IN PARTNERSHIP WITH:
CNRS

SUPELEC (Rennes)

Université Rennes 1

Activity Report 2015

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

Ludovic Mé [Team leader, CentraleSupélec, Professor, HdR]
Christophe Bidan [CentraleSupélec, Professor, HdR]
Sébastien Gambs [Univ. Rennes I, Associate Professor, Inria Research Chair, HdR]
Gilles Guette [Univ. Rennes I, Associate Professor]
Guillaume Hiet [CentraleSupélec, Associate Professor]
Mohamed Kasraoui [Univ. Rennes I, from Sep 2015]
Jean-Francois Lalande [ENSI Bourges, Associate Professor, until Aug 2015]
Guillaume Piolle [CentraleSupélec, Associate Professor]
Nicolas Prigent [CentraleSupélec, Associate Professor]
Eric Totel [CentraleSupélec, Professor, HdR]
Frédéric Tronel [CentraleSupélec, Associate Professor]
Valérie Viet Triem Tong [CentraleSupélec, Associate Professor, HdR]

Engineers

Radoniaina Andriatsimandefitra Ratsisahan [Inria]
David Lanoe [CentraleSupélec]

PhD Students

Simon Boche [Univ. Rennes I]
Solenn Brunet [Orange Labs, granted by CIFRE]
Damien Crémilleux [CentraleSupélec, from Mar 2015]

Laurent Georget [Univ. Rennes I]
Erwan Godefroy [DGA]
Florian Grandhomme [Univ. Rennes I]
Antoine Guellier [Univ. Rennes I]
Kun He [Inst. de Recherche Technologique B-COM]
Mouna Hkimi [Inria]
Christopher Humphries [Inria, until Dec 2015]
Paul Lajoie-Mazenc [Univ. Rennes I, until Sep 2015]
Mourad Leslous [Inria, from Feb 2015]
Thomas Letan [ANSSI]
Julien Lolive [Univ. Rennes I]
Yves Mocquard [Univ. Rennes I, from Mar 2015 to Aug 2015]
Mounir Nasr Allah [CentraleSupélec, from Nov 2015]
Pierre Obame Meye [Orange]
Mounir Assaf [CEA, until Feb 2015]
Regina Paiva Melo Marin [Inria, until Sep 2015, granted by DGA]
Deepak Subramanian [CentraleSupélec]

Post-Doctoral Fellow
Chuanyou Li [Inria]

Administrative Assistant
Lydie Mabil [Inria]

Others
Adrien Abraham [CentraleSupélec, intern, from Feb 2015 until Jun 2015]
Nicolas Kiss [CentraleSupélec, intern, from Apr 2015 until Sep 2015]
Thomas Lepesant [Univ. Rennes I, intern, from Jun 2015 until Aug 2015]
Carlos Rosar Kos Lassance [Univ. Rennes I, intern, from Mar 2015 until Sep 2015]
Mario Julián Sackmann [Inria, intern, until Jan 2015]
Mohamed Kasraoui [ATER, Univ. Rennes I, from Sep 2015]
Romaric Ludinard [ATER, Univ. Rennes I,until Aug 2015]
Frédéric Majorczyk [external collaborator, DGA]

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 three following topics: Intrusion Detection, Privacy Protection, and Trust Management.

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.

By contrast with this traditional conception, we are convinced that by looking at information systems as a combination of possibly revisited basic protocols, each one specified by a set of properties such as synchronization and agreement, security properties should emerge. This vision is shared by others and in particular by Myers *et al.* [64], whose objectives are to explore new methods for constructing distributed systems that are trustworthy in the aggregate even when some nodes in the system have been compromised by malicious attackers.

In accordance with this vision, the first main characteristic of the CIDRE group is to gather researchers from the two aforementioned communities, in order to address intentional failures, using foundations and approaches coming from both communities. The second main characteristic of the CIDRE group lies in the scope of the systems it considers. Indeed, we consider three complementary levels of study:

- The Node Level: 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. Node security management must be the focus of a particular attention, since from the user point of view, security of one's own devices is crucial. Sensitive information and services must therefore be locally protected against various forms of attacks. This protection may take a dual form, namely prevention and detection.
- The Group Level: Distributed applications often rely on the identification of sets of interacting entities. These subsets are either called groups, clusters, collections, neighborhoods, spheres, or communities according to the criteria that define the membership. Among others, the adopted criteria may reflect the fact that its members are administrated by a unique person, or that they share the same security policy. It may also relates to the localization of the physical entities, or the fact that they need to be strongly synchronized, or even that they share mutual interests. Due to the vast number of possible contexts and terminologies, we refer to a single type of set of entities, that we call set of nodes. We assume that a node can locally and independently identify a set of nodes and modify the composition of this set at any time. The node that manages one set has to know the identity of each of its members and should be able to communicate directly with them without relying on a third party. Despite these two restrictions, this definition remains general enough to include most of the examples mentioned above as particular cases. Of course, more restrictive behaviors can be specified by adding other constraints. We are convinced that security can benefit from the existence and the identification of sets of nodes of limited size, as they can help in improving the efficiency of the detection and prevention mechanisms.
- The Open Network Level: In the context of large-scale distributed and dynamic systems, interaction with unknown entities becomes an unavoidable habit, despite the induced risk. For instance, consider a mobile user that connects his laptop to a public Wifi access point to interact with his company. At this point, data (regardless or their value) are updated and managed through non trusted undedicated entities (i.e., communication infrastructure and nodes) that provide multiple services to multiple parties during that user connection. In the same way, the same device (e.g., laptop, smartphone, USB key) is often used for both professional and private activities, each activity accessing and manipulating decisive data.

The third characteristic of the CIDRE group is to focus on three different aspects of security, namely trust, intrusion detection and privacy, as well as on the bridges that exist between these aspects. Indeed, we believe that to study new security solutions for nodes, set of nodes and open network levels, one must take into account that it is now a necessity to interact with devices whose owners are unknown. To reduce the risk of relying on dishonest entities, a trust mechanism is an essential prevention tool that aims at measuring the capacity of a

remote node to provide a service compliant with its specification. Such a mechanism should allow to overcome ill-founded suspicions and to be aware of established misbehaviors. To identify such misbehaviors, intrusion detection systems are necessary. Such systems aim at detecting, by analyzing data flows, whether security policy violations have occurred. Finally, Privacy, which is now recognized as a fundamental individual right, should be respected despite the presence of tools and systems that continuously observe or even control users' actions or behaviors.

In all our studies, we consider a priori than 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

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 intrusion detection systems (IDS) is to detect, by analyzing some data generated on a monitored system, violations of the security policy. From our point of view, while useful in practice, misuse detection is intrinsically limited. Indeed, it requires to update the signatures database in real-time, similarly to what has to be done for antivirus tools. Given that thousands of machines are infected by malware everyday, such an approach may appear as insufficient, especially due to the incredible expansion of malware, drastically limiting the capabilities of human intervention and response. The CIDRE group takes the alternative approach, namely the anomaly approach, which consists in detecting a deviation from a referenced behavior. Specifically, we propose to study four complementary methods:

- Illegal Information Flow Detection: This first method intends to detect information flows that violate the security policy [66], [63]. Our goal is here to detect information flows in the monitored system that are allowed by the access control mechanism, but are illegal from the security policy point of view.
- Data Corruption Detection: This second method aims at detecting intrusions that target specific applications, and make them execute illegal actions by using these applications incorrectly [62], [65]. This approach complements the previous one in the sense that the incorrect use of the application can possibly be legal from the point of view of the information flows and access control mechanisms, but is incorrect considering the security policy.
- Visualization: This third method relies 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).
- Specification-Based Detection: This fourth method consists in comparing the monitored behavior of a system to a formal specification. This specification is focused on security aspects and can be extracted from a more generalized specification of the system. This approach is particularly appealing to detect intrusions in industrial control systems. Indeed, such environments exhibits 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 ressources (memory or CPU).

In these approaches, the access control mechanisms or the monitored applications can be either configured and executed on a single node, or distributed on a set of nodes. Thus, our approach must be studied at least at these two levels.

Here are some concrete examples of our research objectives (both short term and long term objectives) in the intrusion detection field:

- At node level, we apply the defensive programming approach (coming from the dependability field) to data corruption detection. The challenge is to determine which invariant/properties must be and

can be verified either at runtime or statically. Regarding illegal flow detection, we try to extend this method to build anti-viruses by determining virus signatures. We also investigate how dedicated hardware could increase the performance of Dynamic Information Flow Control by decreasing the runtime overhead of the monitoring process and protecting the monitor.

- At the set of nodes level, we revisit distributed problems such as clock synchronization, logical clocks, consensus, property detection, to extend the solutions proposed at node level to cope with distributed flow control checking mechanisms. Regarding illegal flow detection, we study the collaboration and consistency at the node and set of nodes levels to obtain a global intrusion detection mechanism. Regarding the data corruption detection approach, our challenge is to identify local predicates/properties/invariants so that global predicates/properties/invariants would emerge at the system level.

3.3. Privacy

In our world of ubiquitous technologies, each individual constantly leaves digital traces, related to his activities and interests, which can be linked to his identity. The protection of privacy is one of the greatest challenges that lie ahead and also an important condition for the development of the Information Society. Moreover, due to legality and confidentiality concerns, issues linked to privacy emerge naturally for applications working on sensitive data, such as medical records of patients or proprietary datasets of companies. Privacy Enhancing Technologies (PETs) are generally designed to respect both the principles of data minimization and data sovereignty. The data minimization principle states that only the information necessary to complete a particular application should be disclosed (and no more). This principle is a direct application of the legitimacy criteria defined by the European data protection directive (Article 7). This directive is currently being revised into a regulation that is going to strengthen the privacy rights of individuals and puts forward the concept of "privacy-by-design", which integrates the privacy aspects into the conception phase of a service or technology. The data sovereignty principle states that data related to an individual belong to him and that he should stay in control of how this data is used and for which purpose. This principle can be seen as an extension of many national legislations on medical data that consider that a patient record belongs to the patient, and not to the doctors that create or update it, nor to the hospital that stores it. A fundamental hindrance to the achievement of sovereignty is that the trust assumptions given to external entities are often too optimistic, and thus they are many realistic situations in which they might betrayed.

In the CIDRE project, we investigate PETs operating at three different levels (node, set of nodes or open distributed system) and that are generally based on a mix of different foundations such as cryptographic techniques, security policies and access control mechanisms just to name a few. Examples of domains in which privacy and utility aspects collide and that are studied within the context of CIDRE include: identity management, location-based services, social networks, distributed systems and data mining. Here are some concrete examples of our research goals in the privacy field:

- At the node level, we design privacy-preserving identification scheme, automated reasoning on privacy policies and policy-based adaptive PETs;
- At the set of nodes level, we augment distributed algorithms with privacy properties such as anonymity, unlinkability and unobservability;
- At the open distributed system level, we target both privacy concerns linked to location disclosure (which typically occur in location-based services) and to the distribution of social networking and data sharing applications. In the former case, we adopt a sanitization approach while in the latter one we consider privacy policies at user level, and their enforcement by all the intervening actors (*e.g,* at the level of the social network providers, of intermediate servers or of individual peers, depending on the distribution level of the applicative architecture). We design novel algorithms for the resolution of privacy policy conflicts between autonomous entities, taking new concepts into consideration, such as the notion of equity in the context of access control decisions.

3.4. Trust Management

While the distributed computing community relies on the trustworthiness of its algorithms to ensure systems availability, the security community historically makes the hypothesis of a Trusted Computing Base (TCB) that contains the security mechanisms (such as access controls, and cryptography) implementing the security policy. Unfortunately, as information systems get increasingly complex and open, the TCB management may itself get very complex, dynamic and error-prone. From our point of view, an appealing approach is to distribute and manage the TCB on each node and to leverage the trustworthiness of the distributed algorithms to strengthen each node's TCB. Accordingly, the CIDRE group studies automated trust management systems at all the three identified levels:

- At the node level, such a system should allow each node to evaluate by itself the trustworthiness of its neighborhood and to self-configure the security mechanisms it implements;
- At the group level, such a system might rely on existing trust relations with other nodes of the group to enhance the significance and the reliability of the gathered information;
- At the open network level, such a system should rely on reputation mechanisms to estimate the trustworthiness of the peers the node interacts with. The system might also benefit from the information provided by *a priori* trusted peers that, for instance, would belong to the same group (see previous item).

For the last two items, the automated trust management system will de facto follow the distributed computing approach. As such, emphasis will be put on the trustworthiness of the designed distributed algorithms. Thus, the proposed approach will provide both the adequate security mechanisms and a trustworthy distributed way of managing them. Regarding trust management, we still have research goals that are to be tackled. We briefly list hereafter some of our short and long term objectives at node, group and open networks levels:

1. At node level, we investigate how implicit trust relationships identified and deduced by a node during its interactions with its neighborhood could be explicitly used by the node (for instance by means of a series of rules) to locally evaluate the trustworthiness of its neighborhood. The impact of trust on the local security policy, and on its enforcement will be studied accordingly.
2. At the set of nodes level, we take advantage of the pre-existing trust relationship among the set of nodes to design composition mechanisms that would guarantee that automatically configured security policies are consistent with each group member security policy.
3. At the open distributed system level, we design reputation mechanisms to both defend the system against specific attacks (whitewashing, bad mouthing, ballot stuffing, isolation) by relying on the properties guaranteed at nodes and set of nodes levels, and guaranteeing persistent and safe feedback, and for specific cases in guaranteeing the right to be forgotten (i.e., the right to data erasure).

4. Application Domains

4.1. Application Domains

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 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

This year, beside the continuation of the work we realized on intrusion detection, privacy, or trust management (see below), we started to investigate new areas, namely malware analysis and hardware security.

A classical problem in dynamic analysis of malware is to be able automatically execute functions / methods of applications under monitoring. Dynamic analysis is helpful only if a malicious action has been observed, unfortunately some malicious functionality might be hidden or was trimmed for not executing when being called under certain circumstances / in certain environments. We have developed a new approach in the automatic triggering of suspicious code [25]. In few words, our approach consists in identify suspicious code and modifying the bytecode of the infected application in order to force the execution of the suspicious code. We have implemented GroddDroid a tool dedicated to the automatic triggering of Android malware. This work has received the Best Paper award at the 10th International Conference on Malicious and Unwanted Software.

We have initiated this year different research activities in the domain of hardware security. Our goal is not to protect devices against hardware attacks such as side-channels but to use hardware mechanisms to strengthen the software stack against traditional software attacks. In this context, we are particularly interested in software/hardware co-design approaches. More precisely, we want to focus on two challenges :

- We want to use formal methods to evaluate the security guarantees provided by hardware platforms, which combine different CPUs, chipsets and memories;
- We want to investigate how dedicated hardware could be used to monitor the whole software stack (from the firmware to the user-mode applications).

The first challenge is the main objective of a bilateral research project with the French national agency for computer security (ANSSI) started in January 2015. We supervise the PhD of Thomas Lethan in the context of this project. The second challenge is studied in a bilateral research project with HP Inc Research Labs. This project started in 2012 but has been extended this year. The main objective of this extension is to propose an approach combining software instrumentation and external monitoring by a dedicated hardware to detect intrusions in UEFI firmware. The second challenge is also studied in the HardBlare collaborative project started in October 2015. The goal of this project is to use a dedicated co-processor to enforce Dynamic Information Flow Control on the main CPU.

This year, we also contributed in the organization and program committee of two major events of our communities:

- the 19-th edition of OPODIS, the International Conference on Principles of Distributed Systems (https://opodis2015.irisa.fr) was organized in Rennes, December 14-17th, with Emmanuelle Anceaume as the general chair of the conference ;
- Nicolas Prigent was the program chair of the 12th IEEE International Symposium on Visualization for Cyber Security (VizSec) that took place in Chicago, Illinois, USA on the 26th of October, 2015.

5.1.1. Awards

Our work on GroddDroid has received the best paper award at 10th International Conference on Malicious and Unwanted Software .

BEST PAPER AWARD:

[25]
A. ABRAHAM, R. ANDRIATSIMANDEFITRA RATSISAHANANA, A. BRUNELAT, J.-F. LALANDE, V. VIET TRIEM TONG. *GroddDroid: a Gorilla for Triggering Malicious Behaviors*, in "10th International Conference on Malicious and Unwanted Software", Fajardo, Puerto Rico, IEEE Computer Society, October 2015, https://hal.inria.fr/hal-01201743

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 at the OS level for a single node and a set of nodes.
FUNCTIONAL DESCRIPTION

Blare IDS is a set of tools that implements our approach to illegal information flow detection at the OS level for a single node and a set of nodes.

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

6.2. ELVIS

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

The studies that were performed last year 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 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. In the PANOPTESEC project, we will also perform some research on visualization for security monitoring in the context of SCADA systems.
FUNCTIONAL DESCRIPTION

ELVIS is a log visualization tool that allows analyst-friendly log explorations through automated selection of adequate representations. Many log formats can be used and it is quite simple to add new ones. ELVis has been presented in VizSec 2013 (part of Vis 2013) in October in Atlanta.

- Participant: Nicolas Prigent
- Partner: CentraleSupélec
- Contact: Nicolas Prigent

6.3. GEPETO

GEoPrivacy-Enhancing TOolkit
KEYWORDS: 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: Université de Rennes 1 - CNRS
- 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: CentraleSupélec
- Contact: Eric Totel
- URL: http://www.rennes.supelec.fr/ren/perso/etotel/GNG/index.html

6.5. JBlare

FUNCTIONAL DESCRIPTION

JBlare is a Java Virtual Machine (JVM) hypervisor, able to track information flows inside Java programs. Being a modified JVM, it runs vanilla java applications. A cooperation mode with KBlare affords both IDS more precision. JBlare can use hybrid analysis combining dynamic analysis with static analysis using Soot.

- Contact: Guillaume Hiet
- URL: https://www.blare-ids.org/flavors/jblare/

6.6. 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/

6.7. GroddDroid

Automatic Triggering of Android Malware
KEYWORDS: Malware analysis
SCIENTIFIC DESCRIPTION GroddDroid is a tool dedicated to the automatic triggering of suspicious code in Android applications. GroddDroid copes with a classical problem in dynamic analysis which is the triggering of malicious actions. To avoid dynamic analysis, malware authors develop some protections that delay the malicious executions. GroddDroid overrides these protections by modifying the bytecode of the infected applications and reconstructing the application. The modified application can thus be executed and monitored.

- Partner: CentraleSupélec
- Contact: Valérie Viet Triem Tong
- URL: http://kharon.gforge.inria.fr/grodddroid.html

7. New Results

7.1. Intrusion detection

7.1.1. Alert Correlation in Distributed Systems

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 [59], [38], [19], 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. The transformation relies on a detailed description of various aspects of the real execution environment (topology of the system, deployed services, etc.). Consequently, the generated correlation rules are tightly linked to the characteristics of the monitored information system. The proposed transformation process has been implemented in a prototype that generates correlation rules expressed in an attack description language called Adele. Additionally, a work has been performed to assess the approach on real environment, and to evaluate the accuracy of the rules built.

In the context of the PhD of Mouna Hkimi, we propose a 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. 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 curent work aims at identifying the possible errors tolerated by the compacted automaton.

7.1.2. Android Malware Analysis

We explore how information flows induced by a tainted application are helpful to understand how this tainted application interacts within other components inside the operating system. For that purpose, we have defined a new data structure called System Flow Graph representing in a graph how a marked data is disseminated (inside the operating system). We have shown that this data structure is helpful to understand and represent malicious behaviors [31]. Our main challenge is thus to be able to produce relevant graphs which means being able to really observe malicious executions.

For that purpose we developed GroddDroid [25] a tool dedicated to the automatic triggering of Android malware. GroddDroid makes a first static analysis of the application bytecode. During this analysis, GroddDroid identifies the suspicious parts of the bytecode and modifies the bytecode in order to exhibit an execution path that leads to these suspicious parts. The application is later reconstructed/recompiled in order to be executed. This way, GroddDroid offers a way to force the suspicious code to be executed and then observed.

7.1.3. Comparative Study of Alert Formats

In the context of the SECEF project, we conduced a comparative study of different existing alert formats [39]. We analyzed two proprietary formats, CEF (HP ArcSight) and LEEF (IBM QRADAR), as well as 4 standard formats, IDMEF (IETF), CEE (MITRE), CIM and CADF (DMTF). We proposed several metrics to compare them based on an accurate revue of every fields proposed by each format. The results show that IDMEF is the most expressive and structured format. However, some fields proposed by other formats are not covered in IDMEF. We proposed some modification of the alert format to take those limitations into account.

7.1.4. Visualization

This year, research on viusalization for security was oriented towards two objectives. First, as we did during the previous years, we tried to provide solution for security analysts to better analyze *a posteriori* events related to security that are happening on a system. Christopher Humphries, who was the first CIDre Ph.D. student on this topic defended his Ph.D. Thesis *User-Centered Security Events Visualization* this December. We should also mention that we presented a prototype of our tool ELVIS during the FIC 2015 in Lille on the Pôle Cyber-Défense area.

This year, we also started research on a new topic in visualization for security. By contrast with our previous work that was dedicated to forensics, i.e. *a posteriori* analysis of security events, we started this year to study real time analysis of alerts generated by an IDS. The idea here is to allow better monitoring of what is currently happening on a system. We proposed VEGAS, a tool that allows front-line security operators to perform a first triage of the alerts to provide consistent groups of alerts to security analysts. A new Ph.D. student, Damien Crémilleux, was hired on a DGA-MI funding, to work on this topic. VEGAS was presented during the poster session of VizSec 2015 [58] that took place in Chicago, Illinois, USA on the 26th of October 2015.

7.2. Privacy

7.2.1. The Right to be Forgotten

The right to be forgotten, or to oblivion, is an aspect of privacy rights. It relates to the need for individuals to be able to leave a part of their past behind them, to change their mind about something or to take a new start in a given domain. The final report of the DAO project [53] presents an analysis of the concept from a

multidisciplinary point of view, including a sociological study, a legal state of the art assorted with insights of possible evolutions, and a technical state of the art along with the proposal of a new architecture [22]. A joint technical and legal analysis of the conceptual and technical issues specific to social networks is also proposed. From the point of view of a computer scientist, the most obvious issue with the right to be forgotten is the ability to control the deletion of a piece of information once it has been disclosed and disseminated. In the general case, no guarantees can be provided, but under certain conditions it is possible to enforce remote deletion with reasonable guarantees. In general, it implies that architectural and applicative choices are made beforehand, either to allow for future decisions regarding data made available in a controlled framework, like late modifications of its access policy or the triggering of its destruction, or to plan deletion from the beginning and set a time-to-leave when disclosing the data within a particular environment, or . The approach designed in CIDRE, relying on both ephemeral publication and data degradation techniques, falls in the latter category, improving the utility for third parties (when compared to existing ephemeral publication techniques) and building a new trade-off with the users' privacy needs, by making different versions of the original data, more or less precise, available for different durations, the more detailed information being lost the quickliest.

CIDRE also contributes, through the B<>com IRT, to the supervision (by Annie Blandin, professor at Télécom Bretagne, and Guillaume Piolle) of Gustav Malis's doctoral work in law in the domain of a restrictive case of the right to be forgotten. In this context, very original contributions have been made at the intersection between the two fields. In particular, a joint analysis has been proposed on the roles of legal and computing tools for the implementation of the right to be forgotten [50]. In particular, it seems that the two domains consider the issue with very different perspectives: the computer scientist almost takes for granted that he cannot rely on regulations and on "security through legality", hence the tools he designs are intended to directly empower the user, putting him in control of his data by using preventive protection techniques. The tools may fail though, or more likely their applicability conditions may not suit all scenarios. When issues arise they may be captured by the regulatory framework, which intends to provide means for reparation and restoration. Both approaches fail to encompass all possible situations and to solve all potential issues, but they provide users and citizens with complementary tools.

The work combining computer science and law conducted in the DAO projet as well as the main conclusions of the project have also been presented in interdisciplinary colloquium by Sébastien Gambs and Maryline Boizard [48], [47].

7.2.2. Private and Secure Location-based Services

Mobility has always been an important aspect of human activities. Nowadays problems of congestion in urban areas due to the massive usage of cars, last-minutes travel needs and progress in information and communication technologies encourage the rise of new transport modes. Among those are carpooling services, which let car owners share the empty seats of their cars with other travellers having the same travel destination. However, the way carpooling services are implemented today raises several privacy issues. In a recent paper, together with researchers from LAAS-CNRS we have proposed to use privacy enhancing technologies to improve the quality of carpooling services by specially taking in consideration privacy aspects [46].

In addition, publishing directly human mobility data raises serious privacy issues due to its inference potential, such as the (re-)identification of individuals. To address these issues and to foster the development of such applications in a privacy-preserving manner, we propose in a recent paper [26] a novel approach in which Call Detail Records (CDRs) are summarized under the form of a differentially-private Bloom filter for the purpose of privately estimating the number of mobile service users moving from one area (region) to another in a given time frame. Our sanitization method is both time and space efficient, and ensures differential privacy while solving the shortcomings of a solution recently proposed. We also report on experiments conducted using a real life CDRs dataset, which show that our method maintains a high utility while providing strong privacy.

Finally, in authentication protocols, a relay attack allows an adversary to impersonate a legitimate prover, possibly located far away from a verifier, by simply forwarding messages between these two entities. The effectiveness of such attacks has been demonstrated in practice in many environments, such as ISO 14443-compliant smartcards and car-locking mechanisms. Distance-bounding (DB) protocols, which enable the

verifier to check his proximity to the prover, are a promising countermeasure against relay attacks. In such protocols, the verifier measures the time elapsed between sending a challenge and receiving the associated response of the prover to estimate their proximity. So far, distance bounding has remained mainly a theoretical concept. Indeed in practice, up to our knowledge only three ISO 14443-compliant implementations of DB protocols exist. The first two are implemented on proprietary smartcards while the last one is available on a highly-customized and dedicated hardware. In a recent paper [35], we demonstrated a proof-of-concept implementation of the Swiss-Knife DB protocol on smartphones running in RFID-emulation mode. To our best knowledge, this is the first time that such an implementation has been performed. Our experimental results are encouraging as they show that relay attacks introducing more than 1.5 ms are directly detectable (in general off-the-shelf relay attacks introduce at least 10 ms of delay). We also leverage on the full power of the ISO-DEP specification to implement the same protocol with 8-bit challenges and responses, thus reaching a better security level per execution without increasing the possibility of relay attacks. The analysis of our results leads to new promising research directions in the area of distance bounding.

7.3. Trust

Reputation mechanisms allow users to mutually evaluate their trust. This is achieved through the computation of a reputation score summarizing their past behaviors. Depending on these scores, users are free to accept or refuse to interact with each other. Existing solutions often rely on costly cryptographic tools that may lead to impractical solutions. We have proposed in [41], [40], [28] usable privacy preserving reputation mechanisms. These mechanisms are distributed and handles non-monotonic ratings. Evaluation made on our mechanism reveals it to be fully usable even with cheap on-board computers. This is a very encouraging result as it shows that privacy does not impede utility and accuracy. This has been achieved by combining distributed algorithms and cryptographic schemes. Our mechanism is independent of the reputation model, that is, our system can integrate any reputation model, preferably one using both positive and negative ratings.

In a mobile ad hoc network we have also considered the problem of designing a reputation system that allows to update and to propagate the computed reputation scores while tolerating Byzantine failures [42]. Each time a correct node uses directly a service, it can determine by itself the quality of service currently provided. This fresh and valid rating information is broadcast immediately to all its current neighbors. Then, while the mobile node moves, it can receive from other nodes other recommendations also related to the same service. Thus it updates continuously its own opinion. Meanwhile it continues to broadcast this updated information. The freshness and the validity of the received/sent information become questionable. We propose a protocol that allows a node to ignore a second hand information when this information is not fresh or not valid. In particular, fake values provided by Byzantine nodes are eliminated when they are not consistent with those gathered from correct nodes. When the quality of service stabilizes, the correct nodes are supposed to provide quite similar recommendations. In this case, we demonstrate that the proposed protocol ensures convergence to a range of possible reputation scores if a necessary condition is satisfied by the mobile nodes. Simulations are conducted in random mobility scenarios. The results show that our algorithm has a better performance than typical methods proposed in previous works.

7.4. Other Topics Related to Security or Distributed Computing

7.4.1. Detection of distributed denial of service attacks

A Denial of Service (DoS) attack tries to progressively take down an Internet resource by flooding this resource with more requests than it is capable to handle. A Distributed Denial of Service (DDoS) attack is a DoS attack triggered by thousands of machines that have been infected by a malicious software, with as immediate consequence the total shut down of targeted web resources (*e.g.*, e-commerce websites). A solution to detect and to mitigate DDoS attacks it to monitor network traffic at routers and to look for highly frequent signatures that might suggest ongoing attacks. A recent strategy followed by the attackers is to hide their massive flow of requests over a multitude of routes, so that locally, these flows do not appear as frequent, while globally they represent a significant portion of the network traffic. The term “iceberg” has been recently introduced to

describe such an attack as only a very small part of the iceberg can be observed from each single router. The approach adopted to defend against such new attacks is to rely on multiple routers that locally monitor their network traffic, and upon detection of potential icebergs, inform a monitoring server that aggregates all the monitored information to accurately detect icebergs [29]. Now to prevent the server from being overloaded by all the monitored information, routers continuously keep track of the c (among n) most recent high flows (modeled as items) prior to sending them to the server, and throw away all the items that appear with a small probability p_i, and such that the sum of these small probabilities is modeled by probability p_0. Parameter c is dimensioned so that the frequency at which all the routers send their c last frequent items is low enough to enable the server to aggregate all of them and to trigger a DDoS alarm when needed. This amounts to compute the time needed to collect c distinct items among n frequent ones. A thorough analysis of the time needed to collect c distinct items appears in [16], [15].

7.4.2. Metrics Estimation on Very Large Data Streams

Huge data flows have become very common in the last decade. This has motivated the design of online algorithms that allow the accurate estimation of statistics on very large data flows. A rich body of algorithms and techniques have been proposed for the past several years to efficiently compute statistics on massive data streams. In particular, estimating the number of times data items recur in data streams in real time enables, for example, the detection of worms and denial of service attacks in intrusion detection services, or the traffic monitoring in cloud computing applications. Two main approaches exist to monitor in real time massive data streams. The first one consists in regularly sampling the input streams so that only a limited amount of data items is locally kept. This allows to exactly compute functions on these samples. However, accuracy of this computation with respect to the stream in its entirety fully depends on the volume of data items that has been sampled and their order in the stream. In contrast, the streaming approach consists in scanning each piece of data of the input stream on the fly, and in locally keeping only compact synopses or *sketches* that contain the most important information about these data. This approach enables us to derive some data streams statistics with guaranteed error bounds without making any assumptions on the order in which data items are received at nodes. Sketches highly rely on the properties of hashing functions to extract statistics from them. Sketches vary according to the number of hash functions they use, and the type of operations they use to extract statistics. The *Count-Min sketch* algorithm proposed by Cormode and Muthukrishnan in 2005 so far predominates all the other ones in terms of space and time needed to guarantee an additive ε-accuracy on the estimation of item frequencies. Briefly, this technique performs t random projections of the set of items of the input stream into a much smaller co-domain of size k, with $k = \lceil e/\epsilon \rceil$ and $t = \lceil \log(1/\delta) \rceil$ in which $0 < \epsilon, \delta < 1$. The user defined parameters ϵ and δ represent respectively the accuracy of the approximation, and the probability with which the accuracy holds. However, because k is typically much smaller than the total number of distinct items in the input stream, hash collisions do occur. This affects the estimation of item frequency when the size of the stream is large. In this work, we have proposed an alternative approach to reduce the impact of collisions on the estimation of item frequency. The intuition of our idea is that by keeping track of the most frequent items of the stream, and by removing their weight from the one of the items with which these frequent items collide, the over-estimation of non frequent items is drastically decreased [21].

We have also proposed a metric, called codeviation, that allows to evaluate the correlation between distributed streams [27]. This metric is inspired from classical metric in statistics and probability theory, and as such allows us to understand how observed quantities change together, and in which proportion. We then propose to estimate the codeviation in the data stream model. In this model, functions are estimated on a huge sequence of data items, in an online fashion, and with a very small amount of memory with respect to both the size of the input stream and the values domain from which data items are drawn. We give upper and lower bounds on the quality of the codeviation, and provide both local and distributed algorithms that additively approximates the codeviation among n data streams by using a sublinear number of bits of space in the size of the domain value from which data items are drawn, and the maximal stream length. To the best of our knowledge, such a metric has never been proposed so far.

7.4.3. Stream Processing Systems

Stream processing systems are today gaining momentum as a tool to perform analytics on continuous data streams. Their ability to produce analysis results with sub-second latencies, coupled with their scalability, makes them the preferred choice for many big data companies.

A stream processing application is commonly modeled as a direct acyclic graph where data operators, represented by nodes, are interconnected by streams of tuples containing data to be analyzed, the directed edges. Scalability is usually attained at the deployment phase where each data operator can be parallelized using multiple instances, each of which will handle a subset of the tuples conveyed by the operator's ingoing stream. Balancing the load among the instances of a parallel operator is important as it yields to better resource utilization and thus larger throughputs and reduced tuple processing latencies. We have proposed a new key grouping technique targeted toward applications working on input streams characterized by a skewed value distribution [44]. Our solution is based on the observation that when the values used to perform the grouping have skewed frequencies, e.g. they can be approximated with a Zipfian distribution, the few most frequent values (the *heavy hitters*) drive the load distribution, while the remaining largest fraction of the values (the *sparse items*) appear so rarely in the stream that the relative impact of each of them on the global load balance is negligible. We have shown, through a theoretical analysis, that our solution provides on average near-optimal mappings using sub-linear space in the number of tuples read from the input stream in the learning phase and the support (value domain) of the tuples. In particular this analysis presents new results regarding the expected error made on the estimation of the frequency of heavy hitters.

7.4.4. Randomized Message-Passing Test-and-Set

In [30], we have presented a solution to the well-known Test&Set operation in an asynchronous system prone to process crashes. Test&Set is a synchronization operation that, when invoked by a set of processes, returns yes to a unique process and returns no to all the others. Recently many advances in implementing Test&Set objects have been achieved, however all of them target the shared memory model. In this paper we propose an implementation of a Test&Set object in the message passing model. This implementation can be invoked by any number p $\leq$ n of processes where n is the total number of processes in the system. It has an expected individual step complexity in $O(\log p)$ against an oblivious adversary, and an expected individual message complexity in $O(n)$. The proposed Test&Set object is built atop a new basic building block, called selector, that allows to select a winning group among two groups of processes. We propose a message-passing implementation of the selector whose step complexity is constant. We are not aware of any other implementation of the Test&Set operation in the message passing model.

7.4.5. Population Protocol Model

The population protocol model, introduced by Angluin et his colleagues in 2006, provides theoretical foundations for analyzing global properties emerging from pairwise interactions among a large number of anonymous agents. In the population protocol model, agents are modeled as identical and deterministic finite state machines, *i.e.* each agent can be in a finite number of states while waiting to execute a transition. When two agents interact, they communicate their local state, and can move from one state to another according to a joint transition function. The patterns of interaction are unpredictable, however they must be fair, in the sense that any interaction that should possibly appear cannot be avoided forever. The ultimate goal of population protocols is for all the agents to converge to a correct value independently of the interaction pattern. Examples of systems whose behavior can be modeled by population protocols range from molecule interactions of a chemical process to sensor networks in which agents, which are small devices embedded on animals, interact each time two animals are in the same radio range.

In this work, we focus on an quite important related question. Namely, is there a population protocol that exactly counts the difference κ between the number of agents that initially set their state to A and the one that initially set it to B, and can it be solved in an efficient way, that is with the guarantee that each agent should converge to the exact value of κ after having triggered a sub-linear number of interactions in the size of the system [43].

We answer this question by the affirmative by presenting a $O(n^{3/2})$-state population protocol that allows each agent to converge to the exact solution by interacting no more than $O(\log n)$ times. The proposed protocol is very simple (as is true for most known population protocols), but is general enough to be used to solve different types of tasks.

8. Bilateral Contracts and Grants with Industry

8.1. Bilateral Contracts with Industry

- **CS contract (2014-2016): "SecEF"**

  The SecEF contract consists in analyzing current used standards for information security events [39]. Such events following a standardized structure are needed to allow communications between the various security tools, in order to consolidate and correlate information, and for communications between different security response teams, to share information relative to incidents. Examples of such events are IDMEF (Intrusion Detection Message Exchange Format, RFC 4765) or IODEF (Incident Object Description Exchange Format, RFC 5070). Unfortunately, these two standards are insufficiently deployed on a market still dominated by proprietary formats. The objective of the SecEF (Security Exchange Format) project is thus to propose evolutions of these formats, based on the initial feedback from current users. During the first years of the project, we focused our work on alert formats. We conduced a comparative study of different alert formats and propose quantitative metrics to asses format expressiveness. We also proposed some evolutions for the IDMEF format and started the development of a generic library dedicated to IDMEF. This library could be used in different programming languages to generate and parse IDMEF messages. It will also support different encodings and transport protocols.

- **HP contract (2013-2016): "Embedded Systems Security"**

  We have initiated a research program in collaboration with HP Inc Labs in the domain of 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 device architectures. In 2015, the project has been extended. We initiated a knew research work involving a Master student. The main objective of this extension is to monitor low-level software (firmware, OS kernels, hypervisors) thanks to a dedicated external co-processor. HP Inc Labs will fund a PhD on that subject. Details about this research program cannot be provided as they are covered by a non-disclosure agreement.

8.2. Bilateral Grants with Industry

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

  Florian Grandhomme is doing his PhD thesis in the context of a cooperation with DGA-MI. The goal of this thesis 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 hetereogeneity of technology and infrastructure. The solution will be independant from the underlying intra-domain routing protocol and from the infrastructure: wired or wireles, fixed or mobile.

- **DGA-MI: "Visualization for security events monitoring"**

  Damien Crémilleux was hired this year as a Ph.D. student on a DGA-MI funding to work on visualization for security events monitoring. The purpose of this thesis it 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. VEGAS was presented during the poster session in VizSec 2015 [58] that took place in Chicago, Illinois on the 26th of October 2015.

- **Orange Labs: "Data persistence and consistency in ISP infrastructures"**

  Pierre Obame is doing his PhD thesis in the context of a CIFRE contract with Orange Labs at Rennes. Pierre Obame has proposed a distributed storage system called Mistore, dedicated to users who access Internet via a Digital Subscriber Line (DSL) technology. This system aims at guaranteeing data availability, persistence, and low access latency by leveraging millions of home gateways and the hundreds of Points of Presence (POP) of an Internet Service Provider (ISP) infrastructure. Pierre Obame has also proposed a mathematical framework for defining both strong and weak consistency criteria within the same formalism. These criteria are offered by Mistore to its clients when they manipulate their data. Pierre Obame, whose PhD thesis is planned to terminate in 2016, is in the process of writing his PhD manuscript so as to defend it in 2016.

- **Orange Labs: "Privacy-preserving location-based services"**

  Solenn Brunet has started her PhD thesis since 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 will adapt 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. A first paper on the development of a privacy-preserving e-toll service based on the partially blind signature has just been accepted for publication.

- **DGA-MI: "Security events visualization"**

  Christopher Humphries defended his Ph.D. thesis on the 8th of December 2015. This Ph.D. was funded by DGA-MI. The objective of this thesis was to propose new visualization mechanisms dedicated to the analysis of security events, for instance for forensic purposes. Two tools, ELVIS and CORGI, were produced. This research led to two publications in VizSec, which is the most famous venue on the topic of visualization for security.

- **DGA-MI: "Alerts correlation taking the context into account"**

  The PhD of Erwan Godefroy is done in the context of a cooperation with DGA-MI. This PhD started in November 2012 and is expected to finish in 2016. The current work consists in the automatic generation of alert correlation rules in the context of deployed distributed systems. The correlation rules aim at being used by our GnG correlation system.

9. Partnerships and Cooperations

9.1. Regional Initiatives

- **Région Bretagne ARED grant:** the PhD of Regina Marin on privacy protection in distributed social networks (defended in Sep 2015) was supported by a grant from the Région Bretagne.
- **Labex COMINLAB contract (2012-2015): "POSEIDON" - http://www.poseidon.cominlabs.ueb.eu/fr/**

  POSEIDON deals with the protection of data in outsourced or shared systems such as cloud computing and peer-to-peer networks. While these approaches are very promising solutions to outsourced storage space, contents, data and services, they also raise serious security and privacy issues since users lose their sovereignty on their own data, services and systems. Instead of trying

to prevent the bad effects of the cloud and of peer-to-peer systems, the main objective of the POSEIDON project is to turn benefit from their main characteristics (distribution, decentralization, multiple authorities, etc.) to improve the security and the privacy of the users' data, contents and services.

This project is conducted in cooperation with Télécom Bretagne and Université de Rennes I. The PhD of Julien Lolive (co-supervised by Sébastien Gambs and Caroline Fontaine), which deals with the entwining of identification and privacy mechanisms, is funded by the POSEIDON project. The postdoctoral research of Wei Pan (co-supervised by Gouenou Coatrieux and Nicolas Prigent) that deals with a distributed system to ensure patients' privacy in the context of medical imaging is also funded by this project.

POSEIDON will be over at the end of this year. It has received very positive feedback during the COMINLAB review meeting.

- **Labex COMINLAB contract (2012-2015): "SecCloud" - http://www.seccloud.cominlabs.ueb.eu**

  Nowadays attacks targeting the end-user and especially its web browser constitute a major threat. Indeed web browsers complexity has been continuously increasing leading to a very large attack surface. Among all possible threats, we tackle in the context of the SecCloud project those induced by client-side code execution (for example javascript, flash or HTML5).

  Existing security mechanisms such as OS-level access control often only rely on users identity to enforce the security policy. Such mechanisms are not sufficient to prevent client-side browser attacks as the web browser is granted the same privileges as the user. Consequently, a malicious code can perform every actions that are allowed to the user. For instance, it can read and leak user private data (credit cart numbers, registered passwords, email contacts, etc.) or download and install malware.

  One possible approach to deal with such threats 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 information flow rules between user data and distant web sites.

  Dynamically monitoring information flow at the web browser level may dramatically impact runtime performances of executed codes. Consequently, an important aspect of this work will be to benefit as far as possible from static analysis of application code. This static-dynamic hydride approach should reduce the number of verifications performed at run time.

  This study is 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 INS Project: AMORES (2011-2015) - http://amores-project.org/**

  Situated in the mobiquitous context characterized by a high mobility of individuals, most of them wearing devices capable of geolocation (smartphones or GPS-equipped cars), the AMORES project is built around three use-cases related to mobility, namely (1) dynamic carpooling, (2) real-time computation of multi-modal transportation itineraries and (3) mobile social networking. For these three use cases, the main objective of the AMORES project is to define and develop geo-communication primitives at the middleware level that can offer the required geo-located services, while at the same time preserving the privacy of users, in particular with respect to their location (notion of geo-privacy). Within this context, we study in particular the problem of anonymous routing and the design of a key generation protocol tied to a particular geographical location. Each of these services can only work through cooperation of the different entities composing the mobile network. Therefore, we also work on the development of mechanisms encouraging entities to cooperate together in a privacy-preserving manner. The envisioned approach consists in the

definition of generic primitives such as the management of trust and the incentive to cooperation. This project is joint between the Université de Rennes I, Supélec, LAAS-CNRS, Mobigis and Tisséo. The research project AMORES received the Innovation Award at the Toulouse Space Show in June 2013. Simon Boche and Paul Lajoie-Mazenc are doing their PhD in the context of this project. Paul has defended successfully his thesis in September [13] just after the final closing workshop of the project (http://www.irisa.fr/prive/sgambs/journee_AMORES.html).

- **ANR INS Project: LYRICS (2011-2015) - http://projet.lyrics.orange-labs.fr/**

  With the fast emergence of the contactless technology such as NFC, mobile phones will soon be able to play the role of e-tickets, credit cards, transit pass, loyalty cards, access control badges, e-voting tokens, e-cash wallets, etc. In such a context, protecting the privacy of an individual becomes a particularly challenging task, especially when this individual is engaged during her daily life in contactless services that may be associated with his identity. If an unauthorized entity is technically able to follow all the digital traces left behind during these interactions then that third party could efficiently build a complete profile of this individual, thus causing a privacy breach. Most importantly, this entity can freely use this information for some undesired or fraudulent purposes ranging from targeted spam to identity theft. The objective of LYRICS (ANR INS 2011) is to enable end users to securely access and operate contactless services in a privacy-preserving manner that is, without having to disclose their identity or any other unnecessary information related to personal data. Within this project, we work mainly on the privacy analysis of the risks incurred by users of mobile contactless services as well as on the development of the architecture enabling the development of privacy-preserving mobile contactless services. The project is joint between France Télécom, Atos Wordline, CryptoExperts, ENSI Bourges, ENSI Caen, MoDyCo, Oberthur Technologies, NEC Corporation, Microsoft and Université de Rennes I.

  The project was originally suppose to end in 2014 but an extension was granted until May 2015. The final closing workshop of the project was held during this month (http://www.irisa.fr/prive/sgambs/journees_LYRICS.html). The project has finished to develop a first prototype that illustrates how can be used privacy preserving protocols for the transport use case. The prototype implements a transportation pass (similar to the Navigo pass) embedded in the SIM card. This transport pass can be interact with a gate at the entrance of the transportation network in order to check the validity of the pass and answers wirelessly, in less than 300ms, without revealing any information about the user. This result has been presented in "Salon Cartes 2012". During the last year of the project, the partners of the LYRICS projects have also worked on two new use cases and their corresponding prototypes: digital surveys and e-cash solutions that respect the privacy of users. The outcomes of the project have been presented at the RESSI conference [49].

- **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. For instance at the end of November, Sébastien Gambs was co-organizer with Daniel Le Métayer of a joint French-Canadian workshop titled "La vie privée à travers les cultures. Convergences et divergences dans un monde globalisé" (http://www.centrejacquescartier.com/les-entretiens/entretiens-2015lescolloques/3-la-vie-privee-a-travers-les-cultures-convergences-et-divergences-dans-un-monde-globalise/) that had approximately 80 attendees coming either from a law or computer science background.

9.2.3. Competitivity Clusters

The AMORES project (ANR INS 2011, http://www.images-et-reseaux.com/en/content/amores) is recognized by the Images & Réseaux cluster.

9.3. European Initiatives

9.3.1. FP7 & H2020 Projects

The **PANOPTESEC** project (http://www.panoptesec.eu) started on the 1st of November 2013. 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),
- Alcatel-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. Most of our work focused on WP5 and WP6, that deal with the IDS event correlation system and the visualization system. Two prototypes have been produced and a publication was made to VizSec 2015. Next year, we will be entering in the integration phase.

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 2015, one in DEBS [44] and the other one in SRDS [29]. Emmanuelle Anceaume is actively working with James Aspens from Yale University, USA, on population protocols. Their collaboration gave rise to one article published in NCA [43]. Emmanuelle Anceaume is actively working with Ernst Schulte-Geers from the Federal Office for Information Security, Germany. Their collaboration gave rise to one publication in the Journal of Applied Probability [15].

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 [42].

Following the Inria explorer visit of last year, Sébastien Gambs is actively working with Stan Matwin from Dalhousie University (Canada) on the sanitization of location data through non-interactive differentially-private methods, which has lead to a first publication on this subject [26].

9.5. International Research Visitors

9.5.1. Visits of International Scientists

9.5.1.1. Internships

Sackmann Mario Julián

Date: Sep 2014 - Jan 2015

Institution: Universidad de Buenos Aires (Argentina)

Supervisor: Guillaume Piolle

9.5.2. Visits to International Teams

9.5.2.1. Research stays abroad

Thanks to the support of CentraleSupélec, Christophe Bidan has joined the ETS (École Supérieure de Technologie) of Montréal from july 2014 to july 2015 for working with Prof. Jean-Marc Robert. This stay results from a collaboration that has been initiated 2 years ago when Prof. Jean-Marc Robert has spent 4 months (from september to december 2012) in the CIDRE research group. The conducted research has focused on the use of secure multi-party computation to ensure privacy. Specifically, under the co-supervision of Aurélien Dupin, master student at ETS, we focused on the use of secure multi-party computation to provide proof of localization while ensuring privacy of the participants. An article is being written, and a co-supervised thesis should begin shortly.

From September 2014 to May 2015, Antoine Guellier has joined the "Securing Cyberspace" team leaded by Prof. Batten, at Deakin University (Melbourne, Australia). This stay is possible thanks to the international outgoing fellowships of Rennes Métropole and of the UEB (Université Européenne de Bretagne). This doctoral mobility was the opportunity to start a collaboration with personnel from Deakin University, as well as Radboud University (The Netherlands). Research outputs include a paper submitted to the SPT-IOT workshop (IEEE PERCOM venue). Additionally, by participating in the life of the laboratory and in several academic and information security events based in Melbourne, Antoine Guellier was able to build a network abroad. Through discussion and interactions, he was able to confront the contributions in his thesis with people of different horizons, and start new ones.

In March 2015, Deepak Subramanian has joined, as a Visiting Scholar, the "Faculty of Engineering Science" at KU Leuven in Belgian. During this stay, Deepak Subramanian worked on the topic of WebRTC security analysis with Prof. Frank Piessens, Willem De Greof, and Dr. Lieven Desmet. The objectives was to perform a practical analysis of the current WebRTC framework with the motivation of identifying the various shortcomings. The initial results showed that WebRTC is quite robust and built on strong foundations (based on legacy protocols that also form the foundations of the SIP telephony stack). However, the study also showed that some key modules were made optional in the draft and the implementations are quite ambiguous presently. These results were resumed in a paper that has been submitted and accepted to the ACM SEC@SAC 2016.

10. Dissemination

10.1. Promoting Scientific Activities

10.1.1. Scientific events organisation

10.1.1.1. General chair, scientific chair

Emmanuelle Anceaume is General chair of the 19-th edition of the International Conference on Principles of Distributed Systems (OPODIS 2015).

10.1.1.2. Member of the organizing committees

Emmanuelle Anceaume served as a member of the organization committee of the following conference

- International Conference on Principles of Distributed Systems (OPODIS 2015)

Sébastien Gambs served as a member of the organization committee of the following events:

- Journées thématiques: Respect de la vie privée et services mobiles sans contact (27-28 May, Issy-les-Moulineaux).
- Journée thématique: Sécurité et respect de la vie privée dans les systèmes mobiquitaires (24 September, Rennes).
- Entretien Jacques Cartier : La vie privée à travers les cultures. Convergences et divergences dans un monde globalisé (30 November 2015)

Nicolas Prigent served as a member of the organization committees of the following conferences and workshops:

- SSTIC 2015 (Symposium sur la Sécurité des Systèmes d'Information et des Communications 2015).
- VizSec 2015 (12th IEEE International Symposium on Visualization for Cyber Security).

Frédéric Tronel served as a member of the organization committee of the following conference:

- SSTIC 2015 (Symposium sur la Sécurité des Systèmes d'Information et des Communications 2015).

Ludovic Mé served as a member of the organization committee of the following conference:

- C&ESAR 2015 (Computers & Electronics Security Applications Rendez-vous),
- RESSI 2015 (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

Christophe Bidan served as a member of the organization committee of the following conference:

- ICISSP 2015 (International Conference on Information Systems Security and Privacy 2015).

10.1.2. Scientific events selection

10.1.2.1. Chair of conference program committees

Emmanuelle Anceaume served as a co-chair of the following conference

- 4-th IEEE Symposium on Network Cloud Computing and Applications (NCCA15)

Nicolas Prigent was the program chair of the following conference

- 12th IEEE International Symposium on Visualization for Cyber Security (VizSec 2015).

10.1.2.2. Member of the conference program committees

Emmanuelle Anceaume served a member of the program committee of the following conferences:

- 5-th International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS 2015) (http://www.peccs.org/Home.aspx?y=2015)
- 14th IEEE International Symposium on Network Computing and Applications (IEEE NCA15)
- 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15)
- 17eme Rencontres Francophones sur les Aspects Algorithmiques de Télécommunications (ALGOTEL 2015)

Sébastien Gambs served a member of the program committee of the following conferences:

- 13th International Conference on Privacy, Security and Trust (PST'15),
- 15th IFIP TC 6/TC 11 International Conference on Communications and Multimedia Security (CMS'15),
- 10th International Workshop on Data Privacy Management (DPM'15),
- 8th International Symposium on Foundations and Practice of Security (FPS'15).

Michel Hurfin served as a member of the program committee of the following conference:

- 7-th IEEE International Symposium on UbiSafe Computing (Ubisafe 2015)

Ludovic Mé served as a member of the program committee of the following conferences:

- C&ESAR 2015 (Computers & Electronics Security Applications Rendez-vous),
- RESSI 2015 (Rendez-Vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information).

Guillaume Piolle served as a member of the program committee of the following conference:

- ACySe 2015 (Second International Workshop on Agents and CyberSecurity).

Christophe Bidan served as a member of the program committee of the following conference:

- IWTCC 2015 (Second International Workshop on Trust in Cloud Computing).

Nicolas Prigent served as a member of the program committee of the following conferences:

- SSTIC 2015
- 12th IEEE International Symposium on Visualization for Cyber Security (VizSec).

Eric Totel served as a member of the program committee of the following conferences:

- C&ESAR 2015 (Computers & Electronics Security Applications Rendez-vous),
- 7-th IEEE International Symposium on UbiSafe Computing (Ubisafe 2015)

Frédéric Tronel served as a member of the program committee of the following conferences:

- SSTIC 2015.

10.1.2.3. Reviewer

- Gilles Guette as a reviewer for the International Conference on Information System Security and Privacy (ICISSP).

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

- Ludovic Mé and Valérie Viet Triem Tong act as reviewers for the following journal: IEEE Transactions on Network and Service Management (TNSM),
- Gilles Guette acts as a reviewer for the following journals: Security and Communication Networks (SCN),
- Gilles Guette acts as a reviewer for the following journals: Sensors.
- Emmanuelle Anceaume acts as a reviewer for the following journals: IEEE Transactions on Parallel and Distributed Systems (TPDS), IEEE Transactions on Dependable and Secure Computing (TDSC), and the Theoretical Computer Journal (TCS).
- Guillaume Piolle acts as a reviewer for the following journal: International Journal on Information Security (IJIS).
- Frédéric Tronel acts as a reviewer for the following journals: IEEE Transactions on Dependable and Secure Computing (TDSC).

10.1.4. Invited talks

Valérie Viet Triem Tong has been invited at the 3rd International Symposium on Information Systems Security, Kenitra Morocco (CISSI'2015). She has given a talk entitled *Capture de signatures comportementales de malware Android par suivi de flux d'information – Behavioral Signatures of Android Malware using information flow monitoring*.

Ludovic Me and Guillaume Hiet were invited at the 6th *Assises du domaine Cyber Défense et SIEM* organized by the R2GS (*Recherche et Réflexion en Gestion opérationnelle de la Sécurité*) club. They gave a talk entitled *Travaux de recherches en supervision de sécurité : tendances actuelles*.

Sébastien Gambs was invited to give a tutorial on "inference attacks on location data" at the Shonan Seminar on Logic and Verification Methods in Security and Privacy in November in Japan.He has also given an invited talk on "Implementing the right to be forgotten" at the Workshop on Ethics and Artificial Intelligence held in Rennes in June as well as a talk on "Privacy challenges in the Information Society" at the French-Japanese workshop on cybersecurity held in Tokyo in April.

10.1.5. Research administration

Ludovic Mé acts as Scientific Officer for the Rennes - Bretagne Atlantic Inria Research Center.

Emmanuelle Anceaume acts as member of the

- Inria Commission d'Evaluation
- Université Rennes 1 Comité de selection

Sébastien Gambs is a member of the committee for the Gilles Kahn award, which is given each year to the best PhD thesis in computer science in France by the Société d'Informatique de France. He is also the co-chair of Cybersecurity research axis of the IRISA laboratory as well as a member of the Inria-CNIL committee.

10.2. Teaching - Supervision - Juries

10.2.1. Teaching

Licence: Ludovic Mé, *Software Engineering*, 15h, L3 - first year of the engineer degree, Supélec, France

Master: Ludovic Mé, *Information systems*, 4,5 hours, M1 - second year of the engineer degree, Supélec, France

Master: Ludovic Mé, *Supervision of student project*, 1 project, M1 - second year of the engineer degree, Supélec, France

Master: Ludovic Mé, *Supervision of student project*, 1 project, M2 - mastère cybersecurity degree, Supélec, France

Master: until September 2015, Ludovic Mé was responsible for the module "Secured information systems", M2 - third year of the engineer degree, Supélec, France

Master: Sébastien Gambs, *Protection of Privacy*, 16 hours of lectures, M2 - Master Pro SSI, Université de Rennes 1, France.

Master: Sébastien Gambs, *Topics on Authentication*, 16 hours of lectures, M2 - Master Pro SSI, Université de Rennes 1, France.

Master: Sébastien Gambs, *Introduction to Computer Security*, 8 hours of lectures and 4 hours of practical works, M2 - Master Pro SSI, Université de Rennes 1, France.

Licence: Gilles Guette, *Network Initiation*, 27h, L3 - Licence, ISTIC/University of Rennes 1, France

Licence: Gilles Guette, *Network Initiation*, 43h, L3 - first year of the engineer degree, ESIR, France

Master: Gilles Guette, *Network Routing*, 28h, M1 - second year of the engineer degree, ESIR, France

Master: Gilles Guette, *Mobile Network Routing*, 5h, M1 - second year of the engineer degree, ESIR, France

Master: Gilles Guette, *Advanced Network Services*, 13h, M1 - second year of the engineer degree, ESIR, France

Master: Gilles Guette, *Network Project*, 24h, M1 - second year of the engineer degree, ESIR, France

Master: Gilles Guette, *Security*, 26h, M1 - second year of the engineer degree, ESIR, France

Master: Gilles Guette, *Network and System Security*, 12h, M2 - third year of the engineer degree, ESIR, France

Master: Gilles Guette, *Network Modeling*, 10h, M2 - third year of the engineer degree, ESIR, France

Master: Gilles Guette, *Network*, 6h, M2 - third year of the engineer degree, Supélec, 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*, M1 - second year of the engineer degree, ESIR, France

Licence : Guillaume Piolle, *Algorithms*, 21 hours, L3 - first year of the engineer degree, Centrale-Supélec, France

Licence : Guillaume Piolle, *Software engineering*, 24 hours, L3 - first year of the engineer degree, CentraleSupélec, France

Master : Guillaume Piolle, *Modelling, Algorithms and Programming*, 22 hours, M1 - second year of the engineer degree, CentraleSupélec, France

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

Master : Guillaume Piolle, *Software project*, 14 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*, 13.5 hours, M2 - third year of the engineer degree, CentraleSupélec, France

Master : Guillaume Piolle, *Software engineering*, 22 hours, M2 - third year of the engineer degree, CentraleSupélec, France

Master : Guillaume Piolle, *Symbolic Artificial Intelligence*, 4.5 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*, 12 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

Master : Guillaume Piolle, *Java EE*, 21 hours, Mastère spécialisé, 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, Supe´lec, France

Licence : Eric Totel, *Foundations of computer science, data structures and algorithms*, 6 hours, L3 - first year of the engineer degree, Supe´lec, France

Master : Eric Totel, *Computer systems' architecture*, 30 hours, M1 - second year of the engineer degree, Supe´lec, France

Master : Eric Totel, *C language*, 24 hours including 6 hours of lecture, M2 - master CS (Cyber Security), Supe´lec, France

Master : Eric Totel, *C language and C++ language*, 12 hours including 6 hours of lecture, M2 - third year of the engineer degree, Supe´lec, France

Master : Eric Totel, *Dependability* , 9 hours including 7.5 hours of lecture, M2 - third year of the engineer degree and master research, Supe´lec, France

Master : Eric Totel, *Dependability*, 3 hours of lecture, M2 - third year of the engineer degree (inge´nierie des syste`mes automatise´s), Supe´lec, France

Master : Eric Totel, *Dependability*, 4.5 hours of lecture, M2 - post-graduate training (master Architecture des Re´seaux de Communication), Supe´lec, France

Master : Eric Totel, *Intrusion Detection*, 6 hours of lecture, M2 - M2 - master CS (Cyber Security), Supe´lec, 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, Supe´lec, France

Master : Eric Totel, *Supervision of student project*, 1 project, M2 - third year of the engineer degree, Supe´lec, France

Licence: Frédéric Tronel, *Software engineering*, 49h, L3 - first year of the engineer degree, CentraleSupélec, France.

Master: Frédéric Tronel, *Operating systems*, 18h, M2 - third year of the engineer degree, CentraleSupélec, France .

Master: Frédéric Tronel, *Compilers*,37h, M2 - third year of the engineer degree, CentraleSupélec, France.

Master: Frédéric Tronel, *Automatic reasoning*, 7h, M2 - third year of the engineer degree, CentraleSupélec, France.

Master: Frédéric Tronel, *Assembly Language*, 4h30, M2 - third year of the engineer degree, CentraleSupélec, France.

Master: Frédéric Tronel, *Buffer overflow vulnerabilities (theory and practice)*, 7h, M2 - third year of the engineer degree, CentraleSupélec, France.

Master: Frédéric Tronel, *Firewall*, 8h, M2 - third year of the engineer degree, CentraleSupélec, France.

Master: Frédéric Tronel, *Calculability in distributed systems*, 9h, 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;

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 yearof 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*, 7h30 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, Supe´lec, France

Master: Emmanuelle Anceaume, *computer science (MRI) specialism - BIB - Colq*, 36h, M2, Istic, France.

Master: Nicolas Prigent, *Operating systems*, 18h, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Nicolas Prigent, *Automatic reasoning*, 8h, M2 - third year of the engineer degree, CentraleSupélec, France;

Master: Nicolas Prigent, *Web development*, 12 hours, M2 - third year of the engineering degree, CentraleSupélec, France;

Master: Nicolas Prigent, *Python Programming*, 6 hours, M2 - third year of the engineering degree, CentraleSupélec, France;

Master : Nicolas Prigent, *Advanced Java Programming*, 1,5 hours, M2 - third year of the engineering degree, CentraleSupélec, France;

Master: Nicolas Prigent, *Penetration Testing*, 18 hours, M2 - third year of the engineering degree, CentraleSupélec, France;

Master : Nicolas Prigent, *IDS and Visualization*, 2 hours, M2, ESIR, France.

Master : Nicolas Prigent, *Virtualization and Cloud Computing*, 4 hours, M2, ESIR, France.

Master : Nicolas Prigent, *MS Windows Configuration and Administration*, 16 hours, Mastère CS - Specialization year, CentraleSupélec, France.

Master : Nicolas Prigent, *MS Windows Configuration and Administration*, 16 hours, CQP - Specialization year, CentraleSupélec, France.

Master : Nicolas Prigent, *Cryptography, Cryptographic Protocols and Applications*, 32 hours, CQP - Specialization year, CentraleSupélec, France.

Master : Nicolas Prigent, *Supervision of student project* , 2 projects, M1 - second year of the engineer degree, CentraleSupélec, France.

Master : Nicolas Prigent, *Supervision of student project*, 2 project, M2 - third year of the engineer degree, CentraleSupélec, France.

Master : Nicolas Prigent, *Supervision of student project*, 1 project, Mastère CS - Specialization year, CentraleSupélec, France.

Licence: Guillaume Hiet, *Algorithms and Data Structures*, 12.5h, L3 - first year of the engineer degree, CentraleSupélec, France

Master: Guillaume Hiet, *Computer security and privacy for the engineer*, 8h, M1 - second year of the engineer degree, CentraleSupélec, France

Master: Guillaume Hiet, *Buffer overflow vulnerabilities*, 16h, M2 - third year of the engineer degree, CentraleSupélec, France

Master: Guillaume Hiet, *Buffer overflow vulnerabilities*, 16h, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France

Master: Guillaume Hiet, *Pentest*, 19h, M2 - third year of the engineer degree, CentraleSupélec, France

Master: Guillaume Hiet, *Pentest*, 3h, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France

Master: Guillaume Hiet, *Introduction to Linux*, 3h, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France

Master: Guillaume Hiet, *Java Security*, 4.5h, M2 - Mastère Spécialisé CS, CentraleSupélec, France

Master: Guillaume Hiet, *Linux Security*, 18h, M2 - Mastère Spécialisé CS , CentraleSupélec, France

Master: Guillaume Hiet, *Linux Security*, 7.5h, third year of the engineer degree, CentraleSupélec, France

Master: Guillaume Hiet, *LDAP*, 7.5h, third year of the engineer degree, CentraleSupélec, France

Master: Guillaume Hiet, *Intrusion Detection*, 15h, M2 - Mastère Spécialisé CS, CentraleSupélec, France

Master: Guillaume Hiet, *Intrusion Detection*, 13.5h, M2 - third year of the engineer degree, M2 research degree of University of Rennes 1, CentraleSupélec, France

Master: Guillaume Hiet, *Security Monitoring*, 3h, M2, cycle "Sécurité Numérique", INHESJ, France

Master: Guillaume Hiet, *Computer Security*, 31.5h, M2, Mastère Spécialisé Architecte des Systèmes d'Information, CentraleSupélec, France

Master: Guillaume Hiet, *Intrusion Detection*, 16h, M2, University of Rennes 1, France

Master: Guillaume Hiet, *Intrusion Detection*, 10h, M2 - third year of the engineer degree, ESIR, France

Master: Guillaume Hiet, *Intrusion Detection*, 9h, M2, Université of Limoges, France

Master: Guillaume Hiet, *Firewall*, 6h, M2, University of Rennes 1, France

Master: Guillaume Hiet, *Supervision of student project*, 4 projects, M1 - second year of the engineer degree, CentraleSupélec, France

Master: Guillaume Hiet, *Supervision of student project*, 2 projects, M2 - third year of the engineer degree, CentraleSupélec, France

Master: Guillaume Hiet, *Supervision of student project*, 2 projects, M2 - Mastère Spécialisé CS (Cyber Security), CentraleSupélec, France

Master: 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*, 15h including 6 hours of lecture, M2 - third year of the engineer degree, CentraleSupélec, France

Master: Christophe Bidan, *Introduction to security*, lab work (4h30), M2 - third year of the engineer degree, CentraleSupélec, France

Licence: Christophe Bidan, *Algorithms and Data Structures*, 36 hours of lecture including 7,5 hours of lectures, L3 - first year of the engineering degree, CentraleSupélec, France;

Master : Christophe Bidan, *Cryptographic Protocols*, 6 hours of lecture, mastère CS (Cyber Security), CentraleSupélec, France

10.2.2. Supervision

PhD : Christopher Humphries, User-centred Security Event Visualisation, Université de Rennes 1, Defense 8/12/2015, supervised by Christophe Bidan, Nicolas Prigent and Frédéric Majorczyk

PhD : Paul Lajoie-Mazenc, Réputation et respect de la vie privée dans les rśeaux dynamiques et auto-organisés, Université de Rennes 1, Defense 25/09/2015, supervised by Emmanuelle Anceaume and Valérie Viet Triem Tong

PhD : Regina Paiva Melo Marin, Enhancing Privacy Protection in Social Network Systems Through Decentralization and Policy Conflict Management, CentraleSupélec, Defense 7/09/2015, supervised by Christophe Bidan and Guillaume Piolle

PhD : Mounir Assaf, From Qualitative to Quantitative Program Analyses: Permissive Enforcement of Secure Information Flow, Université de Rennes 1, Defense 06/05/2015, supervised by Eric Totel and Frédéric Tronel and Julien Signoles

HdR: Valérie Viet Triem Tong, "Apport du suivi de flux d’information pour la sécurité des systèmes", Université de Rennes 1, Defense 03/12/15.

PhD in progress : Pierre Obame Meye, Sûreté de fonctionnement dans le nuage de stockage, 01/02/2011, supervised by Emmanuelle Anceaume and Frédéric Tronel

PhD in progress: Erwan Godefroy, “Corrélation d’alertes dirigée par la connaissance de l’environnement”, started in November 2012, supervised by Eric Totel (50%), Ludovic Mé (30%), and Michel Hurfin (20%);

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

PhD in progress: Mourad Leslous, “Déclenchement automatique de codes jugés suspects dans les applications Android”, started in October 2015, supervised by , Thomas Genet (Celtique Inria project 20 %), Jean François Lalande (40 %), Valérie Viet Triem Tong (40 %) ;

PhD in progress: Simon Boche, “Respect de la vie prive´e dans les re´seaux ubiquitaires”, started in October 2012, supervised by Christophe Bidan (30 %), Nicolas Prigent (35 %), Gilles Guette (35 %) ;

PhD in progress: Antoine Guellier, “Utilisation de la cryptographie homomorphe pour garantir le respect de la vie prive´e”, started in October 2013, supervised by Christophe Bidan (50 %), Nicolas Prigent (50 %) ;

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

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 %) ;

PhD in progress: Kun He, “Mise en œuvre de technique de droit a` l’oubli pour les contenus nume´riques", started in October 2013, supervised by Christophe Bidan (50 %) and Gaëtan LeGuelvouit (IRT B-Com 50 %) ;

PhD in progress: Julien Lolive, “Entwining identification and privacy mechanisms”, started in December 2012, supervised by Caroline Fontaine (50% - Télécom-Bretagne) and Sébastien Gambs (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: Florian Grandhomme, “Étude de protocoles de routage dynamique externe de type BGP dans un environnement réseaux tactiques adhoc mobiles : faisabilité, performances, qualité de service et passage à l’échelle.”, started in October 2014, supervised by Adlen Ksentini (Dionysos Inria project 30%), Gilles Guette (70%) ;

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: Thomas Letan, “Contribution à la sécurité des couches basses des systèmes d’information”, started in January 2015, supervised by Guillaume Hiet (50 %), Pierre Chifflier (ANSSI, 25 %), 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 (Gipsa-lab, 50 %), Guillaume Hiet (25 %), and Jean-Marc Thiriet (Gipsa-lab, 25 %).

10.2.3. Juries

- Sébastien Gambs was a member of the PhD committee (reviewer) for the PhD of Thibaud Antignac titled « Méthodes formelles pour le respect de la vie privée par construction », prepared at INSA de Lyon, February 2015.
- Sébastien Gambs was a member of the PhD committee (reviewer) for the PhD of Marco Stronati titled « Designing Location Privacy Mechanisms for flexibility over time and space », prepared at Ecole Polytechnique, September 2015.
- Sébastien Gambs was a member of the PhD committee (reviewer) for the PhD of Ali Kassem titled « Automated Verification of Exam, Cash, Reputation, and Routing Protocols », prepared at Université de Grenoble, September 2015.
- Sébastien Gambs was a member of the PhD committee (reviewer) for the PhD of Iraklis Leontiadis titled « Privacy Preserving Data Collection and Analysis », prepared at Eurecom, October 2015.
- Ludovic Mé was a member of the PhD committee (reviewer) for the PhD of Ivan Studnia entitled « Détection d’intrusion pour des réseaux embarqués automobiles : une approche orientée langage », prepared at INSA de Toulouse, Septembre 2015.

- Ludovic Mé was a member of the PhD committee (reviewer) for the PhD of Eric Freyssinet entitled « Lutte contre les botnets : analyse et stratégie », prepared at Université Pierre et Marie Curie, Paris, November 2015.
- Ludovic Mé was a member of the HDR committee (reviewer) for the HDR of Yves Roudier entitled « Advances in the Design and Engineering of Secure Distributed Systems », prepared at Université Nice Sophia-Antipolis, Decembre 2015.
- Eric Totel was a member of the PhD committee (reviewer) for the PhD of Yosra Ben Mustapha entitled « Corrélation d'alertes: un outil plus efficace d'aide à la décision pour répondre aux intrusions », prepared at Telecom Sud Paris, Avril 2015.
- Eric Totel was a member of the PhD committee (reviewer) for the PhD of Samuel Marchal entitled « DNS and Semantic Analysis for Phishing Detection », prepared at Université de Lorraine, Juin 2015.
- Eric Totel was a member of the PhD committee (reviewer) for the PhD of Thibault Probst entitled « Evaluation et analyse des mécanismes de sécurité des réseaux dans les infrastructures virtuelles de cloud computing », prepared at Université fédérale de Toulouse, Septembre 2015.
- Valérie Viet Triem Tong was a member of the PhD committee for the PhD of Aurélien Thierry entitled « Désassemblage et détection de logiciels malveillants auto-modifiants », prepared at Université de Lorraine, March 2015.

10.3. Popularization

Guillaume Piolle has participated to two scientific popularization activities, both oriented towards secondary education pupils. In both cases, 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):

- Les cordées de la réussite : national program aimed at facilitating access to higher education for pupils from various social backgrounds ;
- Bilateral scientific mediation action between CentraleSupélec and the Joliot-Curie high school in Rennes.

Other kinds of popularization activities have taken place in the form of communications aimed at non-academic computing professionals, on the topic of personal data protection regulations and techniques [24], [20].

Sébastien Gambs was also involved in several events dedicated to the public at large such as a presentation at le Pouce (https://iww.inria.fr/ouest-inria/le-pouce-bilan-et-perspectives/).

11. Bibliography

Major publications by the team in recent years

[1] E. ANCEAUME, R. LUDINARD, B. SERICOLA. *Performance evaluation of large-scale dynamic systems*, in "ACM SIGMETRICS Performance Evaluation Review", April 2012, vol. 39, n^{o} 4, pp. 108-117 [*DOI :* 10.1145/2185395.2185447], http://hal.archives-ouvertes.fr/hal-00736918

[2] M. A. AYACHI, C. BIDAN, N. PRIGENT. *A Trust-Based IDS for the AODV Protocol*, in "Proc. of the 12th international conference on Information and communications security (ICICS 2010)", Barcelona, Spain, December 2010

[3] M. BEN GHORBEL-TALBI, F. CUPPENS, N. CUPPENS-BOULAHIA, D. LE MÉTAYER, G. PIOLLE. *Delegation of Obligations and Responsibility*, in "Future Challenges in Security and Privacy for Academia and Industry - 26th IFIP TC 11 International Information Security Conference (SEC2011)", J. CAMENISCH, S. FISCHER-HÜBNER, Y. MURAYAMA, A. PORTMANN, C. RIEDER (editors), IFIP AICT, Springer, 2011, vol. 354, pp. 197–209

[4] J. C. DEMAY, F. MAJORCZYK, E. TOTEL, F. TRONEL. *Detecting illegal system calls using a data-oriented detection model*, in "Proc. of the 26th IFIP TC 11 International Information Security Conference - Future Challenges in Security and Privacy for Academia and Industry (SEC2011)", Lucerne, Switzerland, Jun 2011

[5] S. GAMBS, B. KÉGL, E. AÏMEUR. *Privacy-preserving boosting*, in "Data Mining and Knowledge Discovery", 2007, vol. 14, n° 1, pp. 131-170

[6] G. HIET, V. VIET TRIEM TONG, L. MÉ, B. MORIN. *Policy-based intrusion detection in web applications by monitoring Java information flows*, in "International Journal of Information and Computer Security", 2009, vol. 3, n° 3/4, pp. 265–279

[7] L. MÉ, H. DEBAR. *New Directions in Intrusion Detection and Alert Correlation*, in "The Information - Interaction - Intelligence (I3) Journal", 2010, vol. 10, n° 1

[8] G. PIOLLE, Y. DEMAZEAU. *Representing privacy regulations with deontico-temporal operators*, in "Web Intelligence and Agent Systems", Jul 2011, vol. 9, n° 3, pp. 209-226

[9] E. TOTEL, F. MAJORCZYK, L. MÉ. *COTS Diversity based Intrusion Detection and Application to Web Servers*, in "Proc. of the International Symposium on Recent Advances in Intrusion Detection (RAID'2005)", Seattle, USA, September 2005

[10] D. ZOU, N. PRIGENT, J. BLOOM. *Compressed Video Stream Watermarking for Peer-to-Peer-Based Content Distribution Network*, in "Proc. of the IEEE International Conference on Multimedia and Expo (IEEE ICME)", New York City, USA, June 2009

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] M. ASSAF. *From qualitative to quantitative program analysis : permissive enforcement of secure information flow*, Université Rennes 1, May 2015, https://tel.archives-ouvertes.fr/tel-01184857

[12] C. HUMPHRIES. *User-centred security event visualisation*, Université de Rennes 1, December 2015, https://hal.inria.fr/tel-01242084

[13] P. LAJOIE-MAZENC. *Reputation and privacy preservation in dynamic auto-organized networks*, Université Rennes 1, September 2015, https://tel.archives-ouvertes.fr/tel-01232139

[14] R. PAIVA MELO MARIN. *Enhancing Privacy Protection in Social Network Systems Through Decentralization and Policy Conflict Management*, CentraleSupélec, September 2015, https://hal.inria.fr/tel-01242091

Articles in International Peer-Reviewed Journals

[15] E. ANCEAUME, Y. BUSNEL, E. SCHULTE-GEERS, B. SERICOLA. *Optimization Results for a Generalized Coupon Collector Problem*, in "Journal of Applied Probability", June 2015, 9 p. , https://hal.archives-ouvertes.fr/hal-01189578

[16] E. ANCEAUME, Y. BUSNEL, B. SERICOLA. *New results on a generalized coupon collector problem using Markov chains*, in "Journal of Applied Probability", 2015, 17 p. [*DOI :* 10.1239/JAP/1437658606], https://hal.archives-ouvertes.fr/hal-01189564

[17] G. ARFAOUI, J.-F. LALANDE, J. TRAORÉ, N. DESMOULINS, P. BERTHOMÉ, S. GHAROUT. *A Practical Set-Membership Proof for Privacy-Preserving NFC Mobile Ticketing*, in "Proceedings on Privacy Enhancing Technologies", June 2015, vol. 2015, n° 2, pp. 25-45 [*DOI :* 10.1515/POPETS-2015-0019], https://hal.inria.fr/hal-01192867

[18] 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", 2016 [*DOI :* 10.1109/TIFS.2015.2510825], https://hal.archives-ouvertes.fr/hal-01247495

[19] E. GODEFROY, E. TOTEL, M. HURFIN, F. MAJORCZYK. *Automatic Generation of Correlation Rules to Detect Complex Attack Scenarios*, in "Journal of Information Assurance and Security", 2015, vol. 10, n° 3, 11 p. , https://hal.inria.fr/hal-01241807

Articles in National Peer-Reviewed Journals

[20] G. PIOLLE. *Protection des données personnelles dans le système d'information*, in "Techniques de l'Ingenieur", October 2015, vol. TIB458DUO, n° h5455, 21 p. , https://hal.inria.fr/hal-01221892

Invited Conferences

[21] E. ANCEAUME, Y. BUSNEL, N. RIVETTI. *Estimating the Frequency of Data Items in Massive Distributed Streams*, in "IEEE 4th Symposium on Network Cloud Computing and Applications (NCCA)", Munich, Germany, June 2015, 9 p. , https://hal.archives-ouvertes.fr/hal-01194529

[22] S. GAMBS, G. PIOLLE. *Les techniques d'effacement des données*, in "Le droit à l'oubli numérique, enjeux et perspectives", Rennes, France, Institut de l'Ouest : Droit et Europe, March 2015, https://hal.inria.fr/hal-01241492

[23] J.-F. LALANDE. *Sécurité Android: exemples de malware*, in "Colloque International sur la Sécurité des Systèmes d'Information", Kénitra, Morocco, March 2015, https://hal.inria.fr/hal-01136768

[24] G. PIOLLE. *La protection des données personnelles vue par un informaticien*, in "Journées thématiques: Respect de la vie privée et services mobiles sans contact", Meudon, France, May 2015, https://hal.inria.fr/hal-01241511

International Conferences with Proceedings

[25] *Best Paper*
A. ABRAHAM, R. ANDRIATSIMANDEFITRA RATSISAHANANA, A. BRUNELAT, J.-F. LALANDE, V. VIET TRIEM TONG. *GroddDroid: a Gorilla for Triggering Malicious Behaviors*, in "10th International Conference on Malicious and Unwanted Software", Fajardo, Puerto Rico, IEEE Computer Society, October 2015, https://hal.inria.fr/hal-01201743.

[26] M. ALAGGAN, S. GAMBS, S. MATWIN, M. TUHIN. *Sanitization of Call Detail Records via Differentially-Private Bloom Filters*, in "Data and Applications Security and Privacy XXIX (DBSec'15)", Fairfax, United States, July 2015 [*DOI :* 10.1007/978-3-319-20810-7_15], https://hal.inria.fr/hal-01244580

[27] E. ANCEAUME, Y. BUSNEL. *Estimer la corrélation à la volée entre flux massifs est possible avec très peu de mémoire*, in "ALGOTEL 2015 — 17èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", Beaune, France, June 2015, https://hal.archives-ouvertes.fr/hal-01147072

[28] E. ANCEAUME, Y. BUSNEL, P. LAJOIE-MAZENC, G. TEXIER. *Reputation for Inter-Domain QoS Routing*, in "International Symposium on Network Computing and Applications (NCA)", Boston, United States, IEEE, September 2015, 5 p. , https://hal.archives-ouvertes.fr/hal-01190451

[29] E. ANCEAUME, Y. BUSNEL, N. RIVETTI, B. SERICOLA. *Identifying Global Icebergs in Distributed Streams*, in "34th International Symposium on Reliable Distributed Systems (SRDS)", Montreal, Canada, September 2015, 10 p. , https://hal.archives-ouvertes.fr/hal-01194511

[30] E. ANCEAUME, F. CASTELLA, A. MOSTEFAOUI, B. SERICOLA. *A Message-Passing and Adaptive Implementation of the Randomized Test-and-Set Object*, in "International Symposium on Network Computing and Applications (NCA)", Boston, United States, September 2015, 9 p. , https://hal.archives-ouvertes.fr/hal-01190379

[31] R. ANDRIATSIMANDEFITRA RATSISAHANANA, V. VIET TRIEM TONG. *Detection and Identification of Android Malware Based on Information Flow Monitoring*, in "The 2nd IEEE International Conference on Cyber Security and Cloud Computing (CSCloud 2015)", New York, United States, November 2015, https://hal.inria.fr/hal-01191595

[32] G. ARFAOUI, J.-F. LALANDE, S. GHAROUT, J. TRAORÉ. *Practical and Privacy-Preserving TEE Migration*, in "9th IFIP WG 11.2 International Conference on Information Security Theory and Practice", Heraklion, Greece, R. AKRAM, S. JAJODIA (editors), LNCS, Springer, August 2015, vol. 9311, pp. 153-168 [*DOI :* 10.1007/978-3-319-24018-3_10], https://hal.inria.fr/hal-01183508

[33] L. CAVIGLIONE, J.-F. LALANDE, W. MAZURCZYK, S. WENDZEL. *Analysis of Human Awareness of Security and Privacy Threats in Smart Environments*, in "HAS - 3rd International Conference on Human Aspects of Information Security, Privacy and Trust", Los Angeles, United States, T. TRYFONAS, I. G. ASKOXYLAKIS (editors), LNCS, August 2015, vol. 9190 [*DOI :* 10.1007/978-3-319-20376-8], https://hal.inria.fr/hal-01182303

[34] P. COTRET, G. HIET, G. GOGNIAT, V. LAPOTRE. *HardBlare: an efficient hardware-assisted DIFC for non-modified embedded processors*, in "CHES 2015 - Workshop on Cryptographic Hardware and Embedded Systems", Saint-Malo, France, September 2015, https://hal-centralesupelec.archives-ouvertes.fr/hal-01252597

[35] S. GAMBS, C. EDUARDO ROSAR KOS LASSANCE, C. ONETE. *The Not-so-distant Future: Distance-Bounding Protocols on Smartphones*, in "14th Smart Card Research and Advanced Application Conference", Bochum, Germany, November 2015, https://hal.inria.fr/hal-01244606

[36] L. GEORGET, G. PIOLLE, F. TRONEL, V. VIET TRIEM TONG, M. JAUME. *Towards a Formal Semantics for System Calls in terms of Information Flow*, in "Tenth International Conference on Systems (ICONS 2015)", Barcelone, Spain, IARIA, April 2015, pp. 1-4, ISBN: 978-1-61208-399-5ISSN: 2308-4243, https://hal-supelec.archives-ouvertes.fr/hal-01149471

[37] L. GEORGET, F. TRONEL, V. VIET TRIEM TONG. *Kayrebt: An Activity Diagram Extraction and Visualization Toolset Designed for the Linux Codebase*, in "3rd IEEE Working Conference on Software Visualization - VISSOFT 2015", Bremen, Germany, IEEE, September 2015, https://hal-supelec.archives-ouvertes.fr/hal-01213233

[38] E. GODEFROY, E. TOTEL, M. HURFIN, F. MAJORCZYK. *Assessment of an Automatic Correlation Rules Generator*, in "Eleventh International Conference on Information Systems Security (ICISS 2015)", Kolkata, India, December 2015, https://hal.inria.fr/hal-01241810

[39] G. HIET, H. DEBAR, S. MÉNOUAR, V. HOUDEBINE. *Etude comparative des formats d'alertes*, in "C&ESAR (Computer & Electronics Security Applications Rendez-vous) 2015", Rennes, France, November 2015, pp. 125-148, https://hal-supelec.archives-ouvertes.fr/hal-01242786

[40] P. LAJOIE-MAZENC, E. ANCEAUME, G. GUETTE, T. SIRVENT, V. VIET TRIEM TONG. *Mécanisme de réputation distribué préservant la vie privée avec témoignages négatifs*, in "ALGOTEL 2015 - 17èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", Beaune, France, June 2015, https://hal.archives-ouvertes.fr/hal-01148072

[41] P. LAJOIE-MAZENC, E. ANCEAUME, G. GUETTE, T. SIRVENT, V. VIÊT TRIEM TONG. *Privacy-Preserving Reputation Mechanism: A Usable Solution Handling Negative Ratings*, in "IFIP WG 11.1 International Conference on Trust Management", Hambourg, Germany, May 2015, https://hal-supelec.archives-ouvertes.fr/hal-01131975

[42] C. LI, M. HURFIN, Y. WANG. *Reputation Propagation and Updating in Mobile Ad Hoc Networks with Byzantine Failures*, in "14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-15)", Helsinki, Finland, August 2015 [*DOI :* 10.1109/TRUSTCOM.2015.364], https://hal.inria.fr/hal-01242694

[43] Y. MOCQUARD, E. ANCEAUME, J. ASPNES, Y. BUSNEL, B. SERICOLA. *Counting with Population Protocols*, in "International Symposium on Network Computing and Applications (NCA)", Boston, United States, IEEE, September 2015, 9 p. , https://hal.archives-ouvertes.fr/hal-01189596

[44] N. RIVETTI, L. QUERZONI, E. ANCEAUME, Y. BUSNEL, B. SERICOLA. *Efficient Key Grouping for Near-Optimal Load Balancing in Stream Processing Systems* , in "The 9th ACM International Conference on Distributed Event-Based Systems (DEBS)", Oslo, Norway, June 2015 [*DOI :* 10.1145/2675743.2771827], https://hal.archives-ouvertes.fr/hal-01194518

Conferences without Proceedings

[45] R. ANDRIATSIMANDEFITRA RATSISAHANANA, T. GENET, L. GUILLO, J.-F. LALANDE, D. PICHARDIE, V. VIET TRIEM TONG. *Kharon : Découvrir, comprendre et reconnaître des malware Android par suivi de flux d'information*, in "Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information", Troyes, France, May 2015, https://hal.inria.fr/hal-01154368

[46] U. M. AÏVODJI, S. GAMBS, M.-J. HUGUET, M.-O. KILLIJIAN. *Privacy-preserving carpooling*, in "Odysseus 2015 - 6th International Workshop on Freight Transportation and Logistics", Ajaccio, France, May 2015, https://hal.archives-ouvertes.fr/hal-01146639

[47] M. BOIZARD, S. GAMBS. *Le droit à l'oubli numérique face aux moteurs de recherche*, in "Sciences et droits de l'homme", Paris, France, Réseau droit, sciences et techniques (GDR 3178) and UMR de droit comparé de Paris I, October 2015, https://halshs.archives-ouvertes.fr/halshs-01216636

[48] M. BOIZARD, S. GAMBS. *Retour d'expérience d'un projet de recherche pluridisciplinaire droit - informatique - sociologie : le droit à l'oubli*, in "Journée SHS et numérique", Rennes, France, Labex CominLabs, June 2015, https://halshs.archives-ouvertes.fr/halshs-01203770

[49] S. GAMBS, J.-F. LALANDE, J. TRAORÉ. *ANR LYRICS: Cryptographie pour la protection de la vie privée, optimisée pour les services mobiles sans contact*, in "Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information", Troyes, France, May 2015, https://hal.inria.fr/hal-01154374

[50] G. MALIS, A. BLANDIN, G. PIOLLE. *The articulation between the legal and technical means of erasure of data online, from the perspective of the user*, in "6ème Atelier sur la Protection de la Vie Privée (APVP'15)", Mosnes, France, June 2015, https://hal-supelec.archives-ouvertes.fr/hal-01166402

Research Reports

[51] E. ANCEAUME, Y. BUSNEL, N. RIVETTI, B. SERICOLA. *Identifying Global Icebergs in Distributed Streams*, Cnrs ; Inria Rennes ; Université de Nantes, April 2015, https://hal.archives-ouvertes.fr/hal-01141829

[52] E. ANCEAUME, Y. BUSNEL, E. SCHULTE-GEERS, B. SERICOLA. *Optimization results for a generalized coupon collector problem*, Inria Rennes ; Cnrs, January 2015, https://hal.archives-ouvertes.fr/hal-01141577

[53] M. BOIZARD, A. BLANDIN, C. CORGAS-BERNARD, G. DEDESSUS LE MOUSTIER, S. GAMBS, C. LEJEALLE, S. MOISDON-CHATAIGNER, P. PIERRE, G. PIOLLE, L. ROUSVOAL. *Le droit à l'oubli*, Mission de recherche Droit et Justice, February 2015, n^{o} 11-25, 216 p. , Responsable scientifique du projet : Maryline Boizard, https://halshs.archives-ouvertes.fr/halshs-01223778

[54] N. RIVETTI, E. ANCEAUME, Y. BUSNEL, L. QUERZONI, B. SERICOLA. *Proactive Online Scheduling for Shuffle Grouping in Distributed Stream Processing Systems*, LINA-University of Nantes ; Sapienza Università di Roma (Italie), December 2015, https://hal.inria.fr/hal-01246701

Other Publications

[55] A. ABRAHAM, R. ANDRIATSIMANDEFITRA RATSISAHANANA, N. KISS, J.-F. LALANDE, V. VIET TRIEM TONG. *Towards Automatic Triggering of Android Malware*, July 2015, 12th International Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Poster, https://hal.inria.fr/hal-01168354

[56] E. ANCEAUME, F. CASTELLA, A. MOSTEFAOUI, B. SERICOLA. *A Message-Passing and Adaptive Implementation of the Randomized Test-and-Set Object*, August 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01075650

[57] G. ARFAOUI, J.-F. LALANDE, J. TRAORÉ, N. DESMOULINS, P. BERTHOMÉ, S. GHAROUT. *A Practical Set-Membership Proof for Privacy-Preserving NFC Mobile Ticketing*, May 2015, working paper or preprint, https://hal.inria.fr/hal-01150321

[58] D. CRÉMILLEUX, F. MAJORCZYK, N. PRIGENT. *VEGAS: Visualizing, Exploring and Grouping AlertS* , October 2015, International Symposium on Visualization for Cyber Security - VizSec 2015, Poster, https://hal-supelec.archives-ouvertes.fr/hal-01246441

[59] E. GODEFROY, E. TOTEL, M. HURFIN, F. MAJORCZYK. *Generation and Assessment of correlation rules to Detect Complex Attack Scenarios*, September 2015, IEEE Conference on Communications and Network Security (CNS 2015), Poster, https://hal.inria.fr/hal-01241813

[60] P. LAJOIE-MAZENC, E. ANCEAUME, G. GUETTE, T. SIRVENT, V. VIET TRIEM TONG. *Efficient Distributed Privacy-Preserving Reputation Mechanism Handling Non-Monotonic Ratings*, January 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01104837

[61] Y. MOCQUARD, E. ANCEAUME, J. ASPNES, Y. BUSNEL, B. SERICOLA. *Counting with Population Protocols*, July 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01170575

References in notes

[62] J. C. DEMAY, F. MAJORCZYK, E. TOTEL, F. TRONEL. *Detecting illegal system calls using a data-oriented detection model*, in "In Proc. of the 26th IFIP TC 11 International Information Security Conference - Future Challenges in Security and Privacy for Academia and Industry (SEC2011)", Lucerne, Switzerland, Jun 2011

[63] G. HIET, V. VIET TRIEM TONG, L. MÉ, B. MORIN. *Policy-Based Intrusion Detection in Web Applications by Monitoring Java Information Flows*, in "3nd International Conference on Risks and Security of Internet and Systems (CRiSIS)", 2008

[64] A. MYERS, F. SCHNEIDER, K. BIRMAN. *Nsf project security and fault tolerance, nsf cybertrust grant 0430161*, 2004, http://www.cs.cornell.edu/Projects/secft/

[65] O. SARROUY, E. TOTEL, B. JOUGA. *Building an application data behavior model for intrusion detection*, in "Proc. of the 23rd Annual IFIP WG 11.3 Working Conference on Data and Applications Security", Montreal Canada, 07 2009, pp. 299–306

[66] J. ZIMMERMANN, L. MÉ, C. BIDAN. *An improved reference flow control model for policy-based intrusion detection*, in "Proc. of the 8th European Symposium on Research in Computer Security (ESORICS)", October 2003