérie Viet Triem Tong, *Supervision of student project*, 1 project, mastere CS (Cyber Security), CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Supervision of student project*, 8 projects, M1 - second year of the engineer degree, CentraleSupélec, France;
- Master : Valérie Viet Triem Tong, *Supervision of student project*, 1 project year of the engineer degre, CentraleSupélec, France;
- Doctorant : Valérie Viet Triem Tong, *Malware analysis by OS information flow tracking*, 2 hours, Summerschool - Cyber in Berry, Bourges, France;

10.2.3. Supervision

10.2.3.1. Theses defended in 2017

- PhD: Laurent Georget, *Suivi de flux d'information correct pour les systèmes d'exploitation Linux*, Octobre 2017, supervised by Mathieu Jaume (25% - MdC LIP6), Guillaume Piolle (25%), Frédéric Tronel (25%), and Valérie Viet Triem Tong (25%);
- PhD: Deepak Subramanian, *Multi-level Information Flow Monitoring*, started in January 2013, supervised by Christophe Bidan (20%) and Guillaume Hiet (80%);
- PhD: Antoine Guellier, *Utilisation de la cryptographie homomorphe pour garantir le respect de la vie privée*, started in October 2013, supervised by Christophe Bidan (50%) and Nicolas Prigent (50%);
- PhD: Kun He, *Mise en œuvre de techniques de droit à l'oubli pour les contenus numériques*, started in October 2013, supervised by Christophe Bidan (50%) and Gaetan LeGuelvouit (50% - IRT B-Com);
- PhD: Solenn Brunet, *Privacy-preserving location-based services*, started in October 2014, supervised by Christophe Bidan(40%), Sébastien Gambs (30%) and Jacques Traoré (30% - Orange Labs Caen);
- PhD: Florian Grandhomme, *Protocole de routage externe type BGP dans un environnement réseaux tactiques adhoc mobiles : faisabilité et performances*, started in October 2014, supervised by Gilles Guette (50%), Adlen Ksentini (25% - Eurecom), and Thierry Plesse (25% - DGA MI).

10.2.3.2. Theses in progress

- PhD in progress: Mouna Hkimi, *Détection d'intrusion dans les systèmes distribués*, started in October 2013, supervised by Eric Totel (50%) and Michel Hurfin (50%);
- PhD in progress: Thomas Letan, *Contribution à la sécurité des couches basses des systèmes d'information*, started in January 2015, supervised by Guillaume Hiet (50%), Pierre Chifflier (25% - ANSSI), and Ludovic Mé (25%);
- PhD in progress: Damien Crémilleux, *Visualisation d'évènements de sécurité pour la supervision*, started in October 2015, supervised by Christophe Bidan (30%), Nicolas Prigent (35%), and Frédéric Majorczyk (35% - DGA MI);
- PhD in progress: Mourad Leslous, *Déclenchement automatique de codes jugés suspects dans les applications Android*, started in October 2015, supervised by Thomas Genet (20% - Celtique Inria project), Jean François Lalande (40% - INSA Centre Val de Loire), and Valérie Viet Triem Tong (40%);
- PhD in progress: Mounir Nasr Allah, *Contrôle de flux d'information par utilisation conjointe d'analyse statique et d'analyse dynamique accélérée matériellement*, started in November 2015, supervised by Guillaume Hiet (75%) and Ludovic Mé (25%);
- PhD in progress: Pernelle Mensah, *Adaptation de la Politique de Sécurité guidée par l'Évaluation du Risque dans les Infrastructures de Communication modernes*, started in January 2016, supervised by Eric Totel (25%), Guillaume Piolle (25%), Christine Morin (25% - Myriad Inria project), and Samuel Dubus (25% - Nokia);

- PhD in progress: David Lanoë, *Détection d'intrusion dans les applications distribuées : l'approche comportementale comme alternative à la corrélation d'alertes*, started in october 2016, supervised by Michel Hurfin (50%) and Eric Totel (50%);
- PhD in progress: Aurélien Trulla, *Caractérisation de malware Android par suivi de flux d'information et nouvelles techniques d'évasion*, started in October 2016, supervised by Jean Louis Lanet (25% - Tamis Inria project) and Valérie Viet Triem Tong (75%);
- PhD in progress : Ronny Chevalier , "Enhanced computer platform security through an intrusion-detection approach", started in November 2016, supervised by Guillaume Hiet (50%), Boris Balacheff (25% - HP), and Ludovic Mé (25%);
- PhD in progress: Laetitia Leichtnam, *Visualisation pour la caractérisation d'événements de sécurité*, started in october 2016, supervised by Eric Totel (40%), Nicolas Prigent (30%) and Ludovic Mé (30%);
- PhD in progress : Charles Xosanavongsa, *Combining Attack Specification and Dynamic Learning from traces for correlation rule generation*, started in december 2016, supervised by Eric Totel (50%) and Ludovic Mé (50%);
- PhD in progress : Pierre Graux, *Security of Hybrid Mobile Applications*, started in october 2017, supervised by Valérie Viet Triem Tong (50%) and Jean-Francçois Lalande (50%);
- PhD in progress : Vasile Cazacu, *Calcul distribué pour la fouille de données cliniques*, started February 2017, supervised by Emmanuelle Anceaume (50%) and Marc Cuggia (50%)
- PhD in progress : Aurélien Dupin, *Secure multi-partie computations*, started February 2016, supervised by Christophe Bidan(40%), David Pointchavalm (30% - ENS) and Renaud Dubois (30% - Thales).

10.2.3.3. Supervision of external PhD candidates

- LL. D. (Doctor of Laws) in progress: Gustav Malis, *Droit à l'effacement des données mises à disposition par les personnes elles-mêmes*, started in March 2014, supervised by Annie Blandin (80% - IODE) and Guillaume Piolle (20%);
- PhD in progress: Oualid Koucham, *Détection d'intrusions pour les systèmes de contrôle industriels*, started in January 2015, supervised by Stéphane Mocanu (50% - Gipsa-lab), Guillaume Hiet (25%), and Jean-Marc Thiriet (25% - Gipsa-lab);
- PhD in progress : Yves Mocquard, *Population protocols*, started in september 2015, supervised by Bruno Sericola (Dyonisos Inria project) and Emmanuelle Anceaume;.

10.2.4. Juries

Ludovic Mé was a member of the PhD committee for the following PhD and HDR thesis:

- Pierre Laperdrix, *Browser Fingerprinting: Diversity to Augment Authentication and Build Client-side Countermesures*, INSA of Rennes, 03/10/2017 (President of the Jury);

Ludovic Mé has reported the following PhD thesis:

- Pierre Parrend, *Emergent Industrial Ecosystems*, University of Strasbourg, 12/12/2017.

Christophe Bidan was a member of the PhD committee for the following PhD thesis:

- Jean Aimé Maxa, *Architecture de communication sécurisée d'une flotte de drones*, Université Toulouse 3 Paul Sabatier (UT3 Paul Sabatier), 28/06/2017;
- Eric Asselin, *Système de détection d'intrusion adapté au système de communication aéronautique ACARS*, Institut National Polytechnique de Toulouse (INP Toulouse), 28/06/2017 (reviewer);

Jean-François Lalande has reported the following PhD thesis:

- Julien Hatin, *Evaluation de la confiance dans un processus d'authentification*, 24/11/2017.

Eric Totel was a member of the PhD commitee for the following PhD thesis:

- Giannakou Anna, *Self-Adaptable Security Monitoring for IaaS Cloud Environments*, 06/07/2017 (President of the Jury).
- Yacine Hebbal, *Semantic monitoring mechanisms dedicated to security monitoring in IaaS cloud*, 18/09/2017 (President of the Jury).

Valérie Viet Triem Tong has reported the following PhD thesis:

- Franck de Goer de Herve, *Rétro-ingénierie de programmes binaires en une exécution - une analyse dynamique légère basée au niveau des fonctions*, 10/20/2017.

10.3. Popularization

Valérie Viet Triem Tong has participated to the scientific television show *l'Esprit Sorcier* recorded at *Musée des Sciences et de l'Industrie* during the *Fête de la Science*. She has also participated to the scientific promotion movie about *High Security Laboratory* recorded at Nancy.

Damien Crémilleux has participated to the event "Ma thèse en 180s" and the "RCC challenge: my thesis 3.0" for the popularization of his work's thesis on security visualization.

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] S. BRUNET. *Design of Anonymous Accreditation and Data Anonymization Mechanisms*, Université de Rennes 1 [UR1], November 2017, https://hal-centralesupelec.archives-ouvertes.fr/tel-01655322

[2] L. GEORGET. *Correct information flow tracking for Linux operating systems*, Université Rennes 1, September 2017, https://hal.inria.fr/tel-01657148

[3] F. GRANDHOMME. *Inter-domain routing studies (BGP-like) for tactical mobile ad hoc networks : feasibility and performances*, Universite de Rennes 1, November 2017, https://hal.archives-ouvertes.fr/tel-01654631

[4] A. GUELLIER. *Strongly Private Communications in a Homogeneous Network*, Centrale Supélec, May 2017, https://hal-centralesupelec.archives-ouvertes.fr/tel-01644172

[5] K. HE. *Content Privacy and Access Control on Image-Sharing Platforms*, CentraleSupélec, September 2017, https://hal-centralesupelec.archives-ouvertes.fr/tel-01636207

Articles in International Peer-Reviewed Journals

[6] E. ANCEAUME, Y. BUSNEL. *Lightweight Metric Computation for Distributed Massive Data Streams*, in "Transactions on Large-Scale Data- and Knowledge-Centered Systems", April 2017, vol. 10430, n^{o} 33, pp. 1–39 [*DOI :* 10.1007/978-3-662-55696-2_1], https://hal.archives-ouvertes.fr/hal-01634353

International Conferences with Proceedings

[7] E. ANCEAUME, R. LUDINARD, M. POTOP-BUTUCARU, F. TRONEL. *Bitcoin a Distributed Shared Register*, in "SSS 2017 - 19th International Symposium on Stabilization, Safety, and Security of Distributed Systems", Boston, MA, United States, Lecture Notes in Computer Science, Springer, November 2017, vol. 10616, pp. 456-468 [*DOI :* 10.1007/978-3-319-69084-1_34], https://hal.archives-ouvertes.fr/hal-01522360

[8] M. ASSAF, D. A. NAUMANN, J. SIGNOLES, E. TOTEL, F. TRONEL. *Hypercollecting Semantics and its Application to Static Analysis of Information Flow*, in "POPL 2017 - ACM Symposium on Principles of Programming Languages", Paris, France, ACM SIGPLAN Notices - POPL '17, ACM, January 2017, vol. 52, n° 1, pp. 874-887 [*DOI :* 10.1145/3009837.3009889], https://hal.inria.fr/hal-01618360

[9] I. BOUREANU, D. GERAULT, P. LAFOURCADE, C. ONETE. *Breaking and fixing the HB+DB protocol*, in "Wisec 2017 - Conference on Security and Privacy in Wireless and Mobile Networks", Boston, United States, July 2017, pp. 241 - 246 [*DOI :* 10.1145/3098243.3098263], https://hal.archives-ouvertes.fr/hal-01588562

[10] R. CHEVALIER, M. VILLATEL, D. PLAQUIN, G. HIET. *Co-processor-based Behavior Monitoring: Application to the Detection of Attacks Against the System Management Mode*, in "ACSAC 2017 - 33rd Annual Computer Security Applications Conference", Orlando, United States, Proceedings of the 33rd Annual Computer Security Applications Conference, ACM, December 2017, vol. 2017, pp. 399-411 [*DOI :* 10.1145/3134600.3134622], https://hal.inria.fr/hal-01634566

[11] *Best Paper*
L. GEORGET, M. JAUME, G. PIOLLE, F. TRONEL, V. VIET TRIEM TONG. *Information Flow Tracking for Linux Handling Concurrent System Calls and Shared Memory*, in "15th International Conference on Software Engineering and Formal Methods (SEFM 2017)", Trento, Italy, A. CIMATTI, M. SIRJANI (editors), LNCS, Springer International Publishing, September 2017, pp. 1-16 [*DOI :* 10.1007/978-3-319-66197-1_1], http://hal.upmc.fr/hal-01535949.

[12] L. GEORGET, M. JAUME, G. PIOLLE, F. TRONEL, V. VIET TRIEM TONG. *Verifying the Reliability of Operating System-Level Information Flow Control Systems in Linux*, in "5th International FME Workshop on Formal Methods in Software Engineering", Buenos Aires, Argentina, IEEE Press, May 2017, pp. 10-16 [*DOI :* 10.1109/FORMALISE.2017.1], https://hal.inria.fr/hal-01535862

[13] T. LAJOIE-MAZENC, R. LUDINARD, E. ANCEAUME. *Handling Bitcoin Conflicts Through a Glimpse of Structure*, in "Proceedings of the 32nd ACM SIGAPP Symposium On Applied Computing", Marrakesh, Morocco, Proceedings of the 32nd ACM SIGAPP Symposium On Applied Computing, April 2017 [*DOI :* 10.1145/3019612.3019657], https://hal.archives-ouvertes.fr/hal-01634368

[14] L. LEICHTNAM, E. TOTEL, N. PRIGENT, L. MÉ. *STARLORD: Linked Security Data Exploration in a 3D Graph*, in "VizSec - IEEE Symposium on Visualization for Cyber Security", Phoenix, United States, October 2017, pp. 1 - 4 [*DOI :* 10.1109/VIZSEC.2017.8062203], https://hal.inria.fr/hal-01619234

[15] M. LESLOUS, V. VIET TRIEM TONG, J.-F. LALANDE, T. GENET. *GPFinder: Tracking the Invisible in Android Malware*, in "12th International Conference on Malicious and Unwanted Software", Fajardo, Puerto Rico, IEEE Conputer Society, October 2017, https://hal-centralesupelec.archives-ouvertes.fr/hal-01584989

[16] P. MENSAH, S. DUBUS, W. KANOUN, C. MORIN, G. PIOLLE, E. TOTEL. *Connectivity Extraction in Cloud Infrastructures*, in "CNSM 2017 - 13th International Conference on Network and Service Management", Tokyo, Japan, November 2017, pp. 1-5, https://hal.inria.fr/hal-01593346

[17] P. MENSAH, S. DUBUS, W. KANOUN, C. MORIN, G. PIOLLE, E. TOTEL. *Connectivity Graph Reconstruction for Networking Cloud Infrastructures*, in "NCA 2017 - 16th IEEE International Symposium on Network Computing and Applications", Cambridge, MA, United States, October 2017, https://hal.inria.fr/hal-01612988

[18] Y. MOCQUARD, B. SERICOLA, E. ANCEAUME. *Probabilistic Analysis of Counting Protocols in Large-scale Asynchronous and Anonymous Systems*, in "Proceedings of the 16th IEEE International Conference on Network Computing and Applications", Boston, United States, October 2017, https://hal.archives-ouvertes.fr/hal-01580275

[19] V. VIET TRIEM TONG, A. TRULLA, M. LESLOUS, J.-F. LALANDE. *Information flows at OS level unmask sophisticated Android malware*, in "14th International Conference on Security and Cryptography", Madrid, Spain, SciTePress, July 2017, vol. 6, pp. 578-585 [*DOI :* 10.5220/0006476705780585], https://hal-centralesupelec.archives-ouvertes.fr/hal-01535678

[20] M. A. WAHAB, P. COTRET, M. N. ALLAH, G. HIET, V. LAPOTRE, G. GOGNIAT. *ARMHEx: A hardware extension for DIFT on ARM-based SoCs*, in "Field Programmable Logic (FPL)", Ghent, Belgium, September 2017, https://hal.archives-ouvertes.fr/hal-01558473

[21] M. A. WAHAB, P. COTRET, M. NASR ALLAH, G. HIET, V. LAPOTRE, G. GOGNIAT. *ARMHEx: a framework for efficient DIFT in real-world SoCs*, in "Field Programmable Logic (FPL)", Ghent, Belgium, September 2017, https://hal.archives-ouvertes.fr/hal-01558475

National Conferences with Proceedings

[22] G. BROGI, V. VIET TRIEM TONG. *Sharing and replaying attack scenarios with Moirai*, in "RESSI 2017: Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information", Autrans, France, May 2017, https://hal.archives-ouvertes.fr/hal-01533275

[23] G. FOURNIER, P. AUDREN DE KERDREL, P. COTRET, V. VIET TRIEM TONG. *DroneJack: Kiss your drones goodbye!*, in "SSTIC 2017 - Symposium sur la sécurité des technologies de l'information et des communications", Rennes, France, June 2017, pp. 1-8, https://hal.inria.fr/hal-01635125

[24] L. GEORGET, M. JAUME, G. PIOLLE, F. TRONEL, V. VIET TRIEM TONG. *Suivi de flux d'information correct sous Linux*, in "16èmes journées AFADL (Approches formelles dans l'assistance au développement de logiciels)", Montpellier, France, A. IDANI, N. KOSMATOV (editors), June 2017, pp. 19-26, http://hal.upmc.fr/hal-01535937

[25] N. RIVETTI, E. ANCEAUME, Y. BUSNEL, L. QUERZONI, B. SERICOLA. *Ordonnancement dynamique pour un équilibrage de charge quasi-optimal dans les systèmes de traitement de flux*, in "ALGOTEL 2017 - 19èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", Quiberon, France, May 2017, https://hal.archives-ouvertes.fr/hal-01519432

[26] M. A. –. WAHAB, P. COTRET, M. –. NASR ALLAH, G. –. HIET, V. LAPOTRE, G. –. GOGNIAT. *ARMHEx: embedded security through hardware-enhanced information flow tracking*, in "RESSI 2017 : Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information", Grenoble (Autrans), France, May 2017, https://hal.archives-ouvertes.fr/hal-01558155

Other Publications

[27] E. ANCEAUME, Y. BUSNEL. *Byzantine-tolerant Uniform Node Sampling Service*, November 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01634363

[28] Y. MOCQUARD, B. SERICOLA, E. ANCEAUME. *Probabilistic Analysis of Rumor Spreading Time*, November 2017, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01652777

References in notes

[29] G. BROGI, V. VIET TRIEM TONG. *TerminAPTor: Highlighting Advanced Persistent Threats through Information Flow Tracking*, in "8th IFIP International Conference on New Technologies, Mobility and Security", Larnaca , Cyprus, November 2016, https://hal.inria.fr/hal-01417612

[30] N. KISS, J.-F. LALANDE, M. LESLOUS, 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, The USENIX Association, May 2016, https://hal-centralesupelec.archives-ouvertes.fr/hal-01311917