IN PARTNERSHIP WITH:
CNRS

Université Rennes 1

SUPELEC (Rennes)

Activity Report 2014

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

Keywords: Security, Privacy, Distributed Systems, Visualization

Creation of the Project-Team: 2011 July 01.

1. Members

Research Scientists

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

Faculty Members

Ludovic Mé [Team leader, SUPELEC, Professor, HdR]
Christophe Bidan [SUPELEC, Professor, HdR]
Sébastien Gambs [Univ. Rennes I, Associate Professor (Inria research chair), HdR]
Gilles Guette [Univ. Rennes I, Associate Professor]
Guillaume Hiet [SUPELEC, Associate Professor]
Jean-François Lalande [INSA Centre Val de Loire, Associate Professor]
Guillaume Piolle [SUPELEC, Assistant Professor]
Nicolas Prigent [SUPELEC, Associate Professor]
Eric Totel [SUPELEC, Professor, HdR]
Frédéric Tronel [SUPELEC, Associate Professor]
Valérie Viet Triem Tong [SUPELEC, Associate Professor]

Engineers

Guillaume Brogi [Inria, until Nov 2014]
David Lanoe [Univ. Rennes I]
Thomas Letan [SUPELEC, until Sep 2014]

PhD Students

Radoniaina Andriatsimandefitra [SUPELEC]
Georges Bossert [AMOSSYS]
Mounir Assaf [CEA and SUPELEC]
Simon Boche [Univ. Rennes I]
Solenn Brunet [Orange Labs, from Oct 2014]
Erwan Godefroy [DGA]
Laurent Georget [Univ. Rennes I, from Oct 2014]
Florian Grandhomme [Univ. Rennes I, from Oct 2014]
Antoine Guellier [Univ. Rennes I]
Kun He [Inst. de Recherche Technologique B-COM]
Mouna Hkimi [Inria]
Christopher Humphries [Inria]
Paul Lajoie-Mazenc [Univ. Rennes I]
Julien Lolive [Telecom Bretagne]
Regina Paiva Melo Marin [Inria]
Pierre Obame Meye [Orange]
Deepak Subramanian [SUPELEC]

Post-Doctoral Fellow

Maria Cristina Onete [Inria, from Sep 2014 (previously Univ. Rennes 1)]

Visiting Scientists

Özgür Dagdelen [Darmstadt University of Technology, Mar 2014]

Jean-Marc Robert [Univ. Rennes I, until Jun 2014]

Administrative Assistant

Lydie Mabil [Inria]

Others

Adrien Brunelat [Univ. Rennes I, internship from Feb 2014 until Aug 2014]
Karim Chahal [SUPELEC, internship from May 2014 until Jul 2014]
Laurent Georget [Univ. Rennes I, internship from Feb 2014 until Aug 2014]
Romaric Ludinard [ATER, Univ. Rennes I, from Sep 2014]
Frédéric Majorczyk [external collaborator, DGA]
Mario Julian Sackmann [Inria, internship from Sep 2014]
Julien Sicre [SUPELEC, internship until Aug 2014]
Corentin Soriot [SUPELEC, internship from May 2014 until Jul 2014]

2. Overall Objectives

2.1. CIDRE in Brief

Our long term ambition is to contribute to build 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 rely heavily 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.* [63], 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 his 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 can also be related 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 as particular cases most of the examples mentioned above. 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 if it is valuable or not) is 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, PDA, 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 violations of the security policies 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.

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 there are thousands of machines that are every day victims of malware, 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 three complementary methods:

- Illegal Flow Detection: This first method intends to detect information flows that violate the security policy [66], [62]. 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 [60], [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 in detecting 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).

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 viruses signatures.
- At the set of nodes level, we revisit the distributed problems such as clock synchronization, logical clocks, consensus, properties detection, to extend the solutions proposed at node levels 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 challenge that lies ahead and also an important condition for the development of the Information Society. Moreover, due to legality and confidentiality issues, issues linked to privacy emerge naturally for applications working on sensitive data, such as medical records of patients or proprietary datasets of enterprises. 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 product. 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 [64], 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 disclosure of location (that typically occur in location-based services) and privacy issues in social networks. 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). 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 an access control decision.

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. Domain

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 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 brings many challenges that could benefit from ideas, approaches and solutions studied by CIDRE in the context of distributed systems.

5. New Software and Platforms

5.1. Intrusion Detection and Privacy

Members of the team have developed several intrusion detectors and security tools: **Blare** implements our approach of illegal information flow detection at the OS level for a single node and a set of nodes; **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; **Netzob** is an open-source tool for reverse engineering, traffic generation and fuzzing of communication protocols; a log visualization tool called **ELVIS** (Extensible Log VISualization) has been implemented in order to test our approches for log exploration.

In addition, the team participate to the development of **GEPETO** (GEoPrivacy-Enhancing TOolkit), an open source software for managing location data (in cooperation with the CNRS Lab. LAAS, Toulouse). GEPETO can be used to visualize, sanitize, perform inference attacks, and measure the utility of a particular geolocated dataset.

These tools are still under development in the team. Nevertheless, there are not new. For more details, please see previous activity reports.

6. New Results

6.1. Highlights of the Year

The supervision of distributed system relies heavily on correlation mechanisms that are responsible for collecting alerts coming from sensors and detecting complex scenarios in the flow of alerts. The problem is that it requires to write complex correlation rules. The work we have performed proposes a technique to generate semi-automatically such correlation rules. It describes a process that uses an attack tree and a representation of the system as inputs, and generate a correlation tree that can be translated in an alert correlation description language. This work received the best paper award of SAR-SSI 2014 [50].

One approach to protect the privacy of users in personalized recommendation systems is to publish a sanitized version of the profile of the user by relying a non-interactive mechanism compliant with the concept of differential privacy. In a joint work with Raghavendran Balu and Teddy Furon (LinkMedia Inria team), we have consider two existing schemes offering a differentially private representation of profiles: BLIP (BLoom-and-flIP) and JLT (Johnson-Lindenstrauss Transform). For assessing their security levels, we play the role of an adversary aiming at reconstructing a user profile. To realize this, we design two inference attacks named single and joint decoding. The first inference attack tests the presence of a single item in the profile, and is iterated independently for each possible item of the item set. In contrast, the second inference attack aims at deciding whether a particular subset of items is likely to be in the user profile. This attack is tested on all the possible subsets of items. Our contributions are a theoretical analysis and practical implementations of both attacks tested on datasets composed of real user profiles revealing that joint decoding is the most powerful attack. This also gives useful insights on the setting the differential privacy parameter ϵ. This work has received the best student paper award at the conference ESORICS 2014.
BEST PAPER AWARD :
[27] **Challenging differential privacy: the case of non-interactive mechanisms in European Symposium on Research in Computer Security**. R. BALU, T. FURON, S. GAMBS.

6.2. Intrusion Detection

6.2.1. Intrusion detection based on an analysis of information flow control

In 2014, Laurent Georget has started his PhD thesis in the team, working on a subject related to the analysis of information flow control at the kernel level. The goal of his PhD thesis is to propose a formal semantics of the system calls for a real operating systems (namely Linux). This semantics will provide insights about these system calls in terms of information flow. This work will help us to test in a more systematic and efficient way, our reference implementation of a information monitor at the kernel level (Blare).

Blare allows monitoring information flow and identifies the flows that do not conform to a security policy that has been previously defined. Please notice that any explicit flows between OS objects (sockets, files, etc.) are monitored and that in consequence hidden channel attacks cannot be detected by this approach.

We have already developed a dedicated test framework for this software. However, each test written by the developer must be accompanied with the possible results in terms of information flows. The framework simply compares the effective result with the set of expected results. A test passes when the effective result belongs to the set of expected results, and fails otherwise. However, this strategy has turned to be less intuitive than expected. Some system calls must be tested by using several processes operating concurrently. In these cases, the scheduling of processes can produce many different scenarios that will translate quite differently in terms of information flows. To be more confident in our implementation, we really need a stronger and more formal path. The PhD thesis of Laurent Georget is trying to bridge the gap between Blare implementation and the interpretation of the results obtained by running the information flow monitor.

6.2.2. Malware characterization through information flow monitoring

Monitoring information flows consists in observing how pieces of information are disseminated in a given environment. At system level, it consists in intercepting actions performed by an application to deduce how the application disseminates information within the entire operating system. We have propose a new approach to classify and later detect applications infected by malware based on the way they disseminate their own data within an operating system. For this purpose, we first introduce a data-structure named System Flow Graph [thèse Rado to ref.] that offers a compact representation of how pieces of data flow inside a system. A system flow graph describes the external behavior of an application during one execution. Its construction requires no knowledge about the inner working of the application. The graph is built using Blare as an information-flow monitor and more precisely its produced log. We have presented in [25] how these graphs reveal helpful to understand malware behavior and thus why it can help an expert to give a diagnosis in case of intrusion.

6.2.3. Terminating-insensitive non-interference verification based on information flow control

In 2010-2011, we started an informal collaboration with colleagues from CEA LIST laboratory. This collaboration has turned into a reality by the funding of a PhD student (Mounir Assaf). This PhD thesis is about the verification of security properties of programs written in an imperative language with pointer aliasing (a subset of C language) by techniques borrowed from the domain of static analysis. One of the property of interest for the security field is called terminating-insensitive non-interference. Briefly speaking, when verified by a program, this property ensures that the content of any secret variable can not leak into public ones (for any terminating execution). However, this property is too strict in the sense that a large number of programs although perfectly secure are rejected by classical analyzers. Finally in 2014, Mounir Assaf enhanced his previous work on static analysis by introducing a method permitting to quantify information leakage in a C program. This approach requires a theoretical definition of the quantification of information flow leakage and is very promising.

6.2.4. Visualization of security events

The first part of this year was dedicated to tune a working prototype of ELVIS [38] in order to perform field trials with our partner DGA-MI. The prototype was largely well accepted. We were invited by the DGA-MI to present a poster in the Forum DGA Innovation 2014. We will also present ELVIS during the FIC 2014 in Lille on the Pôle Cyber-Défense area.

However, ELVIS also exhibited some limitations of our approach in the way multiple datasets are handled together. We therefore went for a new cycle of research whose objective is to enhance ELVIS in two ways: first to handle multiple datasets at the same time, and second to improve interactions so as to better fit with the processes in forensics. The results of our research lead to CORGI (Combination, Organization and Reconstruction through Graphical Interactions) [39] which was presented at VizSec 2014 (part of Vis 2014). CORGI improves ELVIS by introducing the concepts of *values of interest* that consist in interesting values found by an analyst and that can be used later to search and filter in the other datasets. They are an intuitive and efficient way to link various datasets while the analyst performs its tasks. An early prototype has been developed.

6.2.5. Control flow integrity

In [40] we have studied physical attacks that could disturb the normal execution of an embedded program of a smartcard. Such attacks can be performed using laser beams, electromagnetic glitches and can corrupt the flow of information or change the control flow of the program. We have studied the particular case of the control flow and we have developed software countermeasures that increase the robustness of the control flow. These countermeasures do not require any additional software or hardware external components which is useful for devices like smartcards whose architecture cannot be modified. The developed countermeasures have been validated with the help of the VIS model checker in order to verify that they do not disturb the original execution of the code.

6.2.6. 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 [50], [47], [36], we focus on the transformation process that allows to translate the description of a complex attack scenario into correlation rules. 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.

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 (occurrence 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 current work aims at identifying the possible errors tolerated by the compacted automaton.

6.3. Privacy

6.3.1. Privacy in location-based services

With the advent of GPS-equipped devices, a massive amount of location data is being collected, raising the issue of the privacy risks incurred by the individuals whose movements are recorded. In [17], we focus on a specific inference attack called the de-anonymization attack, by which an adversary tries to infer the identity of a particular individual behind a set of mobility traces. More specifically, we propose an implementation of this attack based on a mobility model called Mobility Markov Chain (MMC). A MMC is built out from the mobility traces observed during the training phase and is used to perform the attack during the testing phase. We design several distance metrics quantifying the closeness between two MMCs and combine these distances to build de-anonymizers that can re-identify users in an anonymized geolocated dataset. Experiments conducted on real datasets demonstrate that the attack is both accurate and resilient to sanitization mechanisms such as downsampling.

One example of a location-based services is dynamic carpooling (also known as instant or ad-hoc ridesharing), which is a service that arranges one-time shared rides on very short notice. This type of carpooling generally makes use of three recent technological advances: (i) navigation devices to determine a route and arrange the shared ride; (ii) smartphones for a traveller to request a ride from wherever she happens to be; and (iii) social networks to establish trust between drivers and passengers. However, the mobiquitous environment in which dynamic carpooling is expected to operate raises several privacy issues. Among all the personal identifiable information, learning the location of an individual is one of the greatest threats against her privacy. For instance, the spatio-temporal data of an individual can be used to infer the location of her home and workplace, to trace her movements and habits, to learn information about her centre of interests or even to detect a change from her usual behavior. Therefore, preserving location privacy is a major issue to be able to leverage the possibilities offered by dynamic carpooling. In a joint work with researchers from LAAS-CNRS [16], we have propose to follow the privacy-by-design approach by integrating the privacy aspect in the design of dynamic carpooling, henceforth increasing its public (and political) acceptability and trust.

A secure location-based service requires that a mobile user certifies his position before gaining access to a resource. Currently, most of the existing solutions addressing this issue assume a trusted third party that can vouch for the position claimed by a user. However, as computation and communication capacities become ubiquitous with the large scale adoption of smartphones by individuals, these resources can be leverage on to solve this issue in a collaborative and private manner. More precisely together with researchers from LAAS-CNRS, we introduce PROPS, for Privacy-Preserving lOcation Proof System, which allows users to generate proofs of location in a private and distributed way using neighboring nodes as witnesses [35]. PROPS provides security properties such as unforgeability and non-transferability of the proofs, as well as resistance to classical localization attacks.

One of the fundamental building block to construct a location proof system such as PROPS is a distance-bounding protocol. More precisely, in distance-bounding authentication protocols a verifier assesses that a prover is (1) legitimate and (2) in the verifier's proximity. Proximity checking is done by running time-critical exchanges between both parties. This enables the verifier to detect relay attacks (also called mafia fraud). While most distance-bounding protocols offer resistance to mafia, distance, and impersonation attacks, only few protect the privacy of the authenticating prover. One exception is the protocol due to Hermans, Peeters, and Onete, which offers prover untraceability with respect to a Man-in-the-Middle adversary. However in this protocol as well as in all other distance-bounding protocols, any legitimate verifier can identify, and thus track, the prover. In order to counter the threats of possible corruption or data leakage from verifiers, together with Jean-Marc Robert (ETS, Montréal) we propose a distance-bounding protocol providing strong prover privacy with respect to the verifier and deniability with respect to a centralized back-end server managing prover creation and revocation [33]. In particular, we first formalize the notion of prover anonymity, which guarantees that even verifiers cannot trace provers, and deniability, which allows provers to deny that they were authenticated by a verifier. Finally, we prove that our protocol achieves these strong guarantees.

A particular class of relay attacks against distance-bounding protocols is called terrorist fraud in which a distant malicious prover colludes with an attacker located in a verier's proximity when authenticating. Existing distance-bounding protocols resisting such attacks are designed to be lightweight and thus symmetric, relying on a secret shared by the prover and the verifier. Recently, several asymmetric distance-bounding protocols were proposed by Gambs, Onete and Robert as well as by Hermans, Peter and Onete, but they fail to thwart terrorist fraud. One earlier asymmetric protocol aiming to be terrorist-fraud resistant is the DBPK-Log protocol due to Bussard and Bagga, which was unfortunately recently proven to achieve neither distance- nor terrorist-fraud resistance. In this work, we build on some ideas of the DBPK-Log scheme and propose a novel distance-bounding protocol resistant to terrorist fraud that does not require the pre-existence of a shared secret between the prover and the verifier [32]. Our construction, denoted as VSSDB (for Verifiable Secret Sharing and Distance-Bounding Protocol) relies on a veriable secret sharing scheme and on the concept of modes, which we introduce as a novel element to complement fast-round challenges in order to improve security. We prove that VSSDB achieves terrorist-fraud resistance in a relaxed security model called KeyTF-security, which we also present in this paper.

6.3.2. Equity in privacy-enhanced social networks

In [46], we have examined a novel issue in the field of policy conflict resolution, and applied it to privacy policy management in distributed social networking systems. We accepted as a starting point that in a privacy-enhanced social network, when a user publishes a document (e.g., a picture), any user referenced in this document (e.g., people tagged in pictures) should be entitled to issue a privacy policy over this document. In this case, when a given user tries to access a given document, multiple users may issue multiple access control decisions (or rulings), possibly resulting in a normative conflict. Quite a number of strategies are available for the resolution of such conflicts, the most common one being the "deny strategy", allowing any ruling denying access to the resource to take precedence over others. This is usually considered a "secure" way of dealing with access control. However, with this strategy as with many others, it is possible for a user to design her policy in a way that systematically prevents other users from interacting in a normal way, while allowing herself to potentially benefit from other people's more flexible policies. This may leads to unfair situations, in which some users take advantage of the systems while others' experience is damaged. This is particularly an issue in social networking applications, in which information sharing is a core feature and access restrictions, while necessary to protect intimacy, can sometimes be considered aggressive.

To address this particular trade-off between privacy and usability, we have introduced the notion of equity in such scenarios, a situation being equitable when all involved users have seen their policy enforced or violated in the same proportion over past interactions. We have designed a conflict resolution algorithm aimed at improving this equity in our social networking scenario, and evaluated its impact by measuring Gini coefficients (an indicator commonly used by economists to measure the distribution of wealth in a population) over the distribution of enforcement proportions in the population of users. With respect to this criterion, it actually proved more efficient than other strategies. Following these positive results, we have recently taken

steps towards a formalization and generalization of this intuitive concept of equity and the design of systematic tools to evaluate and compare the impact of any conflict resolution strategy over various possible flavors of the notion.

6.3.3. Private mobile services

The development of NFC-enabled smartphones has paved the way to new applications such as mobile payment (m-payment) and mobile ticketing (m-ticketing). However, often the privacy of users of such services is either not taken into account or based on simple pseudonyms, which does not offer strong privacy properties such as the unlinkability of transactions and minimal information leakage. In [48], [15], we introduce a lightweight privacy-preserving contactless transport service that uses the SIM card as a secure element. Our implementation of this service uses a group signature protocol in which costly cryptographic operations are delegated to the mobile phone. We have also conducted an interdisciplinary study with researchers from social sciences to analyze the media coverage in the modern public space on the topic of privacy with respect to mobile technologies [29]. Despite the difficulties highlighted by these studies, we argue that research efforts should support the emergence of mobile services that respect users' privacy as well as the development of a digital culture of privacy.

6.3.4. Architectures for privacy

In the current architecture of the Internet, there is a strong asymmetry in terms of power between the entities that gather and process personal data (e.g., major Internet companies, telecom operators, cloud providers, ...) and the individuals from which this personal data is issued. In particular, individuals have no choice but to blindly trust that these entities will respect their privacy and protect their personal data. In a position paper [34] in a collaboration with researchers from the Université de Montréal and Aarhus University, we propose an utopian crypto-democracy model based on existing scientific achievements from the field of cryptography. More precisely, our main objective is to show that cryptographic primitives, including in particular secure multiparty computation, offer a practical solution to protect privacy while minimizing the trust assumptions. In the crypto-democracy envisioned, individuals do not have to trust a single physical entity with their personal data but rather their data is distributed among several institutions. Together these institutions form a virtual entity called the Trustworthy that is responsible for the storage of this data but which can also compute on it (provided first that all the institutions agree on this). Finally, we also propose a realistic proof-of-concept of the Trustworthy, in which the roles of institutions are played by universities. This proof-of-concept would have an important impact in demonstrating the possibilities offered by the crypto-democracy paradigm.

Active fingerprinting schemes were originally invented to deter malicious users from illegally releasing an item, such as a movie or an image. To achieve this, each time an item is released, a different fingerprint is embedded in it. If the fingerprint is created from an anti-collusion code, the fingerprinting scheme can trace colluding buyers who forge fake copies of the item using their own legitimate copies. Charpentier, Fontaine, Furon and Cox were the first to propose an asymmetric fingerprinting scheme based on Tardos codes, the most efficient anti-collusion codes known to this day. However, their work focuses on security but does not preserve the privacy of buyers. To address this issue, we introduce the first privacy-preserving asymmetric fingerprinting protocol based on Tardos codes [30]. This protocol is optimal with respect traitor tracing. We also formally define the properties of correctness, anti-framing, traitor tracing, as well as buyer- and item-unlinkability. Finally, we prove that our protocol achieves these properties and give exact bounds for each of them.

6.3.5. Privacy and web services

We have proposed [61] a new model of security policy based for a first part on our previous works in information flow policy and for a second part on a model of Myers and Liskov. This new model of information flow serves web services security and allows a user to precisely define where its own sensitive pieces of data are allowed to flow through the definition of an information flow policy. A novel feature of such policy is that they can be dynamically updated, which is fundamental in the context of web services that allow the dynamic discovery of services. We have also presented an implementation of this model in a web services orchestration in BPEL (Business Process Execution Language).

6.3.6. Privacy-preserving ad-hoc routing

Last year, we have proposed NoName, a privacy-preserving ad-hoc routing protocol. Based on trapdoor, virtual switching and partially disjoint multipaths using Bloom filter, NoName ensures the anonymity of the source, of the destination and of intermediate nodes. It also ensures unlinkability between source and message and between destination and message. Since then, we have demonstrated that colluding attackers analyzing Bloom filters can locate the origin node of routes requests messages. Thus, Noname, like ARMR, another privacy-preserving ad-hoc routing protocol using also Bloom filter, do not prevent the localization of the source. We have developed a cryptographic primitive called fuzzy cryptographic Bloom filter that offers the same functions as Bloom filters (in our case, preventing routing loops) while preventing localization of the source of route request messages.

6.4. Trust

Digital reputation mechanisms have indeed emerged as a promising approach to cope with the specificities of large scale and dynamic systems. Similarly to real world reputation, a digital reputation mechanism expresses a collective opinion about a target user based on aggregated feedback about his past behavior. The resulting reputation score is usually a mathematical object (*e.g.* a number or a percentage). It is used to help entities in deciding whether an interaction with a target user should be considered. Digital reputation mechanisms are thus a powerful tool to incite users to behave trustworthily. Indeed, a user who behaves correctly improves his reputation score, encouraging more users to interact with him. In contrast, misbehaving users have lower reputation scores, which makes it harder for them to interact with other users. To be useful, a reputation mechanism must itself be accurate against adversarial behaviors. Indeed, a user may attack the mechanism to increase his own reputation score or to reduce the reputation of a competitor. A user may also free-ride the mechanism and estimate the reputation of other users without providing his own feedback. From what has been said, it should be clear that reputation is beneficial in order to reduce the potential risk of communicating with almost or completely unknown entities. Unfortunately, the user privacy may easily be jeopardized by reputation mechanisms, which is clearly a strong argument to compromise the use of such a mechanism. Indeed, by collecting and aggregating user feedback, or by simply interacting with someone, reputation systems can be easily manipulated in order to deduce user profiles. Thus preserving user privacy while computing robust reputation is a real and important issue that we address in our work [51]. Specifically, our proposal aims at enhancing signatures of reputation mechanism proposed by Bethencourt and his colleagues in 2010 by handling negative votes. Taking into account negative votes implies major modifications with respect to the implementation of the mechanism. Specifically, in the mechanism of Bethencourt and co-authors, service providers locally store votes cast at the end of their interaction with their clients, and compute their reputation score by aggregating the received votes. In particular, they can keep only a subset of them, which clearly makes negative votes useless. We propose to improve upon this solution by guaranteeing that negative votes are taken into account. This is achieved by making both reputation scores and votes of service providers publicly available in order to prevent anyone from modifying or hiding them. Our proposition accomplishes this without jeopardizing the privacy of clients.

6.5. Other topics related to security and distributed computing

6.5.1. Network monitoring and fault detection

Monitoring a system consists in collecting and analyzing relevant information provided by the monitored devices, so as to be continuously aware of the system state (situational awareness). However, the ever growing complexity and scale of systems makes both real time monitoring and fault detection a quite tedious task. Thus the usually adopted option is to focus solely on a subset of information states, so as to provide coarse-grained indicators. As a consequence, detecting isolated failures or anomalies is a quite challenging issue. We propose in [23], [42] to address this issue by pushing the monitoring task at the edge of the network. We present a peer-to-peer based architecture, which enables nodes to adaptively and efficiently self-organize according to their ”health” indicators. By exploiting both temporal and spatial correlations that exist between a device and

its vicinity, our approach guarantees that only isolated anomalies (an anomaly is isolated if it impacts solely a monitored device) are reported on the fly to the network operator. We show that the end-to-end detection process, *i.e.*, from the local detection to the management operator reporting, requires a logarithmic number of messages in the size of the network.

6.5.2. Secure data deduplication scheme

Data grows at the impressive rate of 50% per year, and 75% of the digital world is a copy [1]. Although keeping multiple copies of data is necessary to guarantee their availability and long term durability, in many situations the amount of data redundancy is immoderate. By keeping a single copy of repeated data, data deduplication is considered as one of the most promising solutions to reduce the storage costs, and improve users experience by saving network bandwidth and reducing backup time. However, this solution must now solve many security issues to be completely satisfying. In this paper we target the attacks from malicious clients that are based on the manipulation of data identifiers and those based on backup time and network traffic observation. In [43], we have presented a deduplication scheme mixing an intra-and an inter-user deduplication in order to build a storage system that is secure against the aforementioned type of attacks by controlling the correspondence between files and their identifiers, and making the inter-user deduplication unnoticeable to clients using deduplication proxies. Our method provides global storage space savings, per-client bandwidth network savings between clients and deduplication proxies, and global network bandwidth savings between deduplication proxies and the storage server. The evaluation of our solution compared to a classic system shows that the overhead introduced by our scheme is mostly due to data encryption which is necessary to ensure confidentiality. This work relies on Mistore [44], [45], a distributed storage system aiming at guaranteeing data availability, durability, low access latency by leveraging the Digital Subscriber Line infrastructure of an ISP. Mistore uses the available storage resources of a large number of home gateways and points of presence for content storage and caching facilities reducing the role of the data center to a load balancer. Mistore also targets data consistency by providing multiple types of consistency criteria on content and a versioning system allowing users to get access to any prior versions of their contents.

6.5.3. Metrics estimation on very large data streams

In [12], we consider the setting of large scale distributed systems, in which each node needs to quickly process a huge amount of data received in the form of a stream that may have been tampered with by an adversary (*i.e.*, data items ordering can be manipulated by an oblivious adversary). In this situation, a fundamental problem is how to detect and quantify the amount of work performed by the adversary. To address this issue, we propose AnKLe (for Attack-tolerant eNhanced Kullback- Leibler divergence Estimator), a novel algorithm for estimating the KL divergence of an observed stream compared to the expected one. AnKLe combines sampling techniques and information-theoretic methods. It is very efficient, both in terms of space and time complexities, and requires only a single pass over the data stream. Experimental results show that the estimation provided by AnKLe remains accurate even for different adversarial settings for which the quality of other methods dramatically decreases. Considering n as the number of distinct data items in a stream, we show that AnKLe is an (ε, δ)-approximation algorithm with a space complexity sublinear in the size of the domain value from which data items are drawn and the maximal stream length.

We go a step further by proposing in [22] a metric, called codeviation, that allows to evaluate the correlation between distributed streams. 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.

[1] The digital universe decade. Are you ready? John Gantz and David Reinsel, IDC information, may 2010.

6.5.4. Robustness analysis of large scale distributed systems

In the continuation of [59] which proposed an in-depth study of the dynamicity and robustness properties of large-scale distributed systems, we analyze in [13], the behavior of a stochastic system composed of several identically distributed, but non independent, discrete-time absorbing Markov chains competing at each instant for a transition. The competition consists in determining at each instant, using a given probability distribution, the only Markov chain allowed to make a transition. We analyze the first time at which one of the Markov chains reaches its absorbing state. When the number of Markov chains goes to infinity, we analyze the asymptotic behavior of the system for an arbitrary probability mass function governing the competition. We give conditions for the existence of the asymptotic distribution and we show how these results apply to cluster-based distributed systems when the competition between the Markov chains is handled by using a geometric distribution.

6.5.5. 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. 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 [53].

6.5.6. Randomized message-passing test-and-set

In [56], 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 $p < n$ of processes in which 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.

6.5.7. Agreement problems in unreliable systems

In [18], we consider the problem of approximate consensus in mobile ad-hoc networks in the presence of Byzantine nodes. Each node begins to participate by providing a real number called its initial value. Eventually all correct nodes must obtain final values that are different from each other within a maximum value previously defined (convergence property) and must be in the range of initial values proposed by the

correct nodes (validity property). Due to nodes' mobility, the topology is dynamic and unpredictable. We propose an approximate Byzantine consensus protocol which is based on the linear iteration method. Each node repeatedly executes rounds. During a round, a node moves to a new location, broadcasts its current value, gathers values from its neighbors, and possibly updates its value. In our protocol, nodes are allowed to collect information during several consecutive rounds: thus moving gives them the opportunity to gather progressively enough values. An integer parameter R_c is used to define the maximal number of rounds during which values can be gathered and stored while waiting to be used. A novel sufficient and necessary condition guarantees the final convergence of the consensus protocol. At each stage of the computation, a single correct node is concerned by the requirement expressed by this new condition (the condition is not universal as it is the case in all previous related works). Moreover the condition considers both the topology and the values proposed by correct nodes. If less than one third of the nodes are faulty, the condition can be satisfied. We are working on mobility scenarios (random trajectories, predefined trajectories, meeting points) to assert that the condition can be satisfied for reasonable values of R_c. In [41], we extend the above protocol to solve the problem of clock synchronization in mobile ad-hoc networks.

In [20], we investigate the use of agreement protocols to develop transactional mobile agents. Mobile devices are now equipped with multiple sensors and networking capabilities. They can gather information about their surrounding environment and interact both with nearby nodes, using a dynamic and self-configurable ad-hoc network, and with distant nodes via the Internet. While the concept of mobile agent is appropriate to explore the ad-hoc network and autonomously discover service providers, it is not suitable for the implementation of strong distributed synchronization mechanisms. Moreover, the termination of a task assigned to an agent may be compromised if the persistence of the agent itself is not ensured. In the case of a transactional mobile agent, we identify two services, Availability of the Sources and Atomic Commit, that can be supplied by more powerful entities located in a cloud. We propose a solution in which these two services are provided in a reliable and homogeneous way. To guarantee reliability, the proposed solution relies on a single agreement protocol that orders continuously all the new actions whatever the related transaction and service.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- **Thales contract (2014): "Capalid v2"**

  This contract consists in validating an intrusion detection strategy in a supervised distributed system. This work relies on the results obtained by Erwan Godefroy in his PhD Thesis: considering the description of an attack and a description of the deployed system (topology, cartography, IDS deployment), we must answer the question: "Is it possible to detect this attack?". This answer consists in determining if it is possible to build a correlation rule that a correlation system can use to detect the attack.

- **CS contract (2014-2015): "SecEF"**

  The COSCOM contract consists in analyzing current used standards for information security events. 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 form current users.

- **Technicolor contract (2011-2014): "Data Aggregation in Large Scale Systems"**

The theme of this contract focuses on the management of massively distributed data sets. In a nutshell, our goal is to provide a lightweight yet continuous flow of aggregate and relevant data from a very large number of distributed sources to a management system. Collaborative data aggregation are relevant mechanisms that could help in securely providing digests of information. However, an important aspect that we want to preserve is the privacy of the aggregated information. This is of particular interest for Telco operators or software/hardware providers in order to smoothly manage the current state of their deployed platforms, allowing accordingly to develop new applications based on quick reactions/optimizations to identify and handle services inconsistencies.

This study is conducted in cooperation with the Inria project Dionysos.

- **HP contract (2013-2014): "Embedded Systems Security"**

  We have initiated a research program in collaboration with HP 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. Details about this research program cannot be provided as they are covered by a non-disclosure agreement.

7.2. Bilateral Grants with Industry

- **Amossys: "Evaluation of intrusion detection mechanisms"**

  The PhD of Georges Bossert is done in the context of a CIFRE contract with the SME Amossys (http://www.amossys.fr/). His work consists in proposing new approaches for protocol reverse-engineering. He developed Netzob, a tool dedicated to this task. The goal is to use this tool to generate realistic traffic during IDS assessment. In 2013, Georges has developed two important improvements of the protocol inference process he previously proposed. First, he improved the message format reverse engineering phase. Unlike previous work, our approach uses contextual information and its semantic definition as a key parameter in both the processes of message clustering and field partitioning. We can also detect complex linear and nonlinear relationships between value, size and offset of message fields using correlation-based filtering. Besides, our multi-step pre-clustering phase reduces the required computation time of the main clustering phase. These results have been presented in an article that is under review. The second aspect of his work consisted in enhancing the grammar inference phase. He proposed a new approach that combines passive and active algorithms to infer protocol grammars. This approach also relies on grammar decompositions. Thus, he decreased inference time by using an action-based sequential decomposition and we took into account background noise by using a parallel decomposition. The PhD defense of Georges Bossert was held in December 2014.

- **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 February 2015, is in the process of writing his PhD manuscript so as to defend it by April 2015.

- **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.

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

  The PhD of Christopher Humphries on visualization is done in the context of a cooperation with DGA-MI. The objective is to propose new visulization mechanisms dedicated to the analysis of security events, for instance for forensic purposes. The CORGI tool presented earlier in this documents is the most recent contribution to this contract.

- **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. 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.

8. Partnerships and Cooperations

8.1. Regional Initiatives

- **Région Bretagne ARED grant:** the PhD of Regina Marin on privacy protection in distributed social networks is 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 outsource 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 researcher 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.

- **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. This implies to propose an approach and to design and implement a mechanism that can handle both OS-level and browser-level information flows.

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 (2013-2016): "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://www.securite.cominlabs.ueb.eu/**

  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 Security project to stem the progression of Android pieces of malware. We propose to combine status 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 aim to imagine and develop a malware scanning service that will permit users to analyze their own applications. This service will be available on a online platform that will also deliver previously computed signatures of known malware.

  Project members are from Celtique and Cidre Inria teams.

8.2. National Initiatives

8.2.1. 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.

- **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 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", in [21], and in several French newspapers. It will be published at the end of 2014 in [15]. During 2014, 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.

- **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.

8.2.2. 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 four 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. The postdoctoral position of Cristina Onete since September 2014 is funded by CAPPRIS.

8.2.3. Research mission "Droit et Justice"

- **Droit à l'oubli (2012-2014)** The "right to be forgotten" can be viewed as a consequence and an extension of the right to privacy and to personal data protection, emphasized by the inherent difficulty to erase any given information from the omnipresent digital world. The French ministry of Justice has launched two twin projects (one of which is the DAO project), in order to explore the possible legal definitions of a "right to be forgotten". Even though there are no legal foundations for such a right in France at the moment, the concept is already known from the general public and is also present in courts. Furthermore, individuals expect to be protected by such a right, thus it is important to understand why, how, in which circumstances and to which extent this new right may apply before envisioning a legal notion defining it. The DAO project involves a major legal component, a sociological survey and a technical study. In a nutshell, the legal part explores the possible boundaries and requirements of a right to be forgotten with respect to labor law, civil statuses, personal data protection, legal prescription and IT law. The sociological survey aims at understanding the root causes making people build a desire for forgetfulness in others. Finally, the objective of the computer science part is to elaborate a state of the art of the techniques that could be used to enforce a right

to be forgotten in practice in the digital world. The expected output of the project as a whole is a detailed recommendation about whether an independent legislation proposal for the right to be forgotten would be justified, and how it should be done. This final report summarizing the thinkings of the project will be published at the end of 2014 or the beginning of 2015. The project is joint between Université de Rennes I, Inria and Supélec.

8.2.4. Competitivity Clusters

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

8.3. European Initiatives

8.3.1. 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),
- Supélec (FR).

This year, our work focused on requirements and design. CIDRE was the WP leader of *WP2 - Deficiency and Requirement Analysis* and was also particularly involved in *WP4 - Data Collection and Correlation*, *WP5 - Dynamic Risk Management* and *WP6 - Visual Analytics and Display*. In WP2, we produce an document presenting the state of the art and current limitations in the fields of security data collection and correlation, mission impact evaluation, threat assessment, automated and semi-automated reaction and visualization and interaction. We also produced an operational requirement analysis. In WP4, we produced a document presenting the system requirements for data collectin and low-level correlation. In WP5, we produced a document presenting the system requirements for risk evaluation and dynamic risk management. In WP6, we produced a document presenting visualization challenges and requirements in the context of PANOPTESEC. More generally, we also contributed to the design and architecture of what will be the PANOPTESEC system.

8.4. International Initiatives

8.4.1. Informal International Partners

Sébastien Gambs is collaborating with Jean-Marc Robert (ETS, Montréal, Canada) on the development of privacy-preserving and secure distance-bounding protocols and with Alain Tapp (Université de Montréal, Montréal, Canada) on the design of cryptographic architectures for privacy. He is also collaborating with Panagiotis Papadimitratos (KTH, Stockholm, Sweden) on privacy for location-based services.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

Jean-Marc Robert

Date: June 2014

Institution: École de Technologie Supérieure (Canada).

8.5.1.1. Internships

Sackmann Mario Julián

Date: Sep 2014 - Jan 2015

Institution: Universidad de Buenos Aires (Argentine)

8.5.2. Visits to International Teams

8.5.2.1. Explorer programme

Sébastien Gambs

Date: May 2014

Institution: Institute of Big Data Analytics, Dalhousie University (Halifax, Canada)

8.5.2.2. Research stays abroad

We built a collaboration with Yvan Labiche of the Carleton University in Ottawa to supervise the PhD thesis of Mouna Hkimi. In the context of this collaboration and thanks to the support of SUPELEC and go the SUPELEC foundation, Eric Totel went in Carleton University for four months from March to June 2014, to work on the subject of the modeling of distributed applications.

In May 2014, Sébastien Gambs visited Stan Matwin at the Institute of Big Data Analytics located at Dalhousie university (Halifax, Canada). This visit has foster the beginning of a collaboration on the privacy-preserving analysis of large scale data. In particular, we have started to develop a novel method for sanitizing CDRs (Call Details Records) dataset based on differentially-private variants of sketches, which has been submitted to the D4D challenge. We will also prepare a submission for an associate Inria team for the 2015 call.

Thanks to the support of SUPELEC, 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.

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).

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. member of the organizing committee

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

- SSTIC 2014 (Symposium sur la Sécurité des Systèmes d'Information et des Réseaux 2014).
- VizSec 2014 (Visualization for Cyber-Security), official workshop of IEEE VIS 2014.

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

- SSTIC 2014 (Symposium sur la Sécurité des Systèmes d'Information et des Réseaux 2014).

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

- C&ESAR 2014 (Computers & Electronics Security Applications Rendez-vous).

9.1.2. Scientific events selection

9.1.2.1. member of the conference program committee

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

- 14th IEEE International Conference on Computer and Information Technology (CIT-2014), 11-13 September 2014
- 13th IEEE International Conference on Ubiquitous Computing and Communications (IUCC-2014), 19-21 December, 2014
- 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). September 24th-26th, 2014.

Sébastien Gambs served as a member of the program committees of the following conferences and workshops:

- 6th IEEE International Workshop on SEcurity and SOCial Networking (SESOC 2014), 28 March 2014, Budapest, Hungary.
- 9ème Conférence sur la Sécurité des Architectures Réseau et des Systèmes d'Information (SAR-SSI 2014), 13-16 May 2014, Saint-Germain-Au-Mont-d'Or, France.
- 10th European Dependable Computing Conference (EDCC 2014), 13-16 May 2014, Newcastle Upon Tyne, UK.
- IEEE ICC 2014 - Communication and Information Systems Security Symposium, 10-14 June 2014, Sydney, Australia.
- 5ème Atelier sur la Protection de la Vie Privée (APVP 2014), 15-18 June 2014, Cabourg, France.
- 12th Annual Conference on Privacy, Security and Trust (PST 2014), 23-24 July 2014, Toronto, Canada.
- IEEE Workshop on Privacy and Anonymity in Digital Economy (PADE 2014), September, Edmonton, Canada.
- 9th DPM International Workshop on Data Privacy Management (DPM 2014), 10 September 2014, Wroclaw, Poland.
- 5th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2014), 22-25 September, Halifax, Canada.
- 15th Joint IFIP TC6 and TC11 Conference on Communications and Multimedia Security (CMS 2014), 25-26 September 2014, Aveiro, Portugal.
- 7th International Symposium on Foundations & Practice of Security (FPS 2014), 3-5 November 2014, Montréal, Canada.

Michel Hurfin was a member of the program committee of

- the 6th IEEE International Symposium on UbiSafe Computing (UbisSafe 2014) in conjunction with the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2014), 24-26 September 2014, Beijing, China. http://trust.csu.edu.cn/conference/ubisafe2014/
- the 12th African Conference on Research in Computer Science and Applied Mathematics (CARI'2014), 16-23 October, 2014, Saint Louis, Senegal. http://www.cari-info.org/
- the 6th International Workshop on Workflow Management in Cloud and Big Data (WMCB 2014) in conjunction with the International Conference on Big Data and Cloud Computing (BDCloud 2014), 3-5 December 2014, Sydney, Australia. http://wmcb2014.sinaapp.com/index.html

J.-F. Lalande served as a member of the program committees of the following conferences and workshops:

- International Conference on Emerging Security Information, Systems and Technologies (IARIA SECURWARE 2014)
- International Conference on High Performance Computing & Simulation (IEEE HPCS 2014)
- International Conference on High Performance and Communications (IEEE HPCC 2014)
- International Workshop on Methods for Establishing Trust with Open Data (IEEE METHOD 2014)
- International Workshop on Security and High Performance Computing Systems (Workshop SHPCS 2014)
- International Workshop on Secure Peer-to-Peer Intelligent Networks & Systems (Workshop SPINS 2014)

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

- SSTIC 2014 (Symposium sur la Sécurité des Systèmes d'Information et des Réseaux 2014).
- VizSec 2014 (Visualization for Cyber-Security), official workshop of IEEE VIS 2014.

Guillaume Piolle served as a member of the program committees of the following conferences and workshops:

- First International Workshop on Agents and CyberSecurity (ACySe 2014). https://sites.google.com/site/acyseaamas2014/home
- 16ème Colloque CREIS-TERMINAL. http://www.lecreis.org/?p=1789
- 9ème Conférence sur la Sécurité des Architectures Réseau et des Systèmes d'Information (SAR-SSI 2014). http://sarssi14.liris.cnrs.fr/

Eric Totel was a member of the program committee of:

- the 6th IEEE International Symposium on UbiSafe Computing (UbisSafe 2014) in conjunction with the 13th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom 2014), 24-26 September 2014, Beijing, China. http://trust.csu.edu.cn/conference/ubisafe2014/

Frédéric Tronel was a member of the program committee of:

- SSTIC 2014 (Symposium sur la Sécurité des Systèmes d'Information et des Réseaux 2014).

Gilles Guette served as a member of the program committees of the following conferences:

- 1st International Conference on Information Systems Security and Privacy (ICISSP-2015), 9-11 February 2015,
- 9ème Conference sur la Sécurité des Architectures Réseaux et des Systèmes d'information (SARSSI 2014), 13-16 mai 2014.

Christophe Bidan was a member of the program committees of the following conferences and workshops:

- the Fourth International Workshop on Information Systems Security Engineering (WISSE 2014), in conjunction with the 26th International Conference on Advanced Information Systems Engineering (CAiSE'14), 17th June 2014, Thessaloniki, Greece. http://gsya.esi.uclm.es/WISSE2014/
- the 10th International Conference on Security and Privacy in Communication Networks (SecureComm2014), September 24–26, 2014 Beijing, China. http://securecomm.org/2014/show/home/

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

- ACNS 2014 (Applied Cryptography and Network Security),
- CARI 2014 (Conférence Africaine sur la recherche en Informatique),
- C&ESAR 2014 (Computers & Electronics Security Applications Rendez-vous),
- SAR-SSI 2014 (Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information),
- WESSI 2014 (Workshop sur l'Enseignement de la Sécurité des Systèmes d'Information).

9.1.2.2. reviewer

- Sébastien Gambs acts as an external reviewer for EDBT 2014, DSN 2014 and PETS 2014.
- Michel Hurfin acts as a reviewer for the following conferences: UbiSafe 2014 and CARI'2014.

9.1.3. Journal

9.1.3.1. member of the editorial board

- Sébastien Gambs is member of the editorial board of the International Journal of Data Mining, Modelling and Management and a member of the editorial board of the International Journal of Privacy and Health Information Management.
- Michel Hurfin belongs to the editorial board of the Springer open access journal of Internet Services and Applications (http://www.springer.com/computer/communications/journal/13174).

9.1.3.2. reviewer

- Emmanuelle Anceaume served as a reviewer for the Journal of Parallel and Distributed Computing and the Transactions on Parallel and Distributed Systems Journal.
- Sébastien Gambs served as reviewer for the following journals: Nature Communications, Pervasive and Mobile Computing, Neurocomputing, IEEE Internet Computing and Journal of Selected Topics in Signal Processing.
- Michel Hurfin acts as a reviewer for the following journals: IEEE Transactions on Computers (TC) and Springer Journal of Internet Services and Applications (JISA).
- Guillaume Piolle acts as a reviewer for the following journals: International Journal of Information Security (IJIS), Interstices.
- Gilles Guette acts as a reviewer for the journal Security and Communication Networks and Sensor Networks Journal.
- Nicolas Prigent acts as a reviewer for the Lavoisier TSI journal and the SAR-SSI 2014 conference.
- Ludovic Mé acts as a reviewer for the following journals: IEEE Transactions on Network and Service Management, and Logical Methods in Computer Science.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Master 2: Emmanuelle Anceaume, responsable du module BIB, 35 h. equiv. TD

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

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

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

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

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

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

Master: Eric Totel, *Dependability*, 3 hours of lecture, M2 - third year of the engineer degree (ingénierie des systèmes automatisés), Supélec, France

Master: Eric Totel, *Intrusion Detection*, 6 hours of lecture, M2 - M2 - mastère spécialisé CS (Cyber Security), Supélec, 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, Supélec, France

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

Licence: Frédéric Tronel, *Software engineering*, 40h30, L3 - first year of the engineer degree, Supélec, France.

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

Master: Frédéric Tronel, *Compilers*, 26h, M2 - third year of the engineer degree, Supélec, France.

Master: Frédéric Tronel, *Automatic reasoning*, 8h, M2 - third year of the engineer degree, Supélec, France.

Master: Frédéric Tronel, *Buffer overflow vulnerabilities (theory and practice)*, 16h30, M2 - third year of the engineer degree, Supélec, France.

Master: Frédéric Tronel, *Buffer overflow vulnerabilities (theory and practice)*, 7h30, M2 - third year of the engineer degree, Telecom Bretagne, France.

Master: Frédéric Tronel, *Firewall*, 7h30, M2 - third year of the engineer degree, Supélec, France.

Master: Frédéric Tronel,*Calculability in distributed systems*, 9h, M2, jointly with University of Rennes 1 and Supélec, France.

Licence: Guillaume Piolle, *Programming models and languages*, 18 hours, L3 - first year of the engineering degree, Supélec, France;

Licence: Guillaume Piolle, *Foundations of computing, data structures and algorithms*, 31.5 hours, L3 - first year of the engineering degree, Supélec, France;

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

Master: Guillaume Piolle, *Modelling, algorithms and programming*, 23.7 hours, M1 - second year of the engineer degree, Supélec, France;

Master: Guillaume Piolle, *Computer security and privacy for the engineer*, 6 hours, M1 - second year of the engineer degree, Supélec, France;

Master: Guillaume Piolle, *Security policies*, 4.5 hours, M2 - third year of the engineering degree, Supélec, France;

Master: Guillaume Piolle, *Network supervision in Java*, 3 hours, M2 - third year of the engineering degree, Supélec, France;

Master: Guillaume Piolle, *Computer networks*, 3 hours, M2 - third year of the engineering degree, Supélec, France;

Master: Guillaume Piolle, *C++/Qt*, 12 hours, M2 - third year of the engineering degree, Supélec, France;

Master: Guillaume Piolle, *Symbolic artificial intelligence*, 4.5 hours, M2 - third year of the engineering degree, Supélec, France;

Master: Guillaume Piolle, *Network access protection*, 6 hours, M2 - third year of the engineering degree, Supélec, France;

Master: Guillaume Piolle, *Web development*, 9 hours, M2 - third year of the engineering degree, Supélec, France;

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

Master: Guillaume Piolle, *Privacy protection*, 2.25 hours, course for computing high school teachers, Académie de Rennes, France;

Master: Guillaume Piolle, *Discovering Tor*, 1.5 hours, course for computing high school teachers, Académie de Rennes, France;

Doctorat: Guillaume Piolle, *Privacy and data protection*, 9 hours, doctoral course, Matisse doctoral school, France;

Licence: Nicolas Prigent, *Models and programming languages*, 19.5 hours including 12 hours of lecture, L3 - first year of the engineer degree, Supélec, France.

Licence: Nicolas Prigent, *Foundations of computer science, data structures and algorithms*, 12 hours, L3 - first year of the engineer degree, Supélec, France.

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

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

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

Master: Nicolas Prigent, *Applied Cryptography*, 4,5 hours, M2 - third year of the engineering degree, Supélec, France;

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

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

Master: Nicolas Prigent, *Penetration Testing*, 12 hours, M2 - third year of the engineering degree, Supélec, 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, Supélec Campus de Rennes, France.

Master: Nicolas Prigent, *MS Windows Configuration and Administration*, 8 hours, CQP - Specialization year, Supélec Campus de Gif, France.

Master: Nicolas Prigent, *Cryptography, Cryptographic Protocols and Applications*, 16 hours, CQP - Specialization year, Supélec Campus de Gif, France.

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

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

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

Master: Gilles Guette, *Infrastructure Network*, 22 hours, M2 - third year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Network Security*, 18 hours, M2 - third year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Network and System Security*, 15 hours, M2 - third year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Network Dimensionning*, 6 hours, M2 - third year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Network Administration*, 50 hours, second year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Mobile Network*, 5 hours, second year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Network Routing*, 35 hours, second year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Supervision of student Project*, 3 projects, third year of the engineer degree, ESIR, France;

Master: Gilles Guette, *Supervision of student Project*, 2 projects, second year of the engineer degree, ESIR, France;

Master: Jean-Francois Lalande, *Programmation orientée objet avancée: Java*, 16 hours, M2 - third year of the engineer degree, INSA Centre Val de Loire, France;

Master: Jean-Francois Lalande, *Atelier Sécurité Android*, 2 days, master degree students of ENSA de Kénitra (conférence CISSI 2014) and ENSA de Khouribga (conférence CISTIC 2014), Maroc;

Licence: Christophe Bidan, *Programming models and languages*, 18 hours, L3 - first year of the engineering degree, Supélec, France;

Licence: Christophe Bidan, *Network and Operating Systems*, 6 hours, L3 - second year of the engineering degree, Supélec, France;

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

Master: Valérie Viet Triem Tong, *Games Theory*, 18 hours, M1 - second year of the engineering degree, Supélec, France;

Master: Valérie Viet Triem Tong, *Certified Programming using Coq*, 9 hours, M2 - third year of the engineering degree, Supélec, France;

Master: Valérie Viet Triem Tong, *Intrusion detection using information flow control*, 9 hours, M2 / third yearof the engineering degree, Supélec, France;

Master: Valérie Viet Triem Tong, *Small elements of decidability*, 7h30 hours, M2 - third year of the engineering degree, Supélec, France;

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

Master: Ludovic Mé, *Introduction to Computer Security and Privacy*, 6.75 hours, M1 - second year of the engineer degree, Supélec, France

Master: Ludovic Mé, *Information systems*, 6 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 - third year of the engineer degree, Supélec, France

Master: Ludovic Mé is responsible for the module “Secured information systems”, M2 - third year of the engineer degree, Supélec, France

Licence: Guillaume Hiet, *Models and programming languages*, 11 hours, L3 - first year of the engineer degree, Supe´lec, France

Licence: Guillaume Hiet, *Foundations of computer science, data structures and algorithms*, 15 hours, L3 - first year of the engineer degree, Supe´lec, France

Master: Guillaume Hiet, *Computer security and privacy for the engineer*, 10 hours including 4,5 hours of lecture, M1 - second year of the engineer degree, Supe´lec, France

Master: Guillaume Hiet, *Buffer overflow vulnerabilities*, lab work (16h), M2 - third year of the engineer degree, Supélec.

Master: Guillaume Hiet, *Pentest*, lab work (9h00), M2 - third year of the engineer degree, Supélec, France

Master: Guillaume Hiet, *Introduction to Linux*, lab work (3h), M2 - mastère CS (Cyber Security), Supélec, France

Master: Guillaume Hiet, *Java Security*, lecture (3h), M2 - mastère CS, Supélec, France

Master: Guillaume Hiet, *Linux Security*, lab work (6h), M2 - mastère CS , Supélec, France

Master: Guillaume Hiet, *Linux Security*, lecture (3h) and lab work (3h), third year of the engineer degree, Supélec, France

Master: Guillaume Hiet, *Intrusion Detection*, lecture (6h) and lab work (6h), M2 - mastère CS, Supélec, France

Master: Guillaume Hiet, *Intrusion Detection*, lecture (3h) and lab work (6h), M2 - third year of the engineer degree, M2 research degree of University of Rennes 1, Supélec

Master: Guillaume Hiet, *Intrusion Detection*, lecture (8h) and lab work (12h), M2, University of Rennes 1, France

Master: Guillaume Hiet, *Intrusion Detection*, lecture (4h) and lab work (6h), M2 - third year of the engineer degree, ESIR, France

Master: Guillaume Hiet, *Intrusion Detection*, 6 hours of lecture, M2, Université de Limoges, France

Master: Guillaume Hiet, *Firewall*, lecture (4h), M2, University of Rennes 1, France

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

Master: Guillaume Hiet, *Supervision of student project*, 1 project, M2 - third year of the engineer degree, Supélec, France

9.2.2. Supervision

HdR: Sébastien Gambs, Protection de la vie privée dans la Société de l’Information, Université de Rennes 1, 23 June 2014.

PhD: Romaric Ludinard, Caractérisation locale de fautes dans les systèmes large échelle, Université Rennes I, Defense: 02/10/2014, Emmanuelle Anceaume and Bruno Sericola

PhD: Radoniaina Andriatsimandefitra, Caractérisation et détection de malware Android basées sur les flux d’information, SUPELEC, Defense: 15/12/2014, Valérie Viet Triem Tong and Ludovic Mé.

PhD: Georges Bossert, Exploiting Semantic for the Automatic Reverse Engineering of Communication Protocols, SUPELEC, Defense: 17/12/2014, Guillaume Hiet and Ludovic Mé.

PhD in progress: Mounir Assaf, “Calcul de propriétés dans des programmes C de grande taille”, supervised by Eric Totel (50%) and Frederic Tronel (50%);

PhD in progress: Laurent Georget, “Formal validation of an information flow monitor”, started in October 2014, supervised by Valérie Viet Triem Tong (25%), Frédéric Tronel (25%), Guillaume Piolle (25%) and Mathieu Jaume (25%);

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: Paul Lajoie-Mazenc, “Privacy preserving reputation system in large scale and self organizing systems”, started in october 2012, supervised by Emmanuelle Anceaume (50%) and Valérie Viet Triem Tong (50%);

PhD in progress: Pierre Obame, “Dependability issues in large scale systems”, started in February 2012, supervised by Emmanuelle Anceaume (50%) and Frédéric Tronel (50%);

PhD in progress: Regina Paiva Melo Marin, “Privacy protection in distributed social networks”, started in November 2011, supervised by Christophe Bidan (20%) and Guillaume Piolle (80%).

PhD in progress: Simon Boche, “Réputation et respect de la vie privée dans les réseaux auto-organisé”, started in September 2012, supervised by Christophe Bidan (30%), Gilles Guette (35%) and Nicolas Prigent (35%);

PhD in progress: Florian Grandhomme, “Études 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 (25%), Gilles Guette (50%) and Thierry Pless (25%);

PhD in progress: Christopher Humphries, “Visualisation d’évènements de sécurité", started in December 2011, supervised by Christophe Bidan (20%) and Nicolas Prigent (80%).

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

PhD in progress: 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: Antoine Guellier, “Utilisation de la cryptographie homomorphe pour garantir le respect de la vie privée", started in October 2013, supervised by Christophe Bidan (50%) and Nicolas Prigent (50%).

Some members of the team also participate to the supervision of external PhD students. Sébastien Gambs is co-supervising Raghavendran Balu (PhD student for LinkMedia, Inria Rennes) and Moussa Traore (PhD student from LAAS-CNRS, Toulouse).

9.2.3. Juries

- Emmanuelle Anceaume was a member of the PhD committee for the PhD of Nagham Alhadad entitled "Bridging the gap between social and digital worlds: system modeling and trust evaluation", prepared at LINA, Nantes, June 20th 2014.
- Michel Hurfin was a member of the PhD committee (reviewer) for the PhD of Linda Zeghache entitled ’Tolérance aux pannes dans les systèmes d’agents mobiles transactionnels’, prepared at Université des sciences et de la Technologie Houari Boumediene (USTHB), Algeria, April 27th 2014.
- Jean-François Lalande was a member of the PhD committee for the PhD of Nicolas Moro entitled "Sécurisation de programmes assembleur face aux attaques visant les processeurs embarqués", prepared at Université Pierre et Marie Curie, Paris, November 13rd 2014.

- Eric Totel was a member of the PhD committee (reviewer) for the PhD of Aurélien Wailly entitled "Architecture de bout en bout et mécanismes d'autoprotection pour les environnements Cloud", prepared at Telecom Sud Paris, Paris, September 30th 2014.
- Christophe Bidan was a member of the PhD committee (reviewer) for the PhD of Nesrine Kaaniche entitled "Cloud Data Storage Security based on Cryptographic Mechanisms", prepared at Telecom Sud Paris, Paris, December 15th 2014.
- Christophe Bidan was a member of the HDR committee (examiner) for the HDR of Julien Iguchi-Cartigny entitled "Contributions à la sécurité des Java Card", prepared at Université de Limoges, Limoges, December 4th, 2014.
- Sébastien Gambs was a member of the jury of the Gilles Kahn PhD award for 2014. This award is given each to the best French PhD thesis in computer science.
- Ludovic Mé was a member of the PhD committee (president) for the PhD of Romaric Ludinard entitled "Caractérisation locale de fautes dans les systèmes large échelle", prepared at Université de Rennes 1, Rennes, October 2nd 2014.
- Eric Totel was a member of the mid-term evaluation committee of Vincent Laporte (PhD student of the university of Rennes), July 2014.
- Ludovic Mé was a member of the mid-term evaluation committee of Florent Marchand de Kerchove (PhD student of the university of Nantes), June 2014.
- Emmanuelle Anceaume was a member of the mid-term evaluation committee of Nicolo Rivetti (PhD student of the university of Nantes), June 2014.
- Sébastien Gambs was a member of the mid-term evaluation committee of George Nassopoulos (PhD student of the university of Nantes), June 2014.
- Michel Hurfin was a member of the mid-term evaluation committee of Ghada Arfaoui (PhD student of the university of Orléans, Cifre Orange Labs), January 2014.
- Christophe Bidan was a member of the mid-term evaluation committee of Mickaël Salaun (PhD student of Telecom Sud Paris), March 2014.
- Christophe Bidan was a member of the mid-term evaluation committee of Malek Belhaouane (PhD student of Telecom Sud Paris), March 2014.

9.3. 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 ;
- *A la découverte de la recherche* : local program aimed at providing high school pupils with insights of research issues and activities.

Nicolas Prigent made a Tutorial Presentation at OSSIR Bretagne dealing with Visualization for Security.

Sébastien Gambs has participated to the event “A la découverte de le recherche”, in which he did five presentations in high school in order to raise the awareness of teenagers on privacy issues related to information technologies and to explain them the research on this topic.

10. 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^{o} 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^{o} 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^{o} 1

[8] G. PIOLLE, Y. DEMAZEAU. *Representing privacy regulations with deontico-temporal operators*, in "Web Intelligence and Agent Systems", Jul 2011, vol. 9, n^{o} 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] R. ANDRIATSIMANDEFITRA. *Characterization and detection of android malware based on information flows*, Supélec, December 2014, https://hal.inria.fr/tel-01095994

Articles in International Peer-Reviewed Journals

[12] E. ANCEAUME, Y. BUSNEL. *A Distributed Information Divergence Estimation over Data Streams*, in "IEEE Transactions on Parallel and Distributed Systems", February 2014, vol. 25, n^{o} 2, pp. 478-487 [*DOI :* 10.1109/TPDS.2013.101], https://hal.archives-ouvertes.fr/hal-00998708

[13] E. ANCEAUME, F. CASTELLA, B. SERICOLA. *Analysis of a large number of Markov chains competing for transitions*, in "International Journal of Systems Science", March 2014, vol. 45, n° 3, pp. 232–240 [*DOI :* 10.1080/00207721.2012.704090], https://hal.archives-ouvertes.fr/hal-00736916

[14] R. ANDRIATSIMANDEFITRA, V. VIET TRIEM TONG. *Information Flow Policies vs Malware – Final Battle –*, in "Journal of Information Assurance and Security", 2014, vol. 9, n° 2, pp. 72-82, https://hal.inria.fr/hal-01062313

[15] G. ARFAOUI, G. DABOSVILLE, S. GAMBS, P. LACHARME, J.-F. LALANDE. *A Privacy-Preserving NFC Mobile Pass for Transport Systems*, in "EAI Endorsed Transactions on Mobile Communications and Applications", December 2014, vol. 2, n° 5, pp. 1-18 [*DOI :* 10.4108/MCA.2.5.E4], https://hal.inria.fr/hal-01091576

[16] J. FRIGINAL, S. GAMBS, J. GUIOCHET, M.-O. KILLIJIAN. *Towards privacy-driven design of a dynamic carpooling system*, in "Pervasive and Mobile Computing", October 2014, vol. 14, 11 p. [*DOI :* 10.1016/J.PMCJ.2014.05.009], https://hal.inria.fr/hal-01089918

[17] S. GAMBS, M.-O. KILLIJIAN, M. NUNEZ DEL PRADO CORTEZ. *De-anonymization attack on geolocated data*, in "Journal of Computer and System Sciences", December 2014, vol. 80, n° 8, 17 p. [*DOI :* 10.1016/J.JCSS.2014.04.024], https://hal.inria.fr/hal-01089883

[18] C. LI, M. HURFIN, Y. WANG. *Approximate Byzantine consensus in sparse, mobile ad-hoc networks*, in "Journal of Parallel and Distributed Computing", September 2014, vol. 74, n° 9, 12 p. [*DOI :* 10.1016/J.JPDC.2014.05.005], https://hal.inria.fr/hal-01083553

[19] R. LUDINARD, E. TOTEL, F. TRONEL, V. NICOMETTE, M. KAÂNICHE, É. ALATA, R. AKROUT, Y. BACHY. *An Invariant-based Approach for Detecting Attacks against Data in Web Applications*, in "International Journal of Secure Software Engineering", June 2014, vol. 5, n° 1, pp. 19-38 [*DOI :* 10.4018/IJSSE.2014010102], https://hal.inria.fr/hal-01083296

[20] L. ZEGHACHE, N. BADACHE, M. HURFIN, I. MOISE. *Reliable mobile agents with transactional behaviour*, in "International Journal of Communication Networks and Distributed Systems", 2014, vol. 13, n° 1, 27 p. [*DOI :* 10.1504/IJCNDS.2014.063977], https://hal.inria.fr/hal-01083544

Invited Conferences

[21] J.-F. LALANDE. *Un titre de transport sur mobile NFC respectueux de la vie privée*, in "Colloque International sur la Sécurité des Systèmes d'Information", Kénitra, Morocco, March 2014, https://hal.inria.fr/hal-00967463

International Conferences with Proceedings

[22] E. ANCEAUME, Y. BUSNEL. *Deviation Estimation between Distributed Data Streams*, in "10th European Dependable Computing Conference (EDCC 2014)", Newcastle, United Kingdom, May 2014, pp. 35-45 [*DOI :* 10.1109/EDCC.2014.27], https://hal.archives-ouvertes.fr/hal-00998702

[23] E. ANCEAUME, Y. BUSNEL, E. LE MERRER, R. LUDINARD, J.-L. MARCHAND, B. SERICOLA. *Anomaly Characterization in Large Scale Networks*, in "44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)", Atlanta, United States, June 2014, https://hal.inria.fr/hal-00948135

[24] E. ANCEAUME, Y. BUSNEL, B. SERICOLA. *Service d'échantillonage uniforme résiliant aux comportments malveillants*, in "ALGOTEL 2014 – 16èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", France, June 2014, pp. 1–4, https://hal.archives-ouvertes.fr/hal-00985631

[25] R. ANDRIATSIMANDEFITRA, V. VIET TRIEM TONG. *Capturing Android Malware Behaviour using System Flow Graph*, in "NSS 2014 - The 8th International Conference on Network and System Security", Xi'an, China, October 2014, https://hal.inria.fr/hal-01018611

[26] D. AUGOT, P.-A. FOUQUE, P. KARPMAN. *Diffusion Matrices from Algebraic-Geometry Codes with Efficient SIMD Implementation*, in "Selected Areas in Cryptology", Montreal, Canada, A. JOUX, A. YOUSSEF (editors), Selected Areas in Cryptology - SAC 2014, Springer, August 2014, vol. LNCS 8781, pp. 243-260 [*DOI :* 10.1007/978-3-319-13051-4_15], https://hal.inria.fr/hal-01094085

[27] *Best Paper*
R. BALU, T. FURON, S. GAMBS. *Challenging differential privacy: the case of non-interactive mechanisms*, in "European Symposium on Research in Computer Security", Wroclaw, Poland, LNCS, Springer-Verlag, September 2014, vol. 8657, Best Student Paper Award [*DOI :* 10.1007/978-3-319-11212-1_9], https://hal.inria.fr/hal-01011346.

[28] G. BOSSERT, F. GUIHÉRY, G. HIET. *Towards Automated Protocol Reverse Engineering Using Semantic Information*, in "ASIA CCS '14", Kyoto, Japan, June 2014, pp. 51-62, 12 pages [*DOI :* 10.1145/2590296.2590346], https://hal-supelec.archives-ouvertes.fr/hal-01009283

[29] M. DE SAINT LÉGER, S. GAMBS, B. JUANALS, J.-F. LALANDE, J.-L. MINEL. *Privacy and Mobile Technologies: the Need to Build a Digital Culture*, in "Digital Intelligence 2014", Nantes, France, September 2014, pp. 100-105, https://halshs.archives-ouvertes.fr/halshs-01065840

[30] C. FONTAINE, S. GAMBS, J. LOLIVE, C. ONETE. *Private asymmetric fingerprinting : a protocol with optimal traitor tracing using Tardos codes*, in "Third International Conference on Cryptology and Information Security in Latin America (Latincrypt'14)", Florianopolis, Brazil, September 2014, https://hal.inria.fr/hal-01090053

[31] P.-A. FOUQUE, A. JOUX, C. MAVROMATI. *Multi-user collisions: Applications to Discrete Logarithm, Even-Mansour and PRINCE (Full version *)*, in "Advances in Cryptology - ASIACRYPT 2014 - 20th International Conference on the Theory and Application of Cryptology and Information Security", Kaoshiung, Taiwan, Springer, December 2014, vol. LNCS 8873, 20 p. , https://hal.inria.fr/hal-01094051

[32] S. GAMBS, M.-O. KILLIJIAN, C. LAURADOUX, C. ONETE, M. ROY, M. TRAORÉ. *VSSDB: A Verifiable Secret-Sharing and Distance-Bounding protocol*, in "International Conference on Cryptography and Information security (BalkanCryptSec'14)", Istanbul, Turkey, October 2014, https://hal.inria.fr/hal-01090056

[33] S. GAMBS, C. ONETE, J.-M. ROBERT. *Prover anonymous and deniable distance-bounding authentication*, in "ASIACCS'14", Kyoto, Japan, Proceedings of the 9th ACM symposium on Information, computer and communications security (ASIACCS'14), June 2014 [*DOI :* 10.1145/2590296.2590331], https://hal.inria.fr/hal-01089793

[34] S. GAMBS, S. RANELLUCCI, A. TAPP. *The crypto-democracy and the Trustworthy*, in "Data Privacy Management (DPM'14)", Wroclaw, Poland, September 2014, https://hal.inria.fr/hal-01090047

[35] S. GAMBS, M. TRAORÉ, M. ROY, M.-O. KILLIJIAN. *PROPS : A PRivacy-preserving lOcation Proof System*, in "33rd IEEE Symposium on Reliable Distributed Systems (SRDS'14)", Nara, Japan, October 2014, https://hal.inria.fr/hal-01090049

[36] E. GODEFROY, E. TOTEL, M. HURFIN, F. MAJORCZYK. *Automatic Generation of Correlation Rules to Detect Complex Attack Scenarios*, in "2014 International Conference on Information Assurance and Security (IAS 2014)", Okinawa, Japan, IEEE, November 2014, 6 p. , https://hal.inria.fr/hal-01091385

[37] A. GUELLIER, C. BIDAN, N. PRIGENT. *Homomorphic Cryptography-based Privacy-Preserving Network Communications*, in "Applications and Techniques in Information Security", Deakin University, Melbourne, VIC, Australia, France, L. BATTEN, G. LI, W. NIU, M. WARREN (editors), Communications in Computer and Information Science, Springer Berlin Heidelberg, November 2014, vol. 490, pp. 159-170 [*DOI :* 10.1007/978-3-662-45670-5_15], https://hal.inria.fr/hal-01088441

[38] C. HUMPHRIES, N. PRIGENT, C. BIDAN, F. MAJORCZYK. *Catégorisation par objectifs de la visualisation pour la sécurité*, in "CESAR", Rennes, France, November 2014, https://hal.inria.fr/hal-01096337

[39] C. HUMPHRIES, N. PRIGENT, C. BIDAN, F. MAJORCZYK. *CORGI: Combination, Organization and Reconstruction through Graphical Interactions*, in "VizSec", Paris, France, November 2014 [*DOI :* 10.1145/2671491.2671494], https://hal.inria.fr/hal-01096331

[40] J.-F. LALANDE, K. HEYDEMANN, P. BERTHOMÉ. *Software countermeasures for control flow integrity of smart card C codes*, in "ESORICS - 19th European Symposium on Research in Computer Security", Wroclaw, Poland, M. KUTYŁOWSKI, J. VAIDYA (editors), LNCS, Springer International Publishing, September 2014, vol. 8713, pp. 200-218 [*DOI :* 10.1007/978-3-319-11212-1_12], https://hal.inria.fr/hal-01059201

[41] C. LI, Y. WANG, M. HURFIN. *Clock Synchronization in Mobile Ad Hoc Networks Based on an Iterative Approximate Byzantine Consensus Protocol*, in "28th IEEE International Conference on Advanced Information Networking and Applications (AINA 2014)", Victoria, Canada, May 2014, 8 p. [*DOI :* 10.1109/AINA.2014.30], https://hal.inria.fr/hal-01083573

[42] R. LUDINARD, E. ANCEAUME, Y. BUSNEL, E. LE MERRER, J.-L. MARCHAND, B. SERICOLA, G. STRAUB. *Anomaly Characterization Problems*, in "ALGOTEL 2014 – 16èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications", France, June 2014, pp. 1–4, https://hal.archives-ouvertes.fr/hal-00985641

[43] P. MEYE, P. RAIPIN, F. TRONEL, E. ANCEAUME. *A secure two-phase data deduplication scheme*, in "6th International Symposium on Cyberspace Safety and Security (CSS)", Paris, France, August 2014, https://hal.archives-ouvertes.fr/hal-01076918

[44] P. MEYE, P. RAIPIN, F. TRONEL, E. ANCEAUME. *Mistore: A distributed storage system leveraging the DSL infrastructure of an ISP*, in "HPCS - International Conference on High Performance Computing & Simulation", Bologne, Italy, July 2014, pp. 260 - 267 [*DOI :* 10.1109/HPCSIM.2014.6903694], https://hal.archives-ouvertes.fr/hal-01076907

[45] P. MEYE, P. RAÏPIN-PARVÉDY, F. TRONEL, E. ANCEAUME. *Toward a distributed storage system leveraging the DSL infrastructure of an ISP*, in "11th IEEE Consumer Communications and Networking Conference", United States, January 2014, 2 p. , https://hal.archives-ouvertes.fr/hal-00924051

[46] R. PAIVA MELO MARIN, G. PIOLLE, C. BIDAN. *Equity-preserving Management of Privacy Conflicts in Social Network Systems*, in "PASSAT 2014", Cambridge, United States, Academy of Science and Engineering, December 2014, https://hal-supelec.archives-ouvertes.fr/hal-01090668

National Conferences with Proceedings

[47] E. GODEFROY, E. TOTEL, M. HURFIN, F. MAJORCZYK, A. MAAROUFI. *Automatiser la construction de règles de corrélation : prérequis et processus*, in "C&ESAR 2014 - Détection et réaction face aux attaques informatiques", Rennes, France, November 2014, 9 p. , https://hal.inria.fr/hal-01091327

Conferences without Proceedings

[48] G. ARFAOUI, G. DABOSVILLE, S. GAMBS, P. LACHARME, J.-F. LALANDE. *Un pass de transport anonyme et intraçable pour mobile NFC*, in "Atelier sur la Protection de la Vie Privée 2014", Cabourg, France, June 2014, https://hal.inria.fr/hal-01009516

[49] G. ARFAOUI, J.-F. LALANDE. *A Privacy Preserving Post-Payment Mobile Ticketing Protocol for Transport Systems*, in "Atelier sur la Protection de la Vie Privée 2014", Cabourg, France, June 2014, https://hal.inria.fr/hal-01091597

[50] E. GODEFROY, E. TOTEL, F. MAJORCZYK, M. HURFIN. *Génération automatique de règles de corrélation pour la détection d'attaques complexes*, in "9eme conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SAR-SSI)", Lyon, France, May 2014, 10 p. , https://hal.inria.fr/hal-01083699

Scientific Books (or Scientific Book chapters)

[51] E. ANCEAUME, G. GUETTE, P. LAJOIE-MAZENC, T. SIRVENT, V. VIET TRIEM TONG. *Extending Signatures of Reputation*, in "Privacy and Identity Management for Emerging Services and Technologies", M. HANSEN, J.-H. HOEPMAN, R. LEENES, D. WHITEHOUSE (editors), IFIP Advances in Information and Communication. Vol. 421, Springer, 2014, pp. 165-176, 8th IFIP WG 9.2, 9.5, 9.6/11.7, 11.4, 11.6 International Summer School, Nijmegen, The Netherlands, June 17-21, 2013 [*DOI :* 10.1007/978-3-642-55137-6_13], https://hal.archives-ouvertes.fr/hal-00997133

[52] F. CUPPENS, C. GARION, G. PIOLLE, N. CUPPENS-BOULAHIA. *Normes et logique déontique*, in "Panorama de l'Intelligence Artificielle : Volume 1. Représentation des connaissances et formalisation des raisonnements", P. MARQUIS, O. PAPINI, H. PRADE (editors), Cépaduès Editions, 2014, pp. 215-237, ISBN : 9782364930414, https://hal.inria.fr/hal-00997137

Research Reports

[53] E. ANCEAUME, Y. BUSNEL, B. SERICOLA. *New results on a generalized coupon collector problem using Markov chains*, February 2014, 14 pages, https://hal.archives-ouvertes.fr/hal-00950161

[54] A. GUELLIER. *Can Homomorphic Cryptography ensure Privacy?*, Inria ; IRISA ; Supélec Rennes, équipe Cidre ; Université de Rennes 1, October 2014, n^{o} RR-8568, 109 p. , https://hal.inria.fr/hal-01052509

Other Publications

[55] E. ANCEAUME, Y. BUSNEL, B. SERICOLA. *New results on a generalized coupon collector problem using Markov chains*, June 2014, Preliminary version of the paper to appear in JAP (Journal of Applied Probability), https://hal.archives-ouvertes.fr/hal-01005333

[56] E. ANCEAUME, F. CASTELLA, A. MOSTÉFAOUI, B. SERICOLA. *Randomized Message-Passing Test-and-Set*, October 2014, https://hal.archives-ouvertes.fr/hal-01075650

[57] R. ANDRIATSIMANDEFITRA, V. VIET TRIEM TONG. *Highlighting Easily How Malicious Applications Corrupt Android Devices*, September 2014, Research in Attacks, Intrusions, and Defenses, https://hal.inria.fr/hal-01083376

[58] 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, https://hal.archives-ouvertes.fr/hal-01104837

References in notes

[59] 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.inria.fr/hal-00736918

[60] 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

[61] T. DEMONGEOT, E. TOTEL, V. VIET TRIEM TONG, Y. LE TRAON. *User Data Confidentiality in an Orchestration of Web Services*, in "International Journal of Information Assurance and Security", 2012, vol. 7, http://hal.inria.fr/hal-00735996

[62] 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

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

[64] G. PIOLLE, Y. DEMAZEAU. *Obligations with deadlines and maintained interdictions in privacy regulation frameworks*, in "Proc. of the 8th IEEE/WIC/ACM International Conference on Intelligent Agent Technology (IAT'08)", Sidney, Australia, December 2008, pp. 162–168

[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