IN PARTNERSHIP WITH:
CNRS

CentraleSupélec

Université Rennes 1

Activity Report 2016

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
Distributed Systems and middleware

Table of contents

Project-Team CIDRE

Creation of the Project-Team: 2011 July 01

Keywords:

Computer Science and Digital Science:

1.2.8. - Network security
1.3. - Distributed Systems
3.3.1. - On-line analytical processing
3.5.2. - Recommendation systems
4.1.1. - Malware analysis
4.1.2. - Hardware attacks
4.4. - Security of equipment and software
4.8. - Privacy-enhancing technologies
4.9.1. - Intrusion detection
4.9.2. - Alert correlation
7.1. - Parallel and distributed algorithms

Other Research Topics and Application Domains:

6.5. - Information systems
9.8. - Privacy

1. Members

Research Scientists

Emmanuelle Anceaume [CNRS, Researcher]
Michel Hurfin [Inria, Researcher, HDR]

Faculty Members

Christophe Bidan [Team Leader, CentraleSupelec, Professor, HDR]
Sébastien Gambs [Univ. Rennes I, Associate Professor, until Jan 2016, HDR]
Gilles Guette [Univ. Rennes I, Associate Professor]
Guillaume Hiet [CentraleSupelec, Associate Professor]
Mohamed Kasraoui [Univ. Rennes I, Associate Professor]
Julien Lolive [Univ. Rennes I, Associate Professor, until Aug 2016]
Ludovic Mé [CentraleSupelec, Professor, HDR]
Guillaume Piolle [CentraleSupelec, Associate Professor]
Nicolas Prigent [CentraleSupelec, Associate Professor, until Sep 2016]
Eric Totel [CentraleSupelec, Professor, HDR]
Frédéric Tronel [CentraleSupelec, Associate Professor]
Valérie Viet Triem Tong [CentraleSupelec, Associate Professor, HDR]

Engineer

Christopher Humphries [Inria]

PhD Students

Solenn Brunet [Orange Labs, granted by CIFRE]
Damien Crémilleux [CentraleSupelec]
Aurélien Dupin [Thales, granted by CIFRE]
Laurent Georget [Univ. Rennes I]

Florian Grandhomme [Univ. Rennes I]
Antoine Guellier [Univ. Rennes I]
Kun He [Inst. de Recherche Technologique B-COM, until Sep 2016]
Mouna Hkimi [Inria, until Oct 2016]
David Lanoé [Inria, from Oct 2016]
Laetitia Leichtnam [Min. de la Défense, from Oct 2016]
Mourad Leslous [Inria]
Thomas Letan [CentraleSupelec]
Pernelle Mensah [Bell Labs (Alcatel), granted by CIFRE]
Mounir Nasr Allah [CentraleSupelec]
Deepak Subramanian [CentraleSupelec, until Aug 2016]
Aurélien Trulla [Inria, from Oct 2016]
Charles Arya Xosanavongsa [Thales, from Feb 2016, granted by CIFRE]

Post-Doctoral Fellow
Chuanyou Li [Inria, until Apr 2016]

Administrative Assistant
Lydie Mabil [Inria]

Others
Ronny Chevalier [CentraleSupelec, Internship, until Jul 2016]
Thibaut Lajoie-Mazenc [CNRS, Internship, from Jun 2016 until Nov 2016]
Frédéric Majorczyk [DGA, External Collaborator]
Evan Pisani [Univ. Rennes I, Internship, from May 2016 until Jul 2016]
Guereguin Der Sylvestre Sidibe [CentraleSupelec, Internship, from Apr 2016 until Aug 2016]
Jianqiao Xu [CentraleSupelec, Internship, from Jul 2016]

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 these 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, being not a team specialized in cryptography, we consider that we can rely on strong unbroken cryto-systems.

3.2. Intrusion Detection / Security Events Monitoring and Management

Today, we are 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 of the Year

5.1.1. Awards

Mounir Assaf, a former PhD student, has received the "prix de thèse du GDR GPL" in June 2016. His PhD thesis is entitled "évaluation des fuites d'information dans les logiciels critiques" and has been defended in 2015.

Emmanuelle Anceaume has received the Most Prolific Author Award during the NCA conference.

BEST PAPERS AWARDS:

[28]
D. SUBRAMANIAN, G. HIET, C. BIDAN. *Preventive Information Flow Control through a Mechanism of Split Addresses*, in "9th International Conference on Security of Information and Networks (SIN 2016)", Rutgers University, New Jersey, United States, July 2016, https://hal.inria.fr/hal-01344565

[24]
Y. MOCQUARD, B. SERICOLA, S. ROBERT, E. ANCEAUME. *Analysis of the Propagation Time of a Rumour in Large-scale Distributed Systems*, in "Symposium on Network Computing and Applications", Boston, United States, October 2016, This article has received the Best Student Paper Award, https://hal.archives-ouvertes.fr/hal-01354815

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.

- Partner: SUPELEC
- Contact: Frédéric Tronel
- URL: http://blare-ids.org

6.2. ELVIS

Extensible Log VISualization
KEYWORDS: Visualization - Cybersecurity - Intrusion Detection Systems (IDS) - SIEM - Cyber attack - Forensics
SCIENTIFIC DESCRIPTION

The studies that were performed since 2012 clearly showed that there was an important need for technologies that would allow analysts to handle in a consistent way the various types of log files that they have to study in order to detect intrusion or to perform forensic analysis. Consequently, we proposed this year ELVis, a security-oriented log visualization system that allows the analyst to import its log files and to obtain automatically a relevant representation of their content based on the type of the fields they are made of. First, a summary view is proposed. This summary displays in an adequate manner each field according to its type (i.e. categorical, ordinal, geographical, etc.). Then, the analyst can select one or more fields to obtain some details about it. A relevant representation is then automatically selected by the tool according to the types of the fields that were selected.

ELVis [35] has been presented in VizSec 2013 (part of Vis 2013) in October 2013 in Atlanta. A working prototype is currently being tuned in order to perform field trials with our partners in DGA-MI. Next year, we are planing to perform research on how various log files can be combined in the same representation.
FUNCTIONAL DESCRIPTION

ELVIS is a visualisation tool geared to system security which enables analysts to visually explore log files using relevant representations. The tool accepts many different types of log file and can easily be extended to accept new ones opportunistically. Thanks to its data typing mechanisms, it can automatically choose relevant representations depending on the type of data that the analyst wants to observe.

- Participant: Nicolas Prigent
- Partner: SUPELEC
- Contact: Nicolas Prigent
- URL: https://hal.inria.fr/hal-00875668

6.3. GEPETO

GEoPrivacy-Enhancing TOolkit
KEYWORDS: Cyber attack - Privacy - Mobility
SCIENTIFIC DESCRIPTION

(GEoPrivacy-Enhancing TOolkit) is an open source software for managing location data (currently in development in cooperation with LAAS). GEPETO can be used to visualize, sanitize, perform inference attacks and measure the utility of a particular geolocated dataset. For each of these actions, a set of different techniques and algorithms can be applied. The global objective of GEPETO is to enable a user to design, tune, experiment and evaluate various sanitization algorithms and inference attacks as well as visualizing the following results and evaluating the resulting trade-off between privacy and utility. An engineer (Izabela Moïse) has contributed to the development of a distributed version of GEPETO based on the MapReduce paradigm and the Hadoop framework that is able to analyze datasets composed of millions of mobility traces in a few minutes [30] .
FUNCTIONAL DESCRIPTION

GEPETO is an open source software for managing location data. GEPETO can be used to visualize, sanitize, perform inference attacks, and measures the utility of a particular geolocated dataset.

- Partners: CNRS - Université de Rennes 1
- Contact: Sébastien Gambs
- URL: https://gforge.inria.fr/projects/gepeto/

6.4. 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: SUPELEC
- Contact: Eric Totel
- URL: http://www.rennes.supelec.fr/ren/perso/etotel/GNG/index.html

6.5. GroddDroid

KEYWORDS: Android - Detection - Malware
FUNCTIONAL DESCRIPTION

GroddDroid

1- locates suspicious code in Android application

2-computes execution paths towards suspicious code

3- forces executions of suspicious code

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

6.6. Kharon platform

KEYWORDS: Android - Malware - Dynamic Analysis
FUNCTIONAL DESCRIPTION

This platform executes Android applications and computes a graph representing all the information flows that occurred in the operating system due to a malicious execution. It can then classify observed behavior as benign or malicious. Access to this platform is currently in physically controlled at the high security laboratory (LHS) of Rennes.

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

6.7. Netzob

FUNCTIONAL DESCRIPTION

Netzob is an opensource tool for reverse engineering, traffic generation and fuzzing of communication protocols. This tool allows to infer the message format (vocabulary) and the state machine (grammar) of a protocol through passive and active processes. Its objective is to bring state of art academic researches to the operational field, by leveraging bio-informatic and grammatical inferring algorithms in a semi-automatic manner.

- Participant: Georges Bossert
- Contact: Ludovic Mé
- URL: http://www.netzob.org/

6.8. VEGAS

Visualizing, Exploring and Grouping AlertS
KEYWORDS: Security - Visualization - Cybersecurity - Intrusion Detection Systems (IDS) - SIEM
SCIENTIFIC DESCRIPTION

VEGAS explore the hypothesis that is is possible to offer to front-line security operators a visualization tool that allows the to perform a first informed triage of the alerts that were received from IDSes so as to group them and transmit them to security analysts in a relevant way.
FUNCTIONAL DESCRIPTION

VEGAS is a visualization tool that allows to easily identify, explore and group alerts generated by an IDS. This tool allows security operators to easily dispatch similar alerts to security analyst to help them study them more efficiently.

- Participants: Damien Cremilleux, Frédéric Majorczyk and Nicolas Prigent
- Partner: SUPELEC
- Contact: Damien Crémilleux

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 [1], 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.

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 [11], we describe 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). Our main contribution is showing that IFT can be used to highlight APTs. Additionally, we describe a generic representation of APTs and validate our IFT-based APT detector.

Inferring the normal behavior of an application: In [29], [6], [41], 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 aims at identifying the possible errors tolerated by the compacted automaton.

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. In [20], we focus on process-aware attacks detection in sequential control systems. We build on results from runtime verification and specification mining to automatically infer and monitor process specifications. Such specifications are represented by sets of temporal safety properties over states and events corresponding to sensors and actuators. The properties are then synthesized as monitors which report violations on execution traces. We develop an efficient specification mining algorithm and use filtering rules to handle the large number of mined properties. Furthermore, we introduce the notion of activity and discuss its relevance to both specification mining and attack detection in the context of sequential control systems. The proposed approach is evaluated in a hardware-in-the-loop setting subject to targeted process-aware attacks. Overall, due to the explicit handling of process variables, the solution provides a better characterization of the alerts and a more meaningful understanding of false positives.

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.

Illegal Information Flow in Web-browser: In the context of the CominLabs SECCLOUD project, we were interested in implementing our approach to detect illegal information flow in web-browser. We have proposed a new secure information flow control model specifically designed for JavaScript [28]. In our approach, we augment the standard symbol table with a mechanism that replaces the reference address for secret values based on the current execution stack. This mechanism also ensures that the secret is stored in a dedicated memory location thereby protecting the secret from any unintended leakage or modification by a malicious JavaScript. This work on detection of illegal information flow in JavaScript has received the best paper award at the 9th International Conference on Security of Information and Networks (SIN 2016) [28].

Later Deepak Subramanian has improved this approach and optimized the computation time required to determine the legacy of information flows. An approach which begins with a learning phase allows to increase the accuracy of the proposed solution. Information about the modified variables are kept in memory to perform a more accurate analysis of the indirect information flows. This self-correcting information flow control model for a web-browser is described in [27].

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. In [32], 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.

More generally, for his research activities during his PhD thesis, Mounir Assaf has received the 2016 thesis prize awarded by the GDR GPL (Engineering Programming and Software).

Characterizing Android Malwares: 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 customise 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 [39]. 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 [19] goes a step further from classical dynamic analysis of malware (http://kharon.gforge.inria.fr). Funded by the Labex CominLabs and involving partners of Centrale-Supélec, 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.

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

Additionally, the main challenge is to be able to trigger malicious behaviours even if the malware tries to escape dynamic analysis.

In this context, we have developed an original solution that mainly consists of 'helping the malware to execute'. In other words we slightly modify the bytecode of the infected application in order to defeat the protection against dynamic analysis and we execute the suspicious code in its most favourable execution conditions. Thus, our software helps us understand malware's objectives and the consequences on the health of a user's device. In particular, we use a global control flow graph (CFG) to exhibit an execution path to reach specific parts of code [42].

To achieve stealthiness when attacking a mobile device, an effective approach is the use of a covert channel built by two colluding applications to locally exchange data. Since this process is tightly coupled with the used hiding method, its detection is a challenging task, also worsened by the very low transmission rates. Using general indicators such as the energy consumed by the device, we propose in [5] an approach to detect the hidden data exchange between colluding applications and show its feasibility and effectiveness through different experimental results.

Our main research direction and challenge is to develop new and original protections against malicious applications that try to defeat classical dynamic analysis.

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 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 Dynamic Information Flow Control on the main CPU. Finally, in the context of the PhD thesis of Thomas Lethan (ANSSI), we investigate the use of formal methods to evaluate the security guarantees provided by hardware platforms, which combine different CPUs, chipsets and memories. 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. In [21], [37], we give 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 [43].

In [30] we introduce an efficient approach for DIFT (Dynamic Information Flow Tracking) implementations on reconfigurable chips. Existing solutions are either hardly portable or bring unsatisfactory time overheads. This work presents an innovative implementation for DIFT on reconfigurable SoCs such as Xilinx Zynq devices.

In [7], we detail a hardware-assisted approach for information flow tracking implemented on reconfigurable chips. Current solutions are either time-consuming or hardly portable (modifications of both software/hardware layers). This work takes benefits from debug components included in ARMv7 processors to retrieve details on instructions committed by the CPU. First results in terms of silicon area and time overheads are also given.

7.1.4. Vizualization

The large quantities of alerts generated by intrusion detection systems (IDS) make very difficult to distinguish on a network real threats from noise. To help solving this problem, we propose VEGAS [12], an alerts

visualization and classification tool that allows first line security operators to group alerts visually based on their principal component analysis (PCA) representation. VEGAS is included in a workflow in such a way that once a set of similar alerts has been collected and diagnosed, a filter is generated that redirects forthcoming similar alerts to other security analysts that are specifically in charge of this set of alerts, in effect reducing the flow of raw undiagnosed alerts.

Our research on visualization of security events has lead to two proofs-of-concept (See ELVIS and VEGAS 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. Christopher Humphries is a technology transfer engineer employed by Inria 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 [18], [17], [16], 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.

7.2.2. Fingerprinting

Active fingerprinting schemes were originally invented to deter malicious users from illegally releasing an item, such as a movie or an image. To achieve this, each time an item is released, a different fingerprint is embedded in it. In the context of the PhD of Julien Lolive, we have defined the first privacy-preserving asymmetric fingerprinting protocol based on Tardos codes [2]. This protocol is optimal with respect to traitor tracing. We also formally proved that our protocol achieves the properties of correctness, anti-framing, traitor tracing, as well as buyer- and item-unlinkability.

7.3. Communication and Synchronization in 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. In [14], [33], we describe and compare three solutions. Based on this analysis, we propose some preconizations to design Inter-domain protocols for MANET.

In [15], we present a coalition context and describe the functional hypothesis we used. Then, we propose a protocol that would fit such a network and conduct experimentation that tend to show that our proposition is quite efficient.

7.3.2. Communication and Synchronization Primitives

Use of Primitives to Limit Equivocation: We consider the approximate consensus problem in a partially connected network of n nodes where at most f nodes may suffer from Byzantine faults. In [22], we study under which conditions this problem can be solved using an iterative algorithm. A Byzantine node can equivocate: it may provide different values to its neighbors. To restrict the possibilities of equivocation, the 3-partial multicast primitive is considered. When a (correct or faulty) node uses this communication primitive, it provides necessarily the same value to the two identified receivers. Based on this communication primitive, a novel condition called f-resilient is proposed and proved to be necessary and sufficient to solve the approximate Byzantine consensus problem in a synchronous network.

The Test&Set Problem: In [35], we present a solution to the well-known problem of synchronization in a distributed asynchronous system prone to process crashes. This problem is also known as the Test&Set problem. The Test&Set is a distributed synchronization protocol that, when invoked by a set of processes, returns a unique winning process. This unique process is then allowed to use, for instance, a shared resource. Recently many advances in implementing Test&Set objects have been achieved, however all of them uniquely target the shared memory model. In this paper we propose an implementation of a Test&Set object for a message passing distributed system. This implementation can be invoked by any number $n \leq N$ of processes where N is the total number of processes in the system. We show in this paper, using a Markov model, that our implementation has an expected step complexity in O(log n) and we give an explicit formula for the distribution of the number of steps needed to solve the problem.

7.3.3. Dependability in Cloud Storage

The quantity of data in the world is steadily increasing bringing challenges to storage system providers to find ways to handle data efficiently in terms of dependability and in a cost-effectively manner. We have been interested in cloud storage which is a growing trend in data storage solution. For instance, the International Data Corporation (IDC) predicts that by 2020, nearly 40% of the data in the world will be stored or processed in a cloud. The thesis of Pierre Obame [3] addressed challenges around data access latency and dependability in cloud storage. We proposed Mistore, a distributed storage system that we designed to ensure data availability, durability, low access latency by leveraging the Digital Subscriber Line (xDSL) infrastructure of an Internet Service Provider (ISP). Mistore uses the available storage resources of a large number of home gateways, Points of Presence, and datacenters for content storage and caching facilities. Mistore also targets data consistency by providing multiple types of data consistency criteria and a versioning system. We also considered the data security and confidentiality in the context of storage systems applying data deduplication which is becoming one of the most popular data technologies to reduce the storage cost and we design a data deduplication method that is secure against malicious clients while remaining efficient in terms of network bandwidth and storage space savings.

7.3.4. Decentralized Cryptocurrency Systems

Decentralized cryptocurrency systems offer a medium of exchange secured by cryptography, without the need of a centralized banking authority. Among others, Bitcoin is considered as the most mature one [10]. Its popularity lies on the introduction of the concept of the blockchain, a public distributed ledger shared by all participants of the system. Double spending attacks and blockchain forks are two main issues in blockchain-based protocols. The first one refers to the ability of an adversary to use the very same bitcoin more than once, while blockchain forks cause transient inconsistencies in the blockchain. In [9], we show through probabilistic analysis that the reliability of recent solutions that exclusively rely on a particular type of Bitcoin actors, called miners, to guarantee the consistency of Bitcoin operations, drastically decreases with the size of the blockchain.

Some recent works have proposed to improve upon Bitcoin weaknesses. In [31], we analyze of one of these recent works, and shows through an analytical performance evaluation that new Bitcoin improvements are still needed.

7.3.5. 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 [23] 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. We propose a solution which guarantees with any high probability that after O(log n) interactions any agent outputs with a precision given in advance, the proportion of agents that start in state A. The population proportion problem is a generalization of both the majority and counting problems, and thus our solution solves both problems. We show that our solution is optimal in time and space. Simulation results illustrate our theoretical analysis.

Propagation Time of a Rumor: the context of this work is the well studied dissemination of information in large scale distributed networks through pairwise interactions. This problem, originally called rumor mongering, and then rumor spreading has mainly been investigated in the synchronous model. This model relies on the assumption that all the nodes of the network act in synchrony, that is, at each round of the protocol, each node is allowed to contact a random neighbor. In [24], we drop this assumption under the argument that it is not realistic in large scale systems. We thus consider the asynchronous variant, where at time unit, a single node interacts with a randomly chosen neighbor. We perform a thorough study of the total number of interactions needed for all the nodes of the network to discover the rumor.

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], [26] 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.

Load shedding is a technique employed by stream processing systems to handle unpredictable spikes in the input load whenever available computing resources are not adequately provisioned. A load shedder drops tuples to keep the input load below a critical threshold and thus avoid unbounded queuing and system trashing. In [38] we propose Load-Aware Shedding (LAS), a novel load shedding solution that, unlike previous works, does not rely neither on a pre-defined cost model nor on any assumption on the tuple execution duration. Leveraging sketches, LAS efficiently builds and maintains at runtime a cost model to estimate the execution duration of each tuple with small error bounds. This estimation enables a proactive load shedding of the input stream at any operator that aims at limiting queuing latencies while dropping as few tuples as possible. We provide a theoretical analysis. Furthermore, through an extensive practical evaluation based on simulations and a prototype, we evaluate its impact on stream processing applications, which validate the robustness and accuracy of LAS.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- **HP (2013-2016): 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. 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 started her PhD thesis in September 2014 within the context of a CIFRE contract with Orange Labs Caen. Her PhD subject concerns the development of privacy-preserving location-based services that are able to personalize the service provided to the user according to his current position while preserving his location privacy. In particular, Solenn Brunet adapts existing cryptographic primitives (private information retrieval, secure multiparty computation, secure set intersection, ...) or design novel ones to use them as building blocks for the construction of these privacy-preserving location-based services.

- **DGA: BGP-like Inter Domain routing protocol for tactical mobile ad hoc networks: feasibility, performances and quality of service**

  Florian Grandhomme has started his PhD thesis in October 2014 in cooperation with DGA-MI. The subject of the PhD is to propose new secure and efficient algorithms and protocols to provide inter-domain routing in the context of tactical mobile ad hoc network. The protocol proposed will have to handle context modification due to the mobility of 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 will have to be 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 will focus 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.

- **B-Com: Privacy Protection for JPEG Content on Image-Sharing Platforms**

  Kun He was hired as a PhD in September 2013 by the IRT B-Com. The subject of the PhD was the protection of users' privacy while publishing images on image-sharing platforms. The proposed solution is an image encryption algorithm that preserve the image format after encryption, and the

experimentation have shown that the proposed encryption algorithm can be used on several widely used image-sharing platforms such as Flickr, Pinterest, Google+, Facebook and Twitter.

- **Thalès: Privacy and Secure Multi-party Computation**

  Aurélien Dupin has started his PhD thesis in January 2016 within the context of a CIFRE contract with Thalès. His PhD subject concerns the development of privacy-preserving location-based services based on secure multi-party computation. As part of his Master of Science from the ETS (Ecole de Technologie Supérieure) in Montreal, co-supervised by Prof. Jean-Marc ROBERT (ETS) and Prof. Christophe BIDAN (CentraleSupélec), Mr Aurélien DUPIN has already addressed the issue and proposed multi-party computation protocols to provide evidence of geolocations while ensuring the secrecy of the geographical location of participants protocols. The thesis is an opportunity to continue the work initiated during the Master of Science.

- **Thalès: 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.

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 COMINLAB contract (2012-2016): "SecCloud" - http://www.seccloud.cominlabs.ueb.eu/** Attacks targeting web browsers constitute a major threat. We tackled in the context of the SecCloud project attacks induced by client-side code execution (javascript, flash or html5). Existing security mechanisms such as os-level access control often are not sufficient to pre- vent client-side browser attacks as the web browser is granted the same privileges as the user. The idea is to monitor information flows within the web browser in order to enforce a security information flow policy. Such a policy should allow to define fine-grained in- formation flow rules between user data and distant web sites. We proposed a new secure information flow control model specifically designed for JavaScript. This study was conducted in cooperation with other Inria Teams (Ascola and Celtique). Deepak Subramanian is doing his PhD in the context of this project.
- **Labex COMINLAB contract (2013-2018): "DeSceNt" - http://www.descent.cominlabs.ueb.eu** In DeSceNt, we propose to investigate how decentralized home-based networks of plug computers can support personal clouds according to sound architectural principles, mechanisms, and programming abstractions. To fulfill this vision we see three core scientific challenges, which we think must be overcome. The first challenge, decentralized churn-poor design, arises from the nature of plug federations, which show much lower levels of churn than traditional peer-to-peer environments. The second challenge, quasi-causal consistency, is caused by the simultaneous needs to produce a highly scalable environment (potentially numbering millions of users), that also offers collaborative editing capabilities of mutable data-structures (to offer rich social interactions). The third and final challenge, intuitive data structures for plug programming, arises from the need by programmers for intuitive and readily reusable data-structures to rapidly construct rich and robust decentralized personal

cloud applications. This study is conducted in cooperation with other teams (GDD Team (University of Nantes), Inria team ASAP)

- **Labex COMINLAB 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, it this dataset, all malware are entirely manually reverse and documented. We have also developed an analysis platform. This platform is currently under private deployment.

- **Labex COMINLAB contract (2015-2018): "HardBlare-Security" - http://www.hardblare.cominlabs.ueb.eu/**

  The general context of the HardBlare project is to address Dynamic Information Flow Control 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 DIFC operations are delegated to a coprocessor. Nevertheless, such approaches are based on modified processors. Beyond the fact hardware-assisted DIFC is hardly adopted, existing works do not take care of coprocessor security and multicore/multiprocessor embedded systems.

  We plan to implement DIFC 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 DIFC using static analysis performed at compile-time. Another objective is to manage labels for persistent memory (i.e., files) using a modified OS kernel.

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.

9.2.2. Inria Project Labs

- **CAPPRIS (2012-2016)**

  CAPPRIS stands for "Collaborative Action on the Protection of Privacy Rights in the Information Society". The main objective of CAPPRIS is to tackle the privacy challenges raised by the most recent developments and usages of information technologies such as profiling, data mining, social networking, location-based services or pervasive computing by developing solutions to enhance the protection of privacy in the Information Society. To solve this generic objective, the project focuses in particular on the following fundamental issues:

  – The design of appropriate metrics to assess and quantify privacy, primarily by extending and integrating the various possible definitions existing for the generic privacy properties such as anonymity, pseudonymity, unlinkability and unobservability, as well as notions coming from information theory or databases such as the recent but promising concept of differential privacy;

  – The definition and the understanding of the fundamental principles underlying "privacy by design", with the hope of deriving practical guidelines to implement notions such as data minimization, proportionality, purpose specification, usage limitation, data sovereignty and accountability directly in the formal specifications of our information systems;

  – The integration between the legal and social dimensions, intensely necessary since the developed privacy concepts, although they may rely on computational techniques, must be in adequacy with the applicable law (even in its heterogeneous and dynamic nature). In particular, privacy-preserving technologies cannot be considered efficient as long as they are not properly understood, accepted and trusted by the general public, an outcome which cannot be achieved by the means of a mathematical proof.

  Three major application domains have been identified as interesting experimentation fields for this work: online social networks, location-based services and electronic health record systems. Each of these three domains brings specific privacy-related issues. The aim of the collaboration is to apply the techniques developed to the application domains in a way that promotes the notion of privacy by design, instead of simply considering them as a form of privacy add-ons on the top of already existing technologies. CAPPRIS is a joint project between Inria, LAAS-CNRS, Université de Rennes I, Supélec, Université de Namur, Eurecom, and Université de Versailles.

  In addition of the scientific advances in the field of privacy, members of CAPPRIS are actively involved in the animation and federation of the French community on privacy, through the APVP workshop but also interdisciplinary colloquiums.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

The **PANOPTESEC** project (http://www.panoptesec.eu) started on the 1st of November 2013 and ended in 2016. It deals with the automated and assisted security management of IT and SCADA system. The main objective of PANOPTESEC is to provide an integrated solution that will allow to efficiently monitor SCADA systems, detect intrusions and react to them. To that end, it encompasses many of the research topics that are addressed by the CIDRE team: alerts aggregation and correlation, policy-aware intrusion detection, architecture-aware intrusion detection, automated trust management, trust-based automated reaction and visualization.

The CIDRE team is involved in the project on all of these aspects. The partners are:

- REHA (BE),
- Nokia-Lucent Bell Labs France (FR),
- Epistematica (IT),
- the University of Rome (IT),
- the University of Hamburg (GE),
- the Institut Mines-Telecom (FR),
- ACEA (IT),
- CentraleSupélec (FR).

This year, our work focused on design and implementation but also on the integration phase. Most of our work focused on WP5 and WP6, that deal with the IDS event correlation system and the visualization system.

9.4. International Initiatives

9.4.1. Inria International Partners

9.4.1.1. 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 two conference publications in 2016, one in Middelware [25] and the other one in Algotel [26].

Since several years, Michel Hurfin works with Professor Yun Wang (Southeast University, Nanjing, China). Their joint work focuses on convergence and synchronization problems in unreliable distributed systems prone to byzantine failures. In 2016, we investigate the iterative approximate byzantine consensus problem during a joint work with Chuanyou Li [22]. A visit of Professor Yun Wang in Rennes is planned next year.

9.5. International Research Visitors

9.5.1. Visits of International Scientists

Prof. Jean-Marc Robert from ETS (Ecole Supérieure de Technologie) of Montréal has made several short visits in the CIDRE research group in 2016.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific Events Organisation

10.1.1.1. General Chair, Scientific Chair

Emmanuelle Anceaume served as the general chair of OPODIS 2015 (19th International Conference on Principles of Distributed Systems), December 2015, Rennes, France.

10.1.1.2. Member of the Organizing Committees

Christophe Bidan served as a member of the organization committee of C&ESAR 2016 (23rd Computers & Electronics Security Applications Rendez-vous), November 2016, Rennes, France.

Nicolas Prigent served as a member of the organization committee of SSTIC 2016 (Symposium sur la sécurité des technologies de l'information et des communications), June 2016, Rennes, France.

Frédéric Tronel served as a member of the organization committee of SSTIC 2016 (Symposium sur la sécurité des technologies de l'information et des communications), June 2016, Rennes, France.

10.1.2. Scientific Events Selection

10.1.2.1. Chair of Conference Program Committees

Nicolas Prigent serves as a program chair of VizSec 2016 (IEEE Symposium on Visualization for Cyber Security), October 2016, Baltimore, MD, USA.

10.1.2.2. Member of the Conference Program Committees

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

- Algotel 2016 (18èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications), May 2016, Bayonne, France.
- DSN 2016 (46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks), June 2016, Toulouse, France.
- ATC 2016 (13th IEEE International Conference on Advanced and Trusted Computing), July 2016, Toulouse, France.
- PECCS 2016 (6th International Joint Conference on Pervasive and Embedded Computing and Communication Systems), July 2016, Lisbon, Portugal.
- TrustCom 2016 (5th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, security track), August 2016, Tianjin, China.
- SRDS 2016 (35th International Symposium on Reliable Distributed Systems), September 2016, Budapest, Hungary.
- NCA 2016 (15th International Symposium on Network Computing and Applications), October 2016, Cambridge, MA, USA.

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

- CRiSIS 2016 (11th International Conference on Risks and Security of Internet and Systems), September 2016, Roscoff, France.
- C&ESAR 2016 (23rd Computers & Electronics Security Applications Rendez-vous), November 2016, Rennes, France.
- IWTCC 2016 (3rd International Workshop on Trust in Cloud Computing), December 2016, Shanghai, China.

Christopher Humphries served as a member of the program committee of VizSec 2016 (IEEE Symposium on Visualization for Cyber Security), October 2016, Baltimore, MD, USA.

Michel Hurfin served as a member of the following program committees:

- Ubisafe 2016 (8th IEEE International Symposium on UbiSafe Computing) August 2016, Tianjin, China.
- CARI 2016 (13rd African Conference on Research in Computer Science and Applied Mathematics), October 2016, Hammamet, Tunisia.

Frédéric Majorczyck served as a member of the program committee of VizSec 2016 (IEEE Symposium on Visualization for Cyber Security), October 2016, Baltimore, MD, USA.

Ludovic Mé served as a member of the following program committees:

- CARI 2016 (13rd African Conference on Research in Computer Science and Applied Mathematics), October 2016, Hammamet, Tunisia.
- AICCSA 2016 (13th ACS/IEEE International Conference on Computer Systems and Applications), November 2016, Agadir, Morocco.

Nicolas Prigent served as a member of the following program committees:

- SSTIC 2016 (Symposium sur la sécurité des technologies de l'information et des communications), June 2016, Rennes, France.
- GraMSec 2016 (3rd International workshop on Graphical Models for Security), June 2016, Lisbon, Portugal.

Eric Totel served as a member of the program committee of Ubisafe 2016 (8th IEEE International Symposium on UbiSafe Computing), August 2016, Tianjin, China.

Frédéric Tronel served as a member of the program committee of SSTIC 2016 (Symposium sur la sécurité des technologies de l'information et des communications) June 2016, Rennes, France.

10.1.2.3. Reviewer

- Laurent Georget - AICCSA 2016 (13th ACS/IEEE International Conference on Computer Systems and Applications).
- Gilles Guette - ICISSP 2016 (International Conference on Information System Security and Privacy) and AICCSA 2016 (13th ACS/IEEE International Conference on Computer Systems and Applications).
- Michel Hurfin - NCA 2016 (15th International Symposium on Network Computing and Applications).
- Ludovic Mé - NETYS 2016 (5th International Conference on NETworked sYStems).
- Valérie Viet Triem Tong - ICISSP 2016 (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 Elsevier JPDC (Journal of Parallel and Distributed Computing).
- Ludovic Mé - journal "Revue Africaine de la Recherche en Informatique et Mathématique Appliquée".
- Guillaume Piolle - IJIS (International Journal on Information Security) and IEEE IS (Intelligent Systems).
- Valérie Viet Triem Tong - IEEE TPDS (Transactions on Parallel and Distributed Systems).

10.1.4. Invited Talks

Eric Totel has been invited to SEC2 (2nd workshop on Security in Clouds), July 2016, Lorient, France. He has given a talk about "Anomaly Based Intrusion Detection in Distributed Applications without global clock".

Valérie Viet Triem Tong has been invited to the Journées scientifiques Inria for a short presentation entitled Helping malware to execute themselves. She was also invited to give a talk during the Séminaire Aristote at the école Polytechnique (Palaiseau, France). Her presentation was concerning Android Malware analysis. Lastly, she has been invited at the 4th International Symposium on Information Systems Security (CISSI'2016 Morocco) for a invited talk about the need and the challenges in Education of formal computer programming.

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. Scientific Expertise

Guillaume Piolle has been heard by the LIBE commission of the 82nd Internal Session of the European Youth Parliament, on "Data encryption, data protection and terrorism".

10.1.7. 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.

Valérie Viet Triem Tong is member of the group working on the new Master proposal in computer science (for both CentraleSupelec and Inria)

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

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, *Network Initiation*, 57.5 hours, L3 - Licence, ISTIC/University of Rennes 1, 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, *Supervision of student project*, 1 project, M2 - third year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Supervision of student internship*, M2 - Université Claude Bernard Lyon 1, France, Institut Francophone International, Hanoï, Viet-Nam;

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;

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, *Operating systems tutorials*, 3 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, *Algorithms*, 16.5 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

Licence : Guillaume Piolle, *Software engineering*, 18 hours, L3 - first year of the engineer degree, CentraleSupélec, France;

Master : Guillaume Piolle, *Modelling, Algorithms and Programming*, 30 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master : Guillaume Piolle, *Computer security and privacy*, 9 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master : Guillaume Piolle, *Computer networks*, 9 hours, M1 - second year of the engineer degree, CentraleSupélec, France;

Master : Guillaume Piolle, *Software project*, 8.5 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*, 18 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*, 18 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master : Guillaume Piolle, *Privacy protection*, 4.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Master : Guillaume Piolle, *Computing project*, 40 hours, M2 - third year of the engineer degree, CentraleSupélec, France;

Licence : Eric Totel, *Models and programming languages*, 19.5 hours including 10.5 hours of lecture, L3 - first year of the engineer degree, CentraleSupélec, France;

Licence : Eric Totel, *Foundations of computer science, data structures and algorithms*, 6 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, *Computer systems' architecture*, 60 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*, 8 hours of lecture, M2 - master 2 degree, University of Rennes 1, France;

Master : Eric Totel, *Intrusion Detection*, 4 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 Télécom Bretagne, 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*, 2 projects mastere CS (Cyber Security), 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, Inria, Summerschool - Cyber in Bretagne, France;

10.2.2. Supervision

PhD : Julien Lolive, *Entrelacement des mécanismes d'identification et de respect de la vie privée pour la protection des contenus externalisés*, May 2016, supervised by Caroline Fontaine (50% - Télécom-Bretagne) and Sébastien Gambs (50%);

PhD : Erwan Godefroy, *Définition et évaluation d'un mécanisme de génération de règles de corrélation liée à l'environnement*, September 2016, supervised by Michel Hurfin (33%), Eric Totel (33%), and Frédéric Majorczyk (34% - DGA MI);

PhD : Pierre Obame Meye, *Sûreté de fonctionnement dans le nuage de stockage*, December 2016, supervised by Emmanuelle Anceaume (33%), Frédéric Tronel (33%), and Philippe Raipin Parvedy (34% - Orange Labs);

PhD in progress: Deepak Subramanian, *Multi-level Information Flow Monitoring*, started in January 2013, supervised by Christophe Bidan (20%) and Guillaume Hiet (80%);

PhD in progress: 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 in progress: 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 Gae¨tan LeGuelvouit (50% - IRT B-Com);

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: Solenn Brunet, *Privacy-preserving location-based services*, started in October 2014, supervised by Sébastien Gambs (50%) and Jacques Traoré (50% - Orange Labs Caen);

PhD in progress: Laurent Georget, *Validation Formelle d'un moniteur de flux d'information pour le noyau Linux*, started in October 2014, supervised by Mathieu Jaume (25% - MdC LIP6), Guillaume Piolle (25%), Frédéric Tronel (25%), and Valérie Viet Triem Tong (25%);

PhD in progress : Florian Grandhomme, *Protocole de routage externe type BGP dans un environnement réseaux tactiques adhoc mobiles : faisabilité, performances et qualité de service*, started in October 2014, supervised by Gilles Guette (50%), Adlen Ksentini (25% - Eurecom), and Thierry Plesse (25% - DGA MI);

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: 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: 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 20), Jean Françoi̧s 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'Evaluation 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 : Yves Mocquard, *Population protocols*, started in september 2015, supervised by Bruno Sericola (Dyonisos Inria project) and Emmanuelle Anceaume.

10.2.3. Juries

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

- Antoine Rault, *Protection de la vie privée des utilisateurs dans un système de recommandations collaboratif distribué*, University of Rennes 1, 06/23/2016 (President of the Jury);
- Tarek Sayeh, '*Contrôle sélectif de l'accès à des données RDF*', University of Lyon 1, 09/08/2016 (President of the Jury);
- Ronan-Alexandre Cherrueau, *Composition de techniques de sécurité pour préserver la vie privée dans le contexte de l'informatique en nuage*, Ecole des Mines de Nantes, 11/18/2016 (Reviewer).

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

- Siwar Kriaa, *Modélisation conjoint de la sûreté et de la sécurité pour l'évaluation des risques dans les systèmes cyber-physiques*, University of Paris-Saclay, Mars 2016 (President of the Jury);
- François Xavier Aguessy, *Evaluation Dynamique de Risque et Calcul de Réponses Basés sur des Modèles d'Attaques Bayésiens*, Telecom Sud-Paris and University Pierre & Marie Curie, September 2016. (Reviewer).

Guillaume Hiet was a member of the PhD committee for the PhD of Florent Marchand de Kerchov entitled *étendre des interpréteurs par détournement, ou comment étendre des interpréteurs sans en modifier le code*, prepared at Ecole des Mines de Nantes, 18 november 2016.

10.3. Popularization

Emmanuelle Anceaume was interviewed on the topic « Blockchain : comment le bitcoin révolutionne l'économie numérique ? » in a broadcast of "le labo des savoirs" (http://labodessavoirs.fr/emissions-du-labo/).

Guillaume Piolle has participated to the scientific popularization program *à la découverte de la recherche* aimed at secondary education pupils. His participation consisted in presentations about the objectives, methods and results of research activities in computer security and privacy (including, but not limited to our activities in CIDRE). It took place in high schools in Redon, Cesson-Sévigné and Dol-de-Bretagne.

Valérie Viet Triem Tong participates to (the stand and demo of) the 8h International Forum of CyberSecurity (FIC 2016).

Valérie Viet Triem Tong has published in Interstice a paper entitled "Lutter contre les codes malveillants" (https://interstices.info/jcms/p_91111/lutter-contre-les-codes-malveillants).

11. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] E. GODEFROY. *Definition and assessment of a mechanism for the generation of environment-specific correlation rules*, CentraleSupélec, September 2016, https://hal.archives-ouvertes.fr/tel-01415703

[2] J. LOLIVE. *Interleaving identification mechanisms and respect of privacy for the protection of outsourced content*, Télécom Bretagne, May 2016, https://hal.inria.fr/tel-01355495

[3] P. O. MEYE. *Dependability in Cloud Storage*, Université Rennes 1, December 2016, https://hal.archives-ouvertes.fr/tel-01413001

Articles in International Peer-Reviewed Journals

[4] E. ANCEAUME, Y. BUSNEL, E. SCHULTE-GEERS, B. SERICOLA. *Optimization Results for a Generalized Coupon Collector Problem*, in "Journal of Applied Probability", 2016, vol. 53, n^{o} 2, https://hal.inria.fr/hal-01397403

[5] L. CAVIGLIONE, M. GAGGERO, J.-F. LALANDE, W. MAZURCZYK, M. URBANSKI. *Seeing the Unseen: Revealing Mobile Malware Hidden Communications via Energy Consumption and Artificial Intelligence*, in "IEEE Transactions on Information Forensics and Security", April 2016, vol. 11, n^{o} 4, pp. 799-810 [*DOI :* 10.1109/TIFS.2015.2510825], https://hal.archives-ouvertes.fr/hal-01247495

Invited Conferences

[6] E. TOTEL, M. HKIMI, M. HURFIN, M. LESLOUS, Y. LABICHE. *Anomaly Based Intrusion Detection in Distributed Applications without global clock*, in "SEC2 2016 - Deuxième atelier sur la Sécurité dans les Clouds", Lorient, France, July 2016, https://hal.inria.fr/hal-01334608

International Conferences with Proceedings

[7] M. ABDUL WAHAB, P. COTRET, M. NASR ALLAH, G. HIET, V. LAPOTRE, G. GOGNIAT. *Towards a hardware-assisted information flow tracking ecosystem for ARM processors*, in "26th International Conference on Field-Programmable Logic and Applications (FPL 2016)", Lausanne, Switzerland, August 2016, https://hal.archives-ouvertes.fr/hal-01337579

[8] E. ANCEAUME, Y. BUSNEL, N. RIVETTI, B. SERICOLA. *Identifier des icebergs parmi des flux de données distribués*, in "ALGOTEL 2016 - 18èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", Bayonne, France, ALGOTEL 2016 - 18èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, May 2016, https://hal.archives-ouvertes.fr/hal-01303873

[9] E. ANCEAUME, T. LAJOIE-MAZENC, R. LUDINARD, B. SERICOLA. *Safety Analysis of Bitcoin Improvement Proposals*, in "IEEE Symposium on Network Computing and Applications", Boston, United States, IEEE, October 2016, https://hal.archives-ouvertes.fr/hal-01397685

[10] E. ANCEAUME, R. LUDINARD, B. SERICOLA. *L'empire romain ne doit pas être géré comme une petite île grecque*, in "ALGOTEL 2016 - 18èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", Bayonne, France, May 2016, https://hal.archives-ouvertes.fr/hal-01305334

[11] 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

[12] D. CRÉMILLEUX, C. BIDAN, F. MAJORCZYK, N. PRIGENT. *VEGAS: Visualizing, exploring and grouping alerts*, in "IEEE/IFIP International Workshop on Analytics for Network and Service Management", Istanbul, Turkey, April 2016, pp. 1097 - 1100 [*DOI :* 10.1109/NOMS.2016.7502968], https://hal.archives-ouvertes.fr/hal-01416464

[13] W. DE GROEF, D. SUBRAMANIAN, J. MARTIN, F. PIESSENS, D. LIEVEN. *Ensuring Endpoint Authenticity in WebRTC Peer-to-Peer Communication*, in "31st Annual ACM Symposium on Applied Computing (SAC 2016)", New York, United States, April 2016, https://hal.inria.fr/hal-01344572

[14] F. GRANDHOMME, G. GUETTE, A. KSENTINI, T. PLESSE. *Comparing inter-domain routing protocol assessment tools for MANET*, in "2016 IEEE International Conference on Communications (ICC)", Kuala Lumpur, Malaysia, 2016 IEEE International Conference on Communications (ICC), May 2016, https://hal.inria.fr/hal-01355402

[15] F. GRANDHOMME, G. GUETTE, A. KSENTINI, T. PLESSE. *ITMAN: An Inter Tactical Mobile Ad Hoc Network Routing Protocol*, in "MILCOM2016", Baltimore, United States, November 2016, https://hal.inria.fr/hal-01397710

[16] K. HE, C. BIDAN, G. LE GUELVOUIT. *Experimentation of Privacy Protection for JPEG Contents on Image-Sharing Platforms*, in "9th International Conference on Security of Information and Networks (SIN 2016)", Rutgers University, New Jersey, United States, July 2016, https://hal.inria.fr/hal-01344469

[17] K. HE, C. BIDAN, G. LE GUELVOUIT. *Privacy Protection for JPEG Content on Image-Sharing Platforms*, in "4th ACM Workshop on Information Hiding and Multimedia Security (IH&MMSEC 2016)", Vigo, Galicia, Spain, June 2016, https://hal.inria.fr/hal-01344472

[18] K. HE, C. BIDAN, G. LE GUELVOUIT. *Robust and Secure Image Encryption Schemes During JPEG Compression Process*, in "2016 IS&T International Symposium on Electronic Imaging (EI 2016)", San Francisco, California, United States, February 2016, https://hal.inria.fr/hal-01344471

[19] 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, USENIX Association, May 2016, pp. 1-12, https://hal-centralesupelec.archives-ouvertes.fr/hal-01311917

[20] O. KOUCHAM, S. MOCANU, G. HIET, J.-M. THIRIET, F. MAJORCZYK. *Detecting Process-Aware Attacks in Sequential Control Systems*, in "21st Nordic Conference on Secure IT Systems (NordSec 2016)", Oulu, Finland, November 2016, https://hal.inria.fr/hal-01361081

[21] T. LETAN, P. CHIFFLIER, G. HIET, P. NÉRON, B. MORIN. *SpecCert: Specifying and Verifying Hardware-based Software Enforcement*, in "21st International Symposium on Formal Methods (FM 2016)", Limassol, Cyprus, 21st International Symposium on Formal Methods (FM 2016), Springer, November 2016, https://hal.inria.fr/hal-01361422

[22] C. LI, M. HURFIN, Y. WANG, L. YU. *Towards a Restrained Use of Non-equivocation for Achieving Iterative Approximate Byzantine Consensus*, in "30th IEEE International Parallel and Distributed Processing Symposium (IPDPS)", Chicago, United States, May 2016, 10 p. [*DOI :* 10.1109/IPDPS.2016.62], https://hal.inria.fr/hal-01339477

[23] Y. MOCQUARD, E. ANCEAUME, B. SERICOLA. *Optimal Proportion Computation with Population Protocols*, in "Symposium on Network Computing and Applications", Boston, United States, IEEE, October 2016, https://hal.archives-ouvertes.fr/hal-01354352

[24] *Best Paper*
Y. MOCQUARD, B. SERICOLA, S. ROBERT, E. ANCEAUME. *Analysis of the Propagation Time of a Rumour in Large-scale Distributed Systems*, in "Symposium on Network Computing and Applications", Boston, United States, October 2016, This article has received the Best Student Paper Award, https://hal.archives-ouvertes.fr/hal-01354815.

[25] N. RIVETTI, E. ANCEAUME, Y. BUSNEL, L. QUERZONI, B. SERICOLA. *Online Scheduling for Shuffle Grouping in Distributed Stream Processing Systems Research Paper*, in "ACM/IFIP/USENIX Middleware 2016", Trento, Italy, ACM/IFIP/USENIX, December 2016 [*DOI :* 10.1145/2988336.2988347], https://hal.archives-ouvertes.fr/hal-01397658

[26] N. RIVETTI, L. QUERZONI, E. ANCEAUME, Y. BUSNEL, B. SERICOLA. *Groupement de clés efficace pour un équilibrage de charge quasi-optimal dans les systèmes de traitement de flux*, in "ALGOTEL 2016 - 18èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", Bayonne, France, ALGOTEL 2016 - 18èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications, May 2016, https://hal.archives-ouvertes.fr/hal-01303887

[27] D. SUBRAMANIAN, G. HIET, C. BIDAN. *A self-correcting information flow control model for the web-browser*, in "The 9th International Symposium on Foundations & Practice of Security (FPS'2016)", Québec City, Canada, October 2016, https://hal.inria.fr/hal-01398192

[28] *Best Paper*
D. SUBRAMANIAN, G. HIET, C. BIDAN. *Preventive Information Flow Control through a Mechanism of Split Addresses*, in "9th International Conference on Security of Information and Networks (SIN 2016)", Rutgers University, New Jersey, United States, July 2016, https://hal.inria.fr/hal-01344565.

[29] E. TOTEL, M. HKIMI, M. HURFIN, M. LESLOUS, Y. LABICHE. *Inferring a Distributed Application Behavior Model for Anomaly Based Intrusion Detection*, in "12th European Dependable Computing Conference", Gothenburg, Sweden, Proceedings of the 12th European Dependable Computing Conference, September 2016, https://hal.inria.fr/hal-01334596

Conferences without Proceedings

[30] M. ABDUL WAHAB, P. COTRET, M. NASR ALLAH, G. HIET, V. LAPOTRE, G. COGNIAT. *A portable approach for SoC-based Dynamic Information Flow Tracking implementations*, in "11ème Colloque du GDR SoC/SiP", Nantes, France, June 2016, https://hal-centralesupelec.archives-ouvertes.fr/hal-01311045

[31] E. ANCEAUME, R. LUDINARD, B. SERICOLA. *Relying on Consensus does not Make Bitcoin Safer*, in "Fast Abstract in the 46th Annual IEEE/IFIP International Conference on Dependable Systems and Networks", Toulouse, France, M. ROY, J. A. LOPEZ, A. CASIMIRO (editors), DSN2016-FAST-ABSTRACT, June 2016, https://hal.archives-ouvertes.fr/hal-01316541

[32] M. ASSAF, J. SIGNOLES, E. TOTEL, F. TRONEL. *The Cardinal Abstraction for Quantitative Information Flow*, in "Workshop on Foundations of Computer Security 2016 (FCS 2016)", Lisbon, Portugal, June 2016, https://hal.inria.fr/hal-01334604

[33] F. GRANDHOMME, G. GUETTE, A. KSENTINI, T. PLESSE. *Comparaison d'outils d'évaluation de performance des protocoles de routage inter-MANET*, in "13ème Conference Francophone sur les Nouvelles Technologies de la Répartition (NOTERE 2016)", Paris, France, July 2016, https://hal.inria.fr/hal-01355407

[34] P. MENSAH. *Dynamic Topology Extraction in Cloud Infrastructures*, in "Second workshop on Security in Clouds (SEC2)", Lorient, France, July 2016, https://hal.inria.fr/hal-01399251

Research Reports

[35] E. ANCEAUME, F. CASTELLA, A. MOSTEFAOUI, B. SERICOLA. *Performance Evaluation of a Distributed Synchronization Protocol*, Inria ; Irisa ; Lina ; Irmar, March 2016, https://hal.inria.fr/hal-01283064

[36] G. BONNORON, D. CRÉMILLEUX, S. T. BULUSU, X. ZHU, G. VALADON. *Survey and analysis of DNS infrastructures*, CNRS, 2016, https://hal.archives-ouvertes.fr/hal-01407640

[37] T. LETAN, P. CHIFFLIER, G. HIET, P. NÉRON, B. MORIN. *SpecCert: Specifying and Verifying Hardware-based Security Enforcement*, CentraleSupélec ; Agence Nationale de Sécurité des Systèmes d'Information, 2016, 20 p. , https://hal.inria.fr/hal-01356690

[38] N. RIVETTI, E. ANCEAUME, Y. BUSNEL, L. QUERZONI, B. SERICOLA. *Load-Aware Shedding in Stream Processing Systems*, LINA-University of Nantes ; Sapienza Università di Roma (Italie) ; Irisa ; Inria Rennes, May 2016, https://hal.inria.fr/hal-01311970

Scientific Popularization

[39] V. VIET TRIEM TONG, J.-F. LALANDE, M. LESLOUS. *Challenges in Android Malware Analysis*, in "ERCIM News", July 2016, n^{o} 106, pp. 42-43, https://hal-centralesupelec.archives-ouvertes.fr/hal-01355122

[40] V. VIET TRIEM TONG. *Lutter contre les codes malveillants*, in "Interstices", December 2016, https://hal.inria.fr/hal-01427326

Other Publications

[41] M. HKIMI. *Apprentissage d'un mode`le comportemental d'une application distribue´e pour la de´tection d'intrusion*, May 2016, Rendez-Vous de la Recherche et de l'enseignement de la Sécurité des Systèmes d'Information (RESSI 2016), Poster, https://hal.inria.fr/hal-01334612

[42] M. LESLOUS, J.-F. LALANDE, V. VIET TRIEM TONG. *Using Implicit Calls to Improve Malware Dynamic Execution*, May 2016, 37th IEEE Symposium on Security and Privacy, Poster, https://hal.archives-ouvertes.fr/hal-01304326

[43] M. NASR ALLAH, G. HIET, M. ABDUL WAHAB, P. COTRET, G. GOGNIAT, V. LAPOTRE. *HardBlare: a Hardware-Assisted Approach for Dynamic Information Flow Tracking*, April 2016, Séminaire des doctorantes et doctorants en informatique de la Société Informatique de France, Poster, https://hal-centralesupelec.archives-ouvertes.fr/hal-01311032