IN PARTNERSHIP WITH:
SUPELEC (Rennes)

Activity Report 2011

Project-Team CIDRE

Confidentialité, Intégrité, Disponibilité et Répartition

RESEARCH CENTER
Rennes - Bretagne-Atlantique

THEME
Distributed Systems and Services

Table of contents

Project-Team CIDRE

Keywords: Security, Privacy, Error Detection And Correction, Distributed System, Peer-to-Peer

CIDRE is a joint team between the INRIA research center of Rennes - Bretagne Atlantique and Supélec.

1. Members

Research Scientist

Michel Hurfin [Junior Researcher INRIA, HdR]

Faculty Members

Ludovic Mé [Team leader, Professor Supélec, HdR]
Christophe Bidan [Professor Supélec, HdR]
Sébastien Gambs [Associate Professor Université de Rennes 1, INRIA research chair in Security of Information Systems]
Guillaume Hiet [Associate Professor Supélec]
Guillaume Piolle [Associate Professor Supélec]
Nicolas Prigent [Associate Professor Supélec]
Eric Totel [Associate Professor Supélec]
Frédéric Tronel [Associate Professor Supélec]
Valérie Viet Triem Tong [Associate Professor Supélec]
Frédéric Majorczyk [ATER université de Rennes 1, until August 2011]

Technical Staff

Julien Lolive [Engineer INRIA since November 2011]

PhD Students

Mohamed Ali Ayachi [PhD Student, université de Rennes 1, until February 2011]
Jean-Marie Borello [PhD Student, université de Rennes 1, until April 2011]
Jonathan Christopher Demay [PhD Student, Supélec, until July 2011]
Izabela Moise [PhD Student, université de Rennes 1]
Radoniaina Andriatsimandefitra [PhD Student, université de Rennes 1, since October 2011]
Mounir Assaf [PhD Student, université de Rennes 1, since November 2011]
Georges Bossert [PhD Student, Supélec, Cifre Amossys]
Thomas Demongeot [PhD Student, Télécom Bretagne]
Olivier Ferrand [PhD Student, université de Rennes 1, DCNS Toulon, since June 2011]
Stéphane Geller [PhD Student, Supélec, DGA Grant]
Ahmed Gmati [PhD Student, université de Rennes 1]
Geoffroy Guéguen [PhD Student, université de Rennes 1, ESIEA Laval, since March 2011]
Christophe Hauser [PhD Student, Supélec, MENRT]
Christopher Humphries [PhD Student, université de Rennes 1, Inria/DGA, since December 2011]
Regina Marin [PhD Student, université de Rennes 1, ARED, since November 2011]

Visiting Scientists

Frédéric Massicotte [Junior Researcher Communications Research Centre Canada, March 2011]
Linda Zeghache [PhD Student, USTBH-CEDRIC université des Sciences et de la Technologie Houari Boumédiène, Algeria, June 2011]
Ai Thanh Ho [PhD Student, université de Montréal, Canada, November 2011]
Chuanyou Li [PhD Student, Southeast university, Nanjing, China, since December 2011]

Administrative Assistants

Lydie Mabil [Administrative Assistant, INRIA, until November 2011]
Loic Lesage [Administrative Assistant, INRIA, since November 2011]

2. Overall Objectives

2.1. Overall Objectives

For many aspects of our everyday life, we rely heavily on informations 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., 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 in a complementary manner both the concerns of accidental and intentional failures. The second main characteristic of the CIDre group lies in the scope of the systems it considers. Indeed, during our research, we will consider three complementary levels of study: the Node Level, the Group Level, and the Open Network Level:

- 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.
- 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.
- 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 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, i.e., trust, intrusion detection, and privacy, and on the different 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 to rely 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 aimed at detecting, by analyzing data flows, whether violations of the security policies have occurred. Finally, Privacy Protection which is now recognized as a basic user right, should be respected despite the presence of tools that continuously observe or even control users actions or behaviors.

3. Scientific Foundations

3.1. Introduction

For many aspects of our everyday life, we rely heavily on informations 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 [50], 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 in a complementary manner both the concerns of accidental and intentional failures.

The second main characteristic of the CIDRE group lies in the scope of the systems it considers. Indeed, during our research, we will consider three complementary levels of study: the Node Level, the Group Level, and the Open Network Level:

- 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.
- 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.

- 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 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, i.e., trust, intrusion detection, and privacy, and on the different 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 to rely 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 aimed at detecting, by analyzing data flows, whether violations of the security policies have occurred. Finally, Privacy Protection which is now recognized as a basic user right, should be respected despite the presence of tools 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 the preventive security mechanisms and violate the security policy of the whole system. The goal of intrusion detection systems (IDS) is to be able 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, i.e. the anomaly approach, which consists in detecting a deviation from a referenced behavior. Specifically, we propose to study two complementary methods:

- Illegal Flow Detection: This first method intends to detect information flows that violate the security policy [53], [46]. 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 [45], [52]. 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.

In both 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 first two levels. Moreover, we plan to work on intrusion detection system evaluation methods. For that research, we set a priori aside no particular IDS approach or technique. Here are some concrete examples of our research goals (both short term and long term objectives) in the intrusion detection field:

- at node level, we are going to 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 plan to extend this method to build anti-viruses and DBMS tools by determining viruses signatures.
- at the set of nodes level, we are going to 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, one of the challenges is to enforce the collaboration and consistency at nodes and set of nodes levels to obtain a global intrusion detection mechanism. Regarding the data corruption detection approach, the 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. In forthcoming years, 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, problematics 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). 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. In the CIDRE project, we will investigate PETs that operate at the three different levels (node, set of nodes or open distributed system) and 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 where privacy and utility aspects collide and that will be studied within the context of CIDRE include: identity and privacy, geo-privacy, distributed computing and privacy, privacy-preserving data mining and privacy issues in social networks. Here are some concrete examples of our research goals in the privacy field:

- at the node level, we aim at designing privacy preserving identification scheme, automated reasoning on privacy policies [51], and policy-based adaptive PETs.
- at the set of nodes level, we plan to augment distributed algorithms (i.e., consensus) with privacy properties such as anonymity, unlinkability, and unobservability.
- at the open distributed system level, we plan to target both geo-privacy concerns (that typically occur in geolocalized systems) and privacy issues in social networks. In the former case, we will adopt a sanitization approach while in the latter one we plan to define privacy policies at user level, and their enforcement by all the intervening actors (e.g, at the social network sites providers).

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) that implement 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 in order to strengthen each node's TCB. Accordingly, the CIDRE group proposes to study 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. By way of examples of our research goals regarding the trust management field, we briefly list some of our short and long term objectives at node, group and open networks levels:

1. at node level, we are going to 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 plan to 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 are going to 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 oblivion (i.e., the right to data erasure).

4. Application Domains

4.1. Application Domains

With the infiltration of computers and software in almost all aspects of our modern life, security can nowadays be seen as an absolutely general concern. As such, the results of the research targeted by CIDRE apply to a wide range of domains. It is clear that critical systems, were security (and safety) is a major concern, may 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 services, social networks, etc.) can also benefit from results obtained by CIDRE, especially relatively to privacy. Systems are getting more and more complex, decentralized, distributed, or spontaneous. The emergence of cloud computing brings many challenges that could benefit from ideas, approaches and solutions studied by CIDRE in the context of distributed systems.

5. Software

5.1. Intrusion Detection

Members of Supélec have developed several intrusion detectors.

Blare implements our approach of illegal information flow detection at the OS level. This implementation is a modification of a standard Linux kernel and it monitors information flows between typical OS containers as files, sockets or IPC. System active entities are processes viewed as black-boxes as we only observe their inputs and outputs. Detection at the OS level is in some cases too coarse-grained to avoid the generation of false positives and to detect attacks targeting the application logic. Even if it remains convenient to define the security policy at the OS-level, sound illegal information flow detection implies an additional detection at the language level. This has led us to implement a detector for Java applications, JBlare, to complement the detection at the OS level. JBlare extends the OS-level one by refining the observation of information flows at the language level.

GNG is an intrusion detection system that correlates different sources (such as different logs) in order to identify attacks against the system. The attack scenarios are defined using the Attack Description Langage (ADeLe) proposed by our team, and are internally translated to attack recognition automatons. GNG intends to define time efficient algorithms based on these automatons to recognize complex attack scenarios.

SIDAN (Software Instrumentation for Detecting Attacks on Non-control-data) is a tool that aims to instrument automatically C-language software with assertions whose role is to detect attacks against the software. This tool is implemented as a plugin of the FRAMA-C framework that provides an implementation of static analysis techniques.

5.2. Privacy

GEPETO (GEoPrivacy-Enhancing TOolkit) is an open source software for managing geolocated data (currently in development in cooperation with LAAS). GEPETO can be used to visualize, sanitize, perform inference attacks and measure the utility of a particular geolocated dataset. For each of these actions, a set of different techniques and algorithms can be applied. The global objective of GEPETO is to enable a user to design, tune, experiment, and evaluate various sanitization algorithms and inference attacks as well as visualizing the following results and assessing their utility.

5.3. Reliable Programming

The Prometeus project, part of the Inria Gforge, is a software environment for reliable programming. The basic elements of Prometeus are Eva, a component-based framework and Adam, a set of group communication services. Eva is an implementation of a component model that aims at supporting the development of distributed abstractions and high-level communication protocols. Adam is a library of agreement components, based on the component model implemented by Eva. The central element of the Adam library is GAC (Generic Agreement Component). It implements a generic and adaptive fault-tolerant consensus algorithm that can be customized to cope with the characteristics of the environment. Moreover, thanks to a set of versatile methods, its behavior can be tuned to fit the exact needs of a specific agreement problem. A range of fundamental Adam components are implemented as specializations of this GAC component. The Adam library currently includes the most important components for reliable distributed programming (Group Membership, Atomic Broadcast).

6. New Results

6.1. Intrusion Detection

Metamorphic codes :

In [12], we have proposed a advance code obfuscation technique for metamorphic codes (i.e., codes that automatically recode themselves each time they propagates or are distributed). We have shown that the detection of such codes was a problem for classical nowadays static detection tools. In [25], we focus on a new dynamic detection approach which allows to detect variants produced by our metamorphic engine. In addition, our approach can detect unknown malware as long as their behavior approaches that of a known malware. For this, we propose to use a measure of similarity between program behaviors. This measure is obtained by lossless compression of execution traces in terms of system calls.

Intrusion Detection based on an Analysis of the Flow Control :

In [13], intrusion detection mechanisms based on the construct a model of normal behavior of the supervised entity are studied. Such a model is used during the detection phase to raise an alarm when a deviation is observed. This approach allows to detect unknown attacks.

The most common anomaly detection mechanisms at application level consist in detecting a deviation of the control-flow of a program. A popular method to detect such anomaly is the use of application sequences of system calls. However, such methods do not detect mimicry attacks or attacks against the integrity of the system call parameters. To enhance such detection mechanisms, we propose in [27] an approach to detect in the application the corruption of data items that have an influence on the system calls. This approach consists in building automatically a data-oriented behavior model of an application by static analysis of its source code. The proposed approach is illustrated on various examples, and an injection method is experimented to obtain an approximation of the detection coverage of the generated mechanisms.

Most of today's MAC implementations can be turned into permissive mode, where no enforcement is performed but alerts are raised instead. This behavior is very close to an anomaly IDS except that the system is configured through a MAC policy. MAC implementations such as SELinux and AppArmor come with a default policy including real life and practical rules ready to be used as is or as a basis for a custom policy. In [30], we first propose an extension of an IDS based on information flow control. We address issues concerning programs execution and improve its expressiveness in terms of security policy. This extended model can be configured to reach a wide variety of different security goals. Particularly, it allows for information flow checking based on users and/or programs dependent policy rules. Furthermore, suspicious modification of binary programs can be detected to avoid malware execution. We also propose an algorithm for deriving an AppArmor MAC policy into an information flow policy, and thus get the advantage of having a ready to use policy offering good security. An integration within Android is described in [37].

Flow based Interpretation of Access Control Policies :

In [32], we introduce a formal property characterizing access control policies for which the interpretations of access control as mechanism over objects and as mechanism over information contained into objects are similar. This leads us to define both a flow based interpretation of access control policies and the information flows generated during the executions of a system implementing an access control mechanism. When these two interpretations are not equivalent, we propose to add a mechanism dedicated to illegal information flow detection to the mechanism of access control over objects. Such a mechanism is parameterized by the access control policy and is proved sound and complete. We also briefly describe two real implementations, at two levels of granularity, of our illegal flow detection mechanism: one for the Linux operating system and one for the Java Virtual Machine.

Intrusion Detection based on Invariants :

RRABIDS (Ruby on Rails Anomaly Based Intrusion Detection System) [40] is an application level intrusion detection system for applications implemented with the Ruby on Rails framework. The goal of this intrusion detection system is to detect attacks against data in the context of web applications. This anomaly based IDS focuses on the modeling of the normal application profile using invariants. These invariants are discovered during a learning phase. Then, they are used to instrument the web application at source code level, so that a deviation from the normal profile can be detected at run-time. On simple examples we show how the approach detects well known categories of web attacks that involve a state violation of the application, such as SQL injections. Finally, an assessment phase is performed to evaluate the accuracy of the detection provided by the proposed approach.

Alert Correlation :

Alert correlation is a crucial problem for monitoring and securing computer networks. It consists in analyzing the alerts triggered by intrusion detection systems (IDSs) and other security related tools in order to detect complex attack plans, discover false alerts, etc. The huge amounts of alerts raised continuously by IDSs and the impossibility for security operators to efficiently analyze them requires tools for eliminating false and redundant alerts on the one hand and prioritize them according the detected activities? dangerousness and preferences of the analysts on the other hand. In [35], we describe an architecture that combines AI-based approaches for representing and reasoning with security operators? knowledge and preferences. Moreover, this architecture allows to combines experts' knowledge with machine learning and classifier based tools. This prototype collects the alerts raised by security related tools and analyzes them automatically.

Trust-Based IDS for the AODV Protocol :

Routing in ad hoc networks is based on mutual trust between collaborating nodes. Security problems arise when supposedly honest nodes lie deliberately to maximize their profit. In [11], we are interested in detecting misbehaving nodes within the ad hoc routing protocol AODV. We propose and implement a real-time intrusion detection system based on implicit trust relations: a node implementing this system collects its neighbors' routing messages and reasons on them to decide on their honesty. We also evaluate our implementation, and, based on simulations, show that the system we have developed to detect dishonest behavior is efficient.

Modelization and Simulation of Zombies Behaviours :

In [26], we study the modelization and simulation of zombie machines for the evaluation of Network Intrusion Detection Systems (NIDS), used to detect botnets. We propose an automatic method to infer zombies behaviours through the analysis of messages exchanged with their masters. Once computed, a model provides a way to generate realistic and manageable traffic, which is mandatory for an NIDS evaluation. We propose to use a Stochastic Mealy Machine to model zombies behaviours, and an active inference algorithm to learn it. With our approach, it is possible to generate a realistic traffic corresponding to the communications of botnets while ensuring its controllability in the context of an NIDS evaluation.

6.2. Privacy

Computer privacy is a domain where the education and information of the general public is paramount. In this perspective, through [44] we have participated to the popularization effort in the area, by exposing a survey of accessible computing tools allowing users to better protect their online privacy.

Formal Privacy Policies and Logical Tools :

One of the obstacles to the improvement of the privacy level in distributed applications is the lack of expressiveness, usability and enforceability of the associated policies. This new research track aims at designing better privacy policies for complex systems, more adapted to the specific needs of personal data protection regulations and easier to enforce in a distributed fashion. Logical languages, in particular, are considered as interesting candidates because of the reasoning capabilities attached to the formalisms, allowing autonomous peers to perform efficient, privacy-aware planning. [18] is a contribution to the modal logics used to model formal norms, focusing on specific deadline-related temporal notions often encountered in privacy policies. In [39], we propose an ambitious, collaborative research project based on an epistemic view of the privacy laws and regulations, which should lead to the design of several tools, including policy writing assistants and validation software. [24] is a generic work in the domain of formal policies, where we propose a logical model of various concepts of responsibility in an organizational framework featuring obligation delegation. This kind of framework is intended to model the handling of complex policies in real-life human institutions.

Privacy in Social Networking Sites :

Social Networking Sites (SNS), such as Facebook and LinkedIn, have become the established place for keeping contact with old friends and meeting new acquaintances. As a result, a user leaves a big trail of personal information about him and his friends on the SNS, sometimes even without being aware of it. This information can lead to privacy drifts such as damaging his reputation and credibility, security risks (for instance identity theft) and profiling risks. Another research challenge stems from the fact that in the digital world where it is possible to copy the information as often as desired, it is not easy to control how information is disseminated once it is out on the Internet. In an ongoing collaboration [23] with Ai Thanh Ho and Esma Aïmeur (Université de Montréal), we investigate tools that can help user to maintain the sovereignty of their data on the World Wide Web. We also introduce PrivacyMarker, an approach drawing on the concept of provenance and accountability to protect user privacy on SNS. More precisely, it is possible to imagine that by a combination of logs and techniques such as watermarking and traitor-tracing schemes, the dissemination of information can be (at least partially) controlled and that in case of a privacy breach, it is possible to identify which persons are potentially suspect because they have previously accessed this information.

Geo-privacy :

A geolocalised system generally belongs to an individual and as such knowing its location reveals the location of its owner, which is a direct threat against his privacy. To protect the privacy of users, a sanitization process, which adds uncertainty to the data and removes some sensible information, can be performed but at the cost of a decrease of utility due to the quality degradation of the data. In a joint work [16] with Marc-Olivier Killijian and Miguel Nunez del Prado (LAAS-CNRS), we describe GEPETO (for GEoPrivacy-Enhancing TOolkit), a flexible open source software which can be used to visualize, sanitize, perform inference attacks and measure the utility of a particular geolocalised dataset. We also introduce a mobility model that we coin as mobility Markov Chain, which can represent in a compact yet precise way the mobility behaviour of an individual. Finally, we describe an algorithm for learning such a structure from the mobility traces of an individual.

Geosocial networks are relatively new compared to the more “traditional“ (i.e. non-geolocated) social networking sites such as Facebook or LinkedIn that have been around since more than 6 years, but they are currently growing relatively fast along with the widespread development of other geolocated applications and technologies. In a study [29] done in cooperation with Olivier Heen (Technicolor) and Christophe Potin, we provide a comparative analysis of some existing geosocial networks with respect to privacy in order to (1) highlight some of privacy issues that are raised by the fast development of these system and (2) propose recommendations that could be integrated in the design of these systems to enhance the privacy of their users based on this analysis.

Privacy in Distributed Systems :

In a joint work [19] with Anne-Marie Kermarrec and Mohammad Alaggan (team INRIA ASAP), we address the problem of computing the similarity between two users (according to their profiles) while preserving their privacy in a fully decentralized system and for the passive adversary model. First, we introduce a two-party protocol for privately computing a threshold version of the similarity and apply it to well-known similarity measures such as the scalar product and the cosine similarity. The output of this protocol is only one bit of information telling whether or not two users are similar beyond a predetermined threshold. Afterwards, we explore the computation of the exact and threshold similarity within the context of differential privacy, a recent notion developed that provides a strong privacy guarantee that holds independently of the auxiliary knowledge that the adversary might have. More specifically, we design several differentially private variants of the exact and threshold protocols and we also analyze their complexity as well as their impact on the utility of the resulting similarity measure. Finally, we provide experimental results validating the effectiveness of the proposed approach on real datasets.

Other ongoing work tackles the problem of computing an aggregation function in a *secure* and *scalable* way in a distributed network [42] (joint work with Rachid Guerraoui, Hamza Harkous, Florian Huc and Anne-Marie Kermarrec).

6.3. Accidental and Malicious Faults in Distributed Systems

Induced Churn to Face Malicious Behaviors :

In reputation mechanisms, ensuring durable access to feedbacks is a first barrier against simple attacks. To bias the reputation mechanism, an adversary can create and use several distinct identities. In that case, if the reputation mechanism is solely based on statistical measurements, the trustworthiness can be violated. Our contribution is centered around the study of robust mechanisms that can resist such attacks.

Toward this goal, we have first investigating the problem of uniform sampling in large scale open systems in presence of adversarial nodes. Uniform sampling ensures that any individual in a population has the same probability to be selected as sample. Uniform sampling finds its root in many problems such as data collection, dissemination, load balancing, and data-caching.

By relying on the topological properties of structured peer-to-peer systems, it has been shown that it is possible to guarantee with high probability that any node is equally likely to appear in the local view of each other honest node in a number of rounds polynomial in the size of the system. This is achieved by imposing nodes to frequently depart from their position and move to another random position in the system. Indeed, in [15], we have shown that an adversary can very quickly subvert overlays based on distributed hash tables by simply never triggering leave operations. We have also demonstrated that when all nodes (honest and malicious ones) are imposed on a limited lifetime, the system eventually reaches a stationary regime where the ratio of polluted clusters is bounded, independently from the initial amount of corruption in the system.

In unstructured peer-to-peer systems, nodes cannot rely on the topological nature of structured graphs to detect undesirable behaviors. The sampling has to be uniform and ergodic. Informally, this second property guarantees that each received node id infinitely often has a non-null probability to locally appear as a sample. In [21], we determine necessary and sufficient conditions under which uniform and ergodic sampling is achievable in unstructured peer-to-peer systems potentially populated with a large proportion of Byzantine nodes. Strict restrictions are imposed on the number of messages gossiped by malicious nodes during a given period of time and providing each honest node with a very large memory (in the size of the system).

In [38], we consider the problem of targeted attacks in large scale peer-to-peer overlays. These attacks aimed at exhausting key resources of targeted hosts to diminish their capacity to provide or receive services. To defend the system against such attacks, we rely on clustering and implement induced churn to preserve randomness of nodes identifiers so that adversarial predictions are impossible. We propose robust join, leave, merge and split operations to discourage brute force denial of services and pollution attacks.

Sequence of Consensus Instances :

To be able to coordinate efficiently the activities of replicas, a significant body of work on replication techniques, group communication services and agreement problems has been done. The Consensus service has been recognized as a fundamental building block for fault-tolerant distributed systems. Many different protocols to implement such a service have been proposed, however, little effort has been placed in evaluating their performance. During her PhD thesis [14], Izabela Moise has presented a protocol designed to solve several consecutive consensus instances in an asynchronous distributed system prone to crash failures and message omissions. The protocol [31] follows the Paxos approach [49], [47] and integrates two different optimizations to reduce the latency of learning a decision value. As one optimization is risky [48], dynamics triggering criterion are defined to check at runtime if the context seems to be favorable or not. The proposed protocol [34] is adaptive as it tries to obtain the best performance gain depending on the current context. Moreover, it guarantees the persistence of all decision values. Our experimentation results [36] focus on the impact of the prediction of collisions (*i.e.*, the cases where the use of the risky optimization is counterproductive).

Transactional Mobile Agent :

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. In [33], we propose a solution where 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. Contracts and Grants with Industry

7.1. Contracts with Industry

- Contract DGA PEA (Exploratory Study Program) : "Security of the ad hoc routing protocols in the context of future tactical military networks" (2011-2012)

  One of the objectives of future tactical networks is to allow non-hierarchical communications between FIST (Future Integrated Soldier Technology) troopers. In this context, ad hoc networks are a candidate of choice : they allow non-hierarchical routing, but also automatically handles the mobility of entities taking part to the network while enabling a fast and simple deployment. Hence, the goal of this contract it to study security of the ad hoc routing protocols in the context of future tactical military networks.

  We first specified the global architecture of the future military tactical networks so as to identify the various use cases of ad hoc networks in this context. Then, we made a state of the art of the various ad hoc routing protocols, so as to define what protocols suit the best the various contexts of the future military tactical networks. We also studied the attacks that exist against the ad hoc routing protocols, and proposed attack scenarios in the context of future military tactical networks. We now are studying the security mechanisms that could be deployed to protect against these attacks. The main idea is to combine cryptographic solutions to protect against identity theft, and misbehavior detection solutions to prevent entities from sending deliberately false routing information. In the last phase of the study, we will develop a proof-of-concept demonstrating the utility of combining these two approaches to protect against attacks previously identified.

  This study is led by Supélec and involves the University of Rennes 1 (CIDer Team) and OPEN, an IT service provider located at Rennes.

- In 2011, four small contracts dedicated to experimental development in security, involving members of the CIDRE project and students of Supélec, have been realized. The objectives of these 4 projects were (1) the elliptic curves based signature of classical paper document such as invoices, (2) the detection of malicious phone calls on Android smartphones, (3), the secured visualization of documents on a computer screen (the user can be sure that the correct document is displayed), and (4) the detection of information leaks in documents that can be found on the web.

7.2. Grants with Industry

The PhD of Georges Bossert (on the evaluation of intrusion detection mechanisms) is done in the context of a Cifre contract with Amossys (http://www.amossys.fr/).

8. Partnerships and Cooperations

8.1. Regional Initiatives

The PhD of Regina Marin (on privacy protection in distributed social networks) is supported by a ARED grant (with Région Bretagne).

8.2. National Initiatives

- **ANR SETIN Project: POLUX (2007-2011)**
  POLUX aimed at configuring automatically the security mechanisms (prevention and detection) from the specification of the system in terms of its security policy. Indeed, current security tools are totally uncoordinated. They come from a large number of vendors. Even worse, they are sometimes developed by newcomers to the security field and they use different configuration logics and languages that bear little resemblance one to another or to the previously proposed formalisms. As a result, ensuring interoperability between these tools is a difficult endeavor. Researchers are facing the same issues, different communities looking at either access control, security protocols or intrusion detection, but with little coordination or fusion between these domains. A few standard

formats have been defined over the years, but they only cover small areas, and they have been very long in the making. We first studied this interoperability problem and developed a framework allowing a unified expression of security policies for the entire range of security tools related to prevention of security issues, detection of threats, and countermeasures. The expression of these security policies obeyed precise constraints permitting the verification of their soundness and the validation of their application to a particular information system. It also allowed interoperability and negotiation of security policies and included the management of the security policy as a meta-policy. This formalism and framework applied to the complete range of security tools covering the three key properties of security, integrity, confidentiality and availability. This project is led by Télécom Bretagne and involves Supélec.

- **ANR SETIN Project: PLACID (2007-2011)** PLACID is an interdisciplinary project that combines expertise in artificial intelligence and computer security. Alarm correlation is a subfield of intrusion detection whose goal is to make heterogeneous IDS sensors cooperate in order to improve the attack detection rate, enrich the semantics of alerts and reduce the overall number of alerts. Several solutions have been proposed in the literature, all of which require knowledge about the attacks and the context in which they occur. At the same time, complementary tools have appeared to support alarm correlation by providing knowledge databases about attacks, as well as local and global contextual observations. However, none of these correlation solutions received a wide acceptance. We believe that one of the reason for this is that the intrusion detection domain lacks a common logic that would allow security systems to reason about complementary evidences and security operators to interact with these systems efficiently. The objective of the PLACID project is twofolds. First we investigate a formal description logic for intrusion detection, called IDDL, which stands for Intrusion Detection Description Logic. IDDL will provide security components with a formal framework to characterize their observation, share their knowledge with third-party components and reason about complementary evidence information. Second, we investigate bayesian-based approaches for alert correlation. Our aim is to model uncertainty associated with alerts, to represent malicious actions, and to model correlation relations between alerts. The use of bayesian networks has several advantages such as evaluating the success of attacks, reducing the set of possible attacks scenarios, learning correlation relations, or finding the root cause of alerts.

  This project is led by the University of Nantes and involves the University of Artois and Supélec.

- **ANR Arpege Project: DALI (2009-2011)**

  DALI aims at developing innovative design solutions to enhance the capabilities of current intrusion detection systems at the application level as well as new methodologies and tools for assessment and evaluation of the proposed solution with respect to their ability to detect potential intrusions. We expect to enhance the detection capability by inserting the mechanisms directly inside the software. Our work focuses on two complementary methods: First, the specification of software security contracts in terms of application level security policy, and second, an introspective method to learn the software specification at run-time. Both methods will lead to instrument the software to insert intrusion detection mechanisms. The challenges that will be addressed include the identification of the security attributes which must be captured by contracts, the ability to have enough introspection at run-time to learn program behavior, and finally the ability to instrument automatically the software. Our analysis of the state of the art reveals that there is still a lack of rigorous methodologies defining how the developers should proceed for testing security and a lack of tools supporting the implementation of such a methodology. Our project aims at fullling these two objectives. One of our objectives is to develop a uniform, repeatable, and cost-effective way to test and evaluate IDS, either as a stand-alone assessment or, more often, for comparative evaluation across systems and components. Particular attention is put on the generation of inputs combining normal and malicious activities and the definition of input selection criteria taking into account the security properties and the specification of the application. Moreover, in the context of the project, we will develop a platform that will permit to show the feasibility of the different approaches in the project, both in terms of intrusion detection design and assessment.

This project is led by Kereval and involves Télécom Bretagne, Supélec and the LAAS/ CNRS.

- **ANR SeSur Project: LISE (2008-2011)**

  The LISE project intends to study the relationship between law and technique in the realization of secure computing systems. In particular, solutions for assessing and proving the responsibility of parties should be defined. LISE follows a top-down approach, starting with the definition of liability and deriving sufficient and acceptable execution traces. The main phases of the project are as follows: (1) State of the art and recommendations for potential evolutions of current regulations in order to make them suitable to the new ICT society and to favor the emergence of a true "liability economy" of software. (2) Method for software liability specification and definition of a legally acceptable link with execution traces. (3) Method for the analysis of execution traces to determine liability based on the agreed specification.

  This project is led by INRIA Rhône-Alpes and involves the University of Versailles Saint-Quentin-en-Yvelines, the University of Caen Basse-Normandie, Supélec and VERIMAG.

- **ANR INS Project: AMORES (2011-2015)**

  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). This project is joint between the Université de Rennes 1, Supélec, LAAS-CNRS, Mobigis and Tisséo.

- **ANR INS Project : LYRICS (2011-2014)**

  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. The project is joint between France Télécom, Atos Wordline, CryptoExperts, ENSI Bourges, ENSI Caen, MoDyCo, Oberthur Technologies, NEC Corporation, Microsoft and Université de Rennes 1.

- **LABEX Comin Labs**

  CIDRE participates in the CominLabs initiative sponsored by the "Laboratoires d'Excellence" program and which federates the best teams from Bretagne and Nantes regions in the broad area of telecommunications, from electronic devices to distributed applications. We are in particular involved in the "security and privacy" focus that is co-chaired by a member of the team.

8.3. European Initiatives

- **Quaero**

  CIDRE is involved in the Quaero project. Quaero is a program promoting research and industrial innovation on technologies for automatic analysis and classification of multimedia and multilingual documents. The partners collaborate on research and the realisation of advanced demonstrators and prototypes of innovating applications and services for access and usage of multimedia information, such as spoken language, images, video and music. The Quaero consortium (composed of French and German public and private research organisations) is coordinated by Technicolor.

Sébastien Gambs is involved in one of the task (leaded by Amedeo Napoli, équipe INRIA Orpailleur) of the Quaero project whose aim is to study the implications in terms of privacy for a user to participate in personalized applications (such as video-on-demand) adapted to the user context, background and preferences as well as proposing solutions that can contribute to enhance this privacy. On one hand using personal data to tailor the content to the user needs may be important for improving the quality of service and its relevance but on the other hand this raises serious privacy issues regarding how this data will be collected, used and disseminated. The main purpose of the solutions developed in this task is to enable an individual to access personalized content/service in a privacy-preserving manner and without having to disclose any unnecessary personal information. Since November 2011, Julien Lolive has also join the project as an engineer.

- **EIT ICT Labs**

  EIT ICT Labs is one of the first three Knowledge and Innovation Communities (KICs) selected by the European Institute of Innovation & Technology (EIT) to accelerate innovation in Europe.

  Nowadays, Information Technologies have invaded many aspects of the daily lives of individuals, thus creating a lot of new possibilities but also raising privacy concerns to the point that some individuals feel that they no longer have suitable guarantees or any control about their privacy. Indeed, protecting the privacy of individuals is one of the main challenges of the « Information Society » but is difficult to achieve as individuals constantly leave digital traces of their actions and whereabouts, often without even knowing it. If an unauthorized entity gathers these digital traces, he (or she) can use them for malicious purposes ranging from targeted spam to profiling, and even identity theft.

  The goal of the action line "Protection of Privacy in the Information Society" (created by Sébastien Gambs together with Daniel Le Métayer and Claude Castelluccia from INRIA Rhône-Alpes) is to address the new challenges raised by the most recent developments and usages of information technologies (e.g., geo-located applications, social networking sites, profiling, pervasive computing, data mining) by providing solutions to enhance the privacy protection of individuals in the Information Society. Essentially, this action line is transversal to most of the thematic and research action lines of EIT ICT labs and it is envisioned that it should also contribute to their developments. While the action line was originally intended to focus on privacy, its scope was recently extended to include security and trust thus being renamed as "Security, Privacy and Trust in the Information Society". In 2012, Sébastien Gambs will lead an activity in this action line related to location privacy that involves partners coming from 3 different nodes of EIT ICT labs.

8.4. International Initiatives

8.4.1. INRIA International Partners

CANADA: Sébastien Gambs is co-supervising Ai Thanh Ho, a PhD student from the Université de Montréal with whom he has been actively collaborating for 2 years on the subject of privacy issues in social networking sites. The main supervisor of Ai Thanh Ho is Esma Aïmeur (full professor, Université de Montréal). Ai Thanh Ho has visited us in November 2011. In 2011, this cooperation has led to a joint publication [23].

BRAZIL: Francisco Brasileiro, Professor at the Federal University of Paraiba (Campina Grande) was involved with us in a four years Capes/Cofecube project (2005-2009). We still cooperate with him on the dependability evaluation of cluster-based systems [15].
We have also strong links with University of Brasilia (Brazil) and in particular with Prof. Rafael de Sousa (Brasilia) who has spent one year and an half in Supélec (March 2006 to August 2007). With his team, we study the concept of trust in the context of mobile ad hoc networks.

AUSTRALIA: With Queensland University of Technology (QUT, Brisbane) we cooperate to study policy-based intrusion detection problems. Jacob Zimmermann (QUT) spent one month in Supélec (January 2007). Two people from Supélec (Benjamin Morin and Ludovic Mé) visited QUT in September 2007. Andrew Clark (QUT) spent 3 months in Supélec from August to November 2009. The PhD thesis of Christophe Hauser, "Détection d'intrusions dans les systèmes distribués", started in October 2009, is supervised jointly with Queensland University of Technology, Brisbane, Australia (Prof. Andrew Clarck). Since February 2011, Christopher Hauser works in Brisbane. His one year visit is supported by a grant from Rennes Métropole.

8.4.2. Visits of International Scientists

ALGERIA: Linda Zeghache, Phd student at USTBH-CEDRIC (université des Sciences et de la Technologie Houari Boumédiène, Algeria) visited us during one month in December 2010/January 2011. This cooperation has led to a joint publication in 2011 [33].

CANADA: Frédéric Massicotte from the "Communications Research Centre Canada" has visited us in March 2011. The CRC is the federal government's primary laboratory for research and development in advanced telecommunications.

CHINA: Chuanyou Li, PhD student at Southeast University (Nanjing, China) is visiting us during a period of one year (December 2011 - November 2012). Since the end of a LIAMA project (2000-2002), strong relationships are maintained with the research team of Prof. Yun Wang of Southeast university. The joint works focus mainly on fault-tolerance in distributed systems and security in ad hoc networks.

8.4.3. Participation In International Programs

CIDRE participates to a project for the ICST Algeria program (Information and Communication Science and Technology). The title of the project is "Utilisation de la plate-forme de test Senslab pour le projet irrigsense". This 2-year project (2011-2012) is leaded by the Project-Team DIONYSOS and involves two other INRIA teams ASAP, CIDRE. The CERIST represents the Algerian partner. The project focuses on using the senslab node of Rennes, for testing different protocols developed by the partners in the context of an algerian project which aims at using sensors for agricultural irrigation.

9. Dissemination

9.1. Animation of the scientific community

Ludovic Mé acts as a

- member of the editorial board of the "Journal in Computer Virology", Springer (http://www.springer.com/computer/journal/11416).
- member of the steering committee of the "Computer & Electronics Security Applications Rendez-vous (C&ESAR 2011)" held in November 2011 in Rennes, france (http://www.cesar-conference.org).
- member of the steering committee of the "6th Conference on Network Architecture and Information Systems Security (SAR-SSI 2011)" held in May 2011 at "Ile De Ré", La Rochelle, France (http://sarssi-conf.org/index.htm).
- member of the program committee of the "6th Conference on Network Architecture and Information Systems Security (SAR-SSI 2011)" held in May 2011 at "Ile De Ré", La Rochelle, France (http://sarssi-conf.org/index.htm).
- member of the program committee of the "6th International Conference on Risks and Security of Internet and Systems (CRISIS 2011)" held in September 2011 in Timisoara, Romania (http://crisis2011.cs.upt.ro/index.html).

- member of the program committee of the “4th Canada-France MITACS Workshop on Foundations & Practice of Security (FPS 2011)” held in May 2011 in Paris, France (http://fps2011.dyndns.org/home.html).
- member of the program committee of the “4th SETOP International Workshop on Autonomous and Spontaneous Security (SETOP 2011)” held in September in Leuven, Belgium (http://setop2011.dyndns.org/home.html).
- external reviewer for RAID (14th International Symposium on Recent Advances in Intrusion Detection).
- member of a DGA’s scientific committee.

Christophe Bidan acts as a

- member of the program committee of the “Computer & Electronics Security Applications Rendez-vous (C&ESAR 2011)” organized in Rennes in November 20111 (http://www.cesar-conference.org).
- member of the program committee of the “6th Conference on Network Architecture and Information Systems Security (SAR-SSI 2011)” held in May 2011 at “Ile De Ré”, La Rochelle, France (http://sarssi-conf.org/index.htm).
- member of the program committee of the “6th International Conference on Risks and Security of Internet and Systems (CRISIS 2011)” held in September 2011 in Timisoara, Romania (http://crisis2011.cs.upt.ro/index.html).
- member of the program committee of the “4th Canada-France MITACS Workshop on Foundations & Practice of Security (FPS 2011)” held in May 2011 in Paris, France (http://fps2011.dyndns.org/home.html).

Sébastien Gambs acts as a

- member of the editorial board of International Journal of Data Mining, Modelling and Management (http://www.inderscience.com/browse/index.php?journalID=342#board).
- member of the organization committee of the Atelier Protection de la Vie Privée / Géolocalisation et Vie Privée (APVP 2011) held in June 2011 in Toulouse, France (http://homepages.laas.fr/mkilliji/APVP2011/Site/APVP2011.html).
- member of the scientific committee of the “2nd workshop on games, logic and security (GIPSy 2011)” held in October 2011 in Rennes, France (http://www.irisa.fr/prive/pinchina/GIPSy/gipsy11.html).
- member of the program committee of the “12th Conference on Communications and Multimedia Security (CMS 2011)” held in October 2011 in Ghent, Belgium (http://www.cms2011.net/index.shtml).
- member of the program committee of the “4th International Workshop on Security and Privacy in GIS and LBS (SPRINGL 2011)” held in November 2011 in Chicago, USA (http://springl2011.modap.org/index.html).
- member of the technical program committee of the “4th International Workshop on SEcurity and SOCial Networking (SESOC 2012)” held in March 2012 in Lugano, Switzerland (http://www.sesoc.org/home.htm).
- external reviewer for PST 2011 (Ninth Annual Conference on Privacy, Security and Trust), GeoProcessing 2011 (Conference on Advanced Geographic Information Systems, Applications, and Services).

Guillaume Hiet acts as a

- member of the program committee of the “6th Conference on Network Architecture and Information Systems Security (SAR-SSI 2011)” held in May 2011 at “Ile De Ré”, La Rochelle, France (http://sarssi-conf.org/index.htm).
- member of the program committee of the “14th International Symposium on Recent Advances in Intrusion Detection (RAID 2011)” held in September 2011 in Menlo Park, California (http://www.raid-symposium.org/raid2011/).
- external reviewer for the TSI journal (Technique et Science Informatiques)

Michel Hurfin acts as a

- member of the editorial board of the Springer Journal of Internet Services and Applications, Springer (http://www.springer.com/computer/communications/journal/13174).
- member of the program committee of the “3rd IEEE International Symposium on UbiSafe Computing” held in November 2011 in Changsha, China (http://trust.csu.edu.cn/conference/ubisafe2011).
- member of the program committee of the “2nd International Workshop on Interconnections of Wireless Sensor Networks (IWSN 2011)” held in conjunction with IEEE/ACM DCOSS 2011 in June 2011, in Barcelona, Spain (http://iwsn2011.gforge.uni.lu/index.html).
- member of the program committee of the “3rd International Workshop on Workflow Management in Service and Cloud Computing (WMSC2011)” held in December 2011 in Sydney, Australia (http://kpnm.hnust.cn/confs/wmsc2011).
- member of the program committee of the “11st African Conference on research In Computer Science and Applied Mathematics (CARI 2012)” held in October 2012 in Algiers, Algeria (http://www.cari-info.org/).
- external reviewer for the Information and Computation Journal.
- member of the COST-GTAI (reviewer for both ARCs and ADT submissions).

Guillaume Piolle acts as a

- member of the program committee of the “6th Conference on Network Architecture and Information Systems Security (SAR-SSI 2011)” held in May 2011 at “Ile De Ré”, La Rochelle, France (http://sarssi-conf.org/index.htm).
- member of the scientific committee of the “2nd workshop on games, logic and security (GIPSy 2011)” held in October 2011 in Rennes, France (http://www.irisa.fr/prive/pinchina/GIPSy/gipsy11.html).
- external reviewer for CDP 2011 (Computers, Privacy & Data Protection), FPS 2011 (Workshop on Foundations & Practice of Security), RAID 2011 (Symposium on Recent Advances in Intrusion Detection), and SecureComm 2011 (Conference on Security and Privacy in Communication Networks).

Nicolas Prigent acts as a

- member of the program committee of the “Symposium sur la Sécurité des Technologies de l’Information et des Communications (SSTIC 2011)” held in June 2011 in Rennes, France (http://www.sstic.org/2011/news/).
- member of the program committee of the “6th Conference on Network Architecture and Information Systems Security (SAR-SSI 2011)” held in May 2011 at “Ile De Ré”, La Rochelle, France (http://sarssi-conf.org/index.htm).
- member of the program committee of the “Symposium sur la Sécurité des Technologies de l’Information et des Communications (SSTIC 2012)” held in June 2012 in Rennes, France (http://www.sstic.org/2012/news/).

- member of the organization committee of the “Symposium sur la Sécurité des Technologies de l’Information et des Communications (SSTIC 2012)” held in June 2012 in Rennes, France (http://www.sstic.org/2012/news/).
- external reviewer for CT-RSA 2011 (Cryptographers’ Track of the RSA Conference).

Eric Totel acts as a

- member of the program committee of the “6th Conference on Network Architecture and Information Systems Security (SAR-SSI 2011)” held in May 2011 at “Ile De Ré”, La Rochelle, France (http://sarssi-conf.org/index.htm).
- external reviewer for RAID 2011 (Recent Advances in Intrusion Detection), FPS 2011 (Foundations & Practice of Security), SecureComm 2011 (Conference on Security and Privacy in Communication Networks), and SAR-SSI 2011 (Conference on Network Architectures and Information Systems Security).

Frédéric Tronel acts as a

- member of the organization committee of the Symposium sur la Sécurité des Technologies de l’Information et des Communications (SSTIC 2011) held in June 2011 in Rennes, France (http://www.sstic.org/2011/news/).
- member of the program committee of the Symposium sur la Sécurité des Technologies de l’Information et des Communications (SSTIC 2011) held in June 2011 in Rennes, France (http://www.sstic.org/2011/news/).
- member of the program committee of the “6th Conference on Network Architecture and Information Systems Security (SAR-SSI 2011)” held in May 2011 at “Ile De Ré”, La Rochelle, France (http://sarssi-conf.org/index.htm)
- external reviewer for RAID 2011 (Recent Advances in Intrusion Detection).

Valérie Viet Triem Tong acts as a

- member of the program committee of the “6th Conference on Network Architecture and Information Systems Security (SAR-SSI 2011)” held in May 2011 at “Ile De Ré”, La Rochelle, France (http://sarssi-conf.org/index.htm)
- external reviewer for the journal “Security and Communication Networks” (Special Issue on Defending Against Insider Threats and Internal Data Leakage).

9.2. Teaching

Ludovic Mé is Professor at Supélec :

Master : “Information systems”, 6 hours, M1 - second year of the engineer degree, Supélec, France

Master : “Security policies”, 3 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Intrusion detection”, 9 hours of lecture, M2 - Master research, Rennes, France

Master : “Intrusion detection”, 6 hours of lecture, M2 - Master SSI, Université de Limoges, France

Master : “Intrusion detection”, 8 hours of lecture, M2 - Master Pro SSI, université de Rennes 1, France

Master : “Intrusion detection”, 9 hours of lecture, M2 - Master SSI, Supélec & Télécom Bretagne, France

Master : “Security of information systems”, 12 hours of lecture, M2- post-graduate training (master Architecture des Réseaux de Communication), Supélec, France

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

Master : Ludovic Mé is responsible for the module “Security of data and Infrastructure information systems”, M2 - Master research, Rennes, France (until June 2011)

Doctorat : “Introduction to security issues in Computer science”, 9 hours of lecture, Université de Rennes 1, Doctoral School Matisse, France.

Christophe Bidan is Professor at Supélec :

Licence : “Programming models”, 13 hours, L3 - first year of the engineer degree, Supélec, France

Licence : “Foundations of computer science, data structures and algorithms”, 40 hours including 18 hours of lecture, L3 - first year of the engineer degree, Supélec, France

Master : “Information system”, 6 hours, M1 - second year of the engineer degree, Supélec, France

Master : “Software engineering”, 22 hours, M1 - second year of the engineer degree, Supélec, France

Master : “Supervision of student project”, 9 hours, M1 - second year of the engineer degree, Supélec, France

Master : “Introduction to security threat”, 4.5 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Cryptography”, 44 hours including 18 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Audit technique Web”, 3 hours, M2 - third year of the engineer degree, Supélec, France

Sébastien Gambs is Associate Professor at Université de Rennes 1:

Master : “Protection of Privacy”, 32 hours including 16 hours of lectures, M2 - Master Pro SSI, université de Rennes 1, France

Master : “Topics on Authentication”, 16 hours of lectures, M2 - Master Pro SSI, université de Rennes 1, France

Master : Supervision (50%) of the master thesis of Christophe Potin from February to September

Guillaume Hiet is Associate Professor at Supélec :

Licence : “Programming models and languages”, 4 hours, L3 - first year of the engineer degree, Supélec, France

Licence : “Foundations of computer science, data structures and algorithms”, 16 hours, L3 - first year of the engineer degree, Supélec, France

Master : “Introduction to SSI”, 9 hours of lecture, M1 - second year of the engineer degree, Supélec, France

Master : “Supervision of student project”, 9 hours, M1 - second year of the engineer degree, Supélec, France

Master : “Supervision of student project - Computer and electronic”, 1 project, M1 - second year of the engineer degree, Supélec, France

Master : “Security in UNIX/Linux”, 4.5 hours including 1.5 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Intrusion detection sensors”, 3 hours, M2 - third year of the engineer degree, Supélec, France

Master : “Alert correlation”, 3 hours, M2 - third year of the engineer degree, Supélec, France

Master : “Securing an application vulnerable to buffer overflows”, 8 hours, M2 - third year of the engineer degree, Supélec, France

Master : “Supervision of student project”, 3 hours, M2 - third year of the engineer degree, Supélec, France

Master : “Introduction to UNIX/Linux”, 3 hours, M2 - post-graduate training (master Cyber Security), Supélec, France

Master : “Securing Linux (LDAP authentication, ACL and disk encryption)”, 6 hours, M2 - post-graduate training (master Cyber Security), Supélec, France

Master : “Security of Passwords”, 3 hours, M2 - post-graduate training (master Cyber Security), Supélec, France

Master : “Security of Java”, 3 hours, M2 - post-graduate training (master Cyber Security), Supélec, France

Master : “Intrusion detection sensors”, 3 hours, M2 - post-graduate training (master Cyber Security), Supélec, France

Master : “Preparation for the ICTF competition in computer security”, 12 hours, M2 - post-graduate training (master Cyber Security), Supélec, France

Master : “Securing UNIX/Linux”, 7 hours of lecture, M2 - post-graduate training CQP, Supélec, Gif-sur-Yvette, France

Master : “Intrusion detection”, 10 hours of lecture, M2 - post-graduate training CQP, Supélec, Gif-sur-Yvette, France

Master : “Intrusion detection (Introduction)”, 20 hours including 8 hours of lecture, M2 - Master Pro SSI, université de Rennes 1, France

Master : “Intrusion detection (Introduction)”, 10 hours including 4 hours of lecture, M2 - ESIR (Ecole supérieure d’ingénieur de Rennes), Université de Rennes 1, France

Supervision (100%) of the master thesis (and engineering internship) of Mounir Assaf (Supélec) from February to September

Supervision (50%) of the master thesis of Vincent Laporte (ENS) from February to June

Michel Hurfin contributes to the transfer of knowledge towards students :

Master : “Distributed protocols”, 7.5 hours of lecture, M2 - post-graduate training (master Architecture des Réseaux de Communication), Supélec, France

Guillaume Piolle is Associate Professor at Supélec :

Licence : “Models and programming languages”, 9 hours, L3 - first year of the engineer degree, Supélec, France

Licence : “Foundations of computer science, data structures and algorithms”, 18 hours, L3 - first year of the engineer degree, Supélec, France

Licence : “Software engineering”, 18 hours, L3 - first year of the engineer degree, Supélec, France

Master : “C++ /Qt”, 12 hours, M2 - third year of the engineer degree, Supélec, France

Master : “Network access protection”, 3 hours, M2 - third year of the engineer degree, Supélec, France

Master : “Web technologies”, 8.25 hours, M2 - post-graduate training, Supélec, France

Master : “Privacy and data protection on Internet”, 9 hours, M2 - post-graduate training, URFIST Ouest (Unité Régionale de Formation à l’Information Scientifique et Technique) – Université Rennes 2, France.

Master : “Supervision of student project”, 9 hours, M1 - second year of the engineer degree, Supélec, France

Nicolas Prigent is Associate Professor at Supélec :

- Licence : “Programming”, 20 hours, L3 - first year of the engineer degree, Supélec, France
- Master : “Network programming”, 15 hours, M2 - third year of the engineer degree, Supélec, France
- Master : “Network programming”, 11 hours, M2 - post-graduate training, Supélec, France
- Master : “Programming and data bases”, 15 hours, M2 - third year of the engineer degree, Supélec, France
- Master : “Computer security”, 4 hours, M2 - third year of the engineer degree, Supélec, France
- Master : “Programming”, 6 hours of lecture, M2 - third year of the engineer degree, Supélec, France
- Master : “Operating systems”, 12 hours of lecture, M2 - third year of the engineer degree, Supélec, France
- Master : “Computer science (computability and complexity)”, 3 hours of lecture, M2 - third year of the engineer degree, Supélec, France
- Master : “Operating systems (MS Windows)”, 2 hours of lecture, M2 - post-graduate training, Supélec, France
- Master : “Data bases”, 3 hours of lecture, M2 - post-graduate training, Supélec, France
- Master : “Security”, 17 hours including 9 hours of lecture, M2 - post-graduate training, Supélec, France

Eric Totel is Associate Professor at Supélec :

Licence : “Models and programming languages”, 19.5 hours including 10.5 hours of lecture, L3 - first year of the engineer degree, Supélec, France

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

Master : “Computer systems’ architecture”, 30 hours, M1 - second year of the engineer degree, Supélec, France

Master : “C language”, 24 hours including 6 hours of lecture, M2 - master SSI (Sécurité des systèmes d’information), Supélec, France

Master : “C language”, 12 hours including 3 hours of lecture, M2 - post-graduate training (master Architecture des Réseaux de Communication), Supélec, France

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

Master : “Description and specification languages”, 12 hours including 3 hours of lecture, M2 - post-graduate training (master Architecture des Réseaux de Communication), Supélec, France

Master : “Dependability”, 6 hours including 4.5 hours of lecture, M2 - third year of the engineer degree and master research, Supélec, France

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

Master : “Dependability”, 4.5 hours of lecture, M2 - post-graduate training (master Architecture des Réseaux de Communication), Supélec, France

Master : “Supervision of student project”, 4 projects, M1 - second year of the engineer degree, Supélec, France

Master : “Supervision of student project”, 1 project, M2 - third year of the engineer degree, Supélec, France

Frédéric Tronel is Associate Professor at Supélec :

Licence : “LISP”, 3 hours, L3 - first year of the engineer degree, Supélec, France

Licence : “Software engineering”, 18 hours, L3 - first year of the engineer degree, Supélec, France

Master : “Operating systems”, 10.5 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master: “Compilation”, 21 hours including 9 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Computation and automated reasoning”, 6 hours including 4.5 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Knowledge of the threat: buffer overflow attack”, 15 hours including 3 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Knowledge of the threat: buffer overflow attack”, 12 hours including 6 hours of lecture, M2 - third year of the engineer degree, Télécom Bretagne, France

Master : “Theory and practice of firewalls”, 6 hours, M2 - third year of the engineer degree, Supélec, France

Master : “Theory and practice of firewalls”, 4.5 hours, M2 - post-graduate training, Supélec, France

Master : “Theory and practice of firewalls”, 3 hours, M2 - master SSI (Sécurité des systèmes d’information), Supélec, France

Master : “Tools for virtualization of operating systems”, 1.5 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Tools for virtualization of operating systems”, 1.5 hours of lecture, M2 - post-graduate training, Supélec, France

Master : “Linux for embedded systems”, 9 hours including 3 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Computability in distributed systems”, 7.5 hours including 6 hours of lecture, M2 Master research Rennes, France

Valérie Viet Triem Tong is Associate Professor at Supélec :

Licence : “Programming”, 9h, L3 - first year of the engineer degree, Supélec, France

Master : ”Computer security”, 13h30 hours including 4h30 of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Game Theory”, 20h of lecture, M1 - second year of the engineer degree, Supélec, France

Master : “Foundations of computer science”, 10h30 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Spontaneous networking”, 3h hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master : “Supervision of student project”, 4 projects, M1 - second year of the engineer degree, Supélec, France

Master : Valérie Viet Triem Tong is responsible for the module “Security of data and Infrastructure information systems”, M2 - Master research, Rennes, France (since September 2011)

Master : “Supervision of student training”, 1 training period (6 months), M2 - Supélec, France

Four PhD defenses in 2011 and eleven thesis in progress:

PhD : Mohamed Ali Ayachi, “Contributions à la détection de comportements malhonnêtes dans les réseaux ad hoc AODV par analyse de la confiance implicite”, université de Rennes 1, February 24th 2011, supervised by Christophe Bidan and Nicolas Prigent.

PhD : Jean-Marie Borello, “Etude du métamorphisme viral : modélisation, conception et détection”, université de Rennes 1, April 1st 2011, supervised by Ludovic Mé (90%) and Eric Filiol (10% - ESIEA Laval).

PhD Jonathan Christopher Demay, “Génération et évaluation de mécanismes de détection des intrusions au niveau applicatif”, Supélec, July 1st 2011, supervised by Ludovic Mé, Eric Totel, and Frédéric Tronel.

PhD : Izabela Moise, “Efficient Agreement Protocols for Asynchronous Distributed Systems (Des protocoles d’accord efficaces pour des systèmes répartis asynchrones)”, université de Rennes 1, December 12th 2011, supervised by Michel Hurfin (70%) and Jean-Pierre Le Narzul (30% - Télécom Bretagne).

PhD in progress : Radoniaina Andriatsimandefitra, “Protection de l’information dans l’environnement Android”, started in October 2011, supervised by Ludovic Mé (20%) and Valérie Viet Triem Tong (80%).

PhD in progress : Mounir Assaf, “Vérification de propriétés de sécurité par analyse statique sur des programmes C de grande taille”, started in November 2011, supervised by Ludovic Mé (20%), Eric Totel (40%), and Frédéric Tronel (40%).

PhD in progress : Georges Bossert, “Méthodologie d’évaluation des systèmes de détection d’intrusions”, started in October 2010, supervised by Ludovic Mé (20%) and Guillaume Hiet (80%).

PhD in progress : Olivier Ferrand, “Contournements des anti-virus et protection contre ces contournements”, started in June 2011, supervised by Eric Filiol (50% - ESIEA Laval) and Ludovic Mé (50%).

PhD in progress : Stéphane Geller, “Administration de politiques de sécurité reposant sur le contrôle des flux d’information”, started in October 2009, supervised by Ludovic Mé (20%) and Valérie Viet Triem Tong (80%).

PhD in progress : Ahmed Gmati, “Redefining the concept of privacy in privacy-preserving data mining”, started in December 2010, supervised by Sébastien Gambs (50%) and Michel Hurfin (50%).

PhD in progress : Geoffroy Guéguen, “Métamorphisme viral et grammaires formelles”, université de Rennes 1, started in March 2011, supervised by Sébastien Josse (50% - ESIEA Laval) and Ludovic Mé (50%).

PhD in progress : Christophe Hauser, “Détection d’intrusions dans les systèmes distribués”, started in October 2009, in coordination with Queensland University of Technology, Brisbane, Australia (Prof. Andrew Clarck), supervised bu Ludovic Mé (20%) and Frédéric Tronel (80%).

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 : Regina Marin, “Privacy protection in distributed social networks (Protection de la vie privé dans les réseaux sociaux distribués”, started in November 2011, supervised by Christophe Bidan (20%) and Guillaume Piolle (80%).

PhD in progress : Thomas Demongeot, “Protection des données utilisateur dans les web services“, Telecom Bretagne, started in September 2008, supervised by Eric Totel (50%) and Valérie Viet Triem Tong (50%).

Some members of the team also participate to the supervision of external PhD students. Sébastien Gambs is co-supervising Ai Thanh Ho (PhD student from the Université de Montréal, Canada), Mohammad Nabil Al-Aggan (PhD student from ASAP, INRIA Rennes), Miguel Nunez del Prado Cortez (PhD student from LAAS-CNRS, Toulouse), and Moussa Traore (PhD student from LAAS-CNRS, Toulouse). Christophe Bidan and Nicolas Prigent are co-supervising Akli Redjedal (PhD student from CIDER/IRISA, Rennes). Some members of the team have participated to PhD committees:

- Ludovic Mé was a member of the PhD committee (reviewer) for the PhD of Thibault Cholez entitled “Supervision des réseaux pair à pair structurés appliquée à la sécurité des contenus”, université Henri Poincaré Nancy, June 2011.
- Ludovic Mé was a member of the PhD committee (reviewer) for the PhD of Sophie Gastellier-Prevost entitled “Vers une détection des attaques de phishing et pharming côté client”, Télécom SudParis, November 2011.
- Ludovic Mé was a member of the PhD committee for the PhD of Samer Wazan entitled “Gestion de la confiance dans les infrastructures à clés publiques”, université de Toulouse - IRIT, December 2011.
- Christophe Bidan was a member of the PhD committee (reviewer) for the PhD of Claire Sondès Larafa entitled “Services AAA dans les réseaux ad hoc mobiles”, Télécom Sud-Paris, October 2011.
- Michel Hurfin was a member of the PhD committee (reviewer) for the PhD of Adrienne Tankeu Choitat entitled “Approches outillées pour le développement des systèmes interactifs intégrant les aspects sûreté de fonctionnement et utilisabilité”, université de Toulouse - IRIT, December 2011.

Knowledge dissemination is also an objective of the team:

- Ludovic Mé gave an invited talk entitled “Pourquoi nos logiciels sont-ils vulnérables ?” during the “Assises nationales de la recherche stratégique” organized by the CSFRS (Conseil Supérieur de la Formation et de la Recherche Stratégiques) in June 2011 in Paris.
- Ludovic Mé gave an invited talk entitled “Software and Networks Vulnerabilities: Why?” during the Session Internationale Asie Moyen-Orient (SIAMO) organized by “l’institut des hautes études de défense nationale (IHEDN)” in November 2011 in Paris.
- To prepare the forthcoming introduction of a new teaching speciality entitled “Informatique et Sciences du Numérique (ISN)” in high schools, Sebastien Gambs and Nicolas Prigent trained teachers and taught a course on the security topic.
- Sébastien Gambs has participated to the event “à la découverte de la recherche” (7 interventions in high schools)
- Under the supervision of the association “Math.en.Jeans”, Sébastien Gambs has interacted with high school students of Rennes and Auray about the topic “definition and quantification of anonymity”.

In January 2011, Guillaume Piolle has been awarded by the Commission nationale de l’informatique et des libertés (CNIL). His thesis entitled “Agents utilisateurs pour la protection des données personnelles : modélisation logique et outils informatiques” (Université Jean Fourier de Grenoble) has received the prize “CNIL informatique et libertés, mention spéciale du jury”.

10. Bibliography

Major publications by the team in recent years

[1] E. ANCEAUME, F. BRASILEIRO, R. LUDINARD, B. SERICOLA, F. TRONEL. *Dependability Evaluation of Cluster-based Distributed Systems*, in "International Journal of Foundations of Computer Science (IJFCS)", Aug 2011, vol. 22, n^{o} 5, p. 1123-1142.

[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] 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.

[4] S. GAMBS, B. KÉGL, E. AÏMEUR. *Privacy-preserving boosting*, in "Data Mining and Knowledge Discovery", 2007, vol. 14, n^{o} 1, p. 131-170.

[5] 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, p. 265–279.

[6] 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.

[7] G. PIOLLE, Y. DEMAZEAU. *Representing privacy regulations with deontico-temporal operators*, in "Web Intelligence and Agent Systems", Jul 2011, vol. 9, n^{o} 3, p. 209-226.

[8] G. PIOLLE. *A dyadic operator for the gradation of desirability*, in "Proc. of the 10th international conference on deontic logic in computer science (DEON'10)", Fiesole, Italy, LNAI, Springer, July 2010, vol. 6181, p. 33-49.

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

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

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] M. ALI AYACHI. *Contributions à la détection de comportements malhonnêtes dans les réseaux ad hoc AODV par analyse de la confiance implicite*, université de Rennes 1, february 2011.

[12] J.-M. BORELLO. *Etude du métamorphisme viral : modélisation, conception et détection*, université de Rennes 1, april 2011.

[13] J. C. DEMAY. *Génération et évaluation de mécanismes de détection des intrusions au niveau applicatif*, Supélec, july 2011.

[14] I. MOISE. *Efficient Agreement Protocols for Asynchronous Distributed Systems (Des protocoles d'accord efficaces pour des systèmes répartis asynchrones)*, université de Rennes 1, december 2011.

Articles in International Peer-Reviewed Journal

[15] E. ANCEAUME, F. BRASILEIRO, R. LUDINARD, B. SERICOLA, F. TRONEL. *Dependability Evaluation of Cluster-based Distributed Systems*, in "International Journal of Foundations of Computer Science (IJFCS)", Aug 2011, vol. 22, n^{o} 5, p. 1123-1142.

[16] S. GAMBS, M.-O. KILLIJIAN, M. NÚNEZ DEL PRADO CORTEZ. *Show Me How You Move and I Will Tell You Who You Are*, in "Transactions on Data Privacy", Aug 2011, vol. 4, n^{o} 2, p. 103-126.

[17] D. LE MÉTAYER, M. MAAREK, E. MAZZA, M.-L. POTET, S. FRÉNOT, V. VIET TRIEM TONG, N. CRAIPEAU, R. HARDOUIN. *Liability Issues in Software Engineering: The Use of Formal Methods to Reduce Legal Uncertainties*, in "Communications of the ACM", Apr 2011, vol. 54, n^{o} 4, p. 99-106.

[18] G. PIOLLE, Y. DEMAZEAU. *Representing privacy regulations with deontico-temporal operators*, in "Web Intelligence and Agent Systems", Jul 2011, vol. 9, n^{o} 3, p. 209-226.

International Conferences with Proceedings

[19] M. ALAGGAN, A.-M. KERMARREC, S. GAMBS. *Private similarity computation in distributed systems: from cryptography to differential privacy*, in "Proc. of the 15th International Conference On Principles Of Distributed Systems (OPODIS'11)", Toulouse, France, Dec 2011.

[20] E. ANCEAUME, C. BIDAN, G. HIET, L. MÉ, G. PIOLLE, N. PRIGENT, E. TOTEL, F. TRONEL, V. VIET TRIEM TONG, S. GAMBS, M. HURFIN. *From SSIR to CIDre: a New Security Research Group in Rennes, France*, in "Proc. of the 1st SysSec Workshop", Amsterdam, The Netherlands, Jul 2011, p. 89-92.

[21] E. ANCEAUME, Y. BUSNEL, S. GAMBS. *Characterizing the adversarial power in uniform and ergodic node sampling*, in "Proc. of the 1st Int. Workshop on Algorithms and Models for Distributed Event Processing (AIMoDEP'11)", Rome, Italy, Sep 2011, p. 12-19, http://hal.inria.fr/inria-00617866/en.

[22] E. ANCEAUME, B. SERICOLA, R. LUDINARD, F. TRONEL. *Modeling and Evaluating Targeted Attacks in Large Scale Dynamic Systems*, in "Proc. of the 41st Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2011) - The Performance and Dependability Symposium (PDS)", Hong Kong, China, Jun 2011.

[23] E. AÏMEUR, S. GAMBS, A. T. HO. *Maintaining sovereignty on personal data on social networking sites*, in "Proc of the Conference Privacy and Accountability (PATS'11)", Berlin, Germany, april 2011.

[24] M. BEN GHORBEL-TALBI, F. CUPPENS, N. CUPPENS-BOULAHIA, D. LE MÉTAYER, G. PIOLLE. *Delegation of Obligations and Responsibility*, 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, p. 197-209.

[25] J.-M. BORELLO, L. MÉ, E. FILIOL. *Dynamic Malware Detection by Similarity Measures Between Behavioral Profiles: an Introduction in French*, in "Proc. of the 6th conference on network and information systems security (SAR-SSI)", La Rochelle, France, May 2011, p. 125-132.

[26] G. BOSSERT, G. HIET, T. HENIN. *Modelling to Simulate Botnet Command and Control Protocols for the Evaluation of Network Intrusion Detection Systems*, in "Proc. of the 6th Conference on Network Architecture and Information Systems Security (SAR-SSI 2011)", La Rochelle, France, May 2011, p. 1-8.

[27] JONATHAN CHRISTOPHER. 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.

[28] T. DEMONGEOT, E. TOTEL, V. VIET TRIEM TONG, Y. LE TRAON. *Preventing data leakage in service orchestration*, in "Proc. of the 7th Int. Conference on Information Assurance and Security (IAS 2011)", Malacca, Malaysia, Dec 2011.

[29] S. GAMBS, O. HEEN, C. POTIN. *A Comparative Privacy Analysis of Geosocial Networks*, in "Proc of the 4th Int. Workshop on Security and Privacy in GIS and LBS (SPRINGL 2011)", Chicago, USA, Nov 2011.

[30] S. GELLER, C. HAUSER, F. TRONEL, V. VIET TRIEM TONG. *Information Flow Control for Intrusion Detection Derived from MAC Policy*, in "Proc. of the IEEE International Conference on Communication (ICC 2011)", Kyoto, Japan, Jun 2011.

[31] M. HURFIN, I. MOISE, J.-P. LE NARZUL. *An Adaptive Fast Paxos for Making Quick Everlasting Decisions*, in "Proc. of the 25th IEEE International Conference on Advanced Information Networking and Applications (AINA)", Biopolis, Singapore, Mar 2011, p. 208-215.

[32] M. JAUME, V. VIET TRIEM TONG, L. MÉ. *Flow based interpretation of access control: Detection of illegal information flows*, in "Proc. of the 7th International Conference on Information Systems Security (ICISS)", Kolkata, India, LNCS, Springer Verlag, Dec 2011, vol. 7093, p. 72-86.

[33] I. MOISE, M. HURFIN, L. ZEGHACHE, N. BADACHE. *Cloud-Based Support for Transactional Mobile Agents*, in "Proc. of the 7th International Symposium on Frontiers of Information Systems and Network Applications (FINA) in conjunction with the 25th IEEE International Conference on Advanced Information Networking and Applications (AINA)", Biopolis, Singapore, Mar 2011, p. 190-197.

[34] I. MOISE, M. HURFIN, J.-P. LE NARZUL, F. MAJORCZYK. *Evaluation du caractère adaptatif d'un protocole de consensus de type "Fast Paxos"*, in "Proc. of the 13es Rencontres Francophones sur les Aspects Algorithmiques de Télécommunications (AlgoTel)", Cap Estérel, France, B. DUCOURTHIAL, P. FELBER (editors), Mai 2011, http://hal.inria.fr/inria-00588203/en.

[35] K. TABIA, S. BENFERHAT, P. LERAY, L. MÉ. *Alert correlation in intrusion detection: Combining AI-based approaches for exploiting security operators' knowledge and preferences*, in "Proc. of the 3rd Workshop on Intelligent Security - Security and Artificial Intelligence (Sec-Art 2011)", Barcelona, Spain, Jul 2011, p. 42-49.

National Conferences with Proceeding

[36] I. MOISE, M. HURFIN, J.-P. LE NARZUL, F. MAJORCZYK. *Évaluation de politiques d'adaptation au risque de collisions dans un consensus de type "Fast Paxos"*, in "Proc. of the 20ièmes Rencontres francophones du parallélisme (RenPar'20)", Saint-Malo, France, Mai 2011.

[37] V. VIET TRIEM TONG, R. ANDRIATSIMANDEFITRA, S. GELLER, S. BOCHE, F. TRONEL, C. HAUSER. *Mise en oeuvre de politiques de protection des flux d'information dans l'environnement Androïd*, in "Proc. of the Computer & Electronics Security Applications Rendez-vous (C&ESAR 2011)", Rennes, France, Nov 2011.

Conferences without Proceedings

[38] E. ANCEAUME, R. LUDINARD, B. SERICOLA, F. TRONEL. *Modélisation et Evaluation des Attaques Ciblées dans un Overlay Structuré*, in "Colloque Francophone sur l Ingénierie des Protocoles (CFIP 2011)", Sainte Maxime, France, May 2011, http://hal.inria.fr/inria-00586875/en.

[39] G. AUCHER, C. BARREAU-SALIOU, G. BOELLA, A. BLANDIN-OBERNESSER, S. GAMBS, G. PIOLLE, L. VAN DER TORRE. *The Coprelobri project: the logical approach to privacy*, in "2e Atelier Protection de la Vie Privée (APVP 2011)", Sorèze, France, Jun 2011, http://hal.inria.fr/hal-00606014/en.

[40] R. LUDINARD, L. LE HENNAFF, E. TOTEL. *RRABIDS, un système de détection d'intrusion pour les applications Ruby on Rails*, in "Proc. of the Symposium sur la sécurité des technologies de l'information et des communications (SSTIC 2011)", Rennes, France, Jun 2011.

Research Reports

[41] G. BRASSARD, F. DUPUIS, S. GAMBS, A. TAPP. *An optimal quantum algorithm to approximate the mean and its application for approximating the median of a set of points over an arbitrary distance*, INRIA, June 2011, Ten pages, no figures, three algorithms.

[42] S. GAMBS, R. GUERRAOUI, H. HARKOUS, F. HUC, A.-M. KERMARREC. *Scalable and Secure Aggregation in Distributed Networks*, INRIA, November 2011.

[43] R. LUDINARD, E. TOTEL, F. TRONEL, V. NICOMETTE, M. KAANICHE, E. ALATA, R. AKROUT, Y. BACHY. *RRABIDS: ruby on rails anomaly based intrusion detection system*, LAAS, June 2011, n^{o} 11294.

Scientific Popularization

[44] G. PIOLLE. *Outils informatiques pour la protection de la vie privée*, June 2011, Interstices.

References in notes

[45] JONATHAN CHRISTOPHER. 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.

[46] 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)", 2008.

[47] L. LAMPORT. *Paxos Made Simple*, in "ACM SIGACT News", December 2001, vol. 32, n^{o} 4, p. 51–58.

[48] L. LAMPORT. *Fast Paxos*, in "Distributed Computing", 2006, vol. 19, n^{o} 2, p. 79–103.

[49] L. LAMPORT. *The part-time parliament*, in "ACM Transaction on Computer Systems", May 1998, vol. 16, n^{o} 2, p. 133–169.

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

[51] 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, p. 162–168.

[52] 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, p. pp. 299–306.

[53] 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.