IN PARTNERSHIP WITH:
CNRS

Université Rennes 1

SUPELEC (Rennes)

Activity Report 2012

Project-Team CIDRE

Confidentialité, Intégrité, Disponibilité et Répartition

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

RESEARCH CENTER
Rennes - Bretagne-Atlantique

THEME
Distributed Systems and Services

Table of contents

Project-Team CIDRE

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

Creation of the Project-Team: January 09, 2013 .

1. Members

Research Scientists

Emmanuelle Anceaume [Junior Researcher CNRS]
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]
Gilles Guette [Associate Professor Université de Rennes 1]
Guillaume Hiet [Associate Professor Supélec]
Guillaume Piolle [Assistant Professor Supélec]
Nicolas Prigent [Associate Professor Supélec]
Eric Totel [Associate Professor Supélec, HdR]
Frédéric Tronel [Associate Professor Supélec]
Valérie Viet Triem Tong [Associate Professor Supélec]

External Collaborator

Frédéric Majorczyk [External Collaborator, DGA, since November 2012]

Engineers

Izabela Moise [Engineer Inria since May 2012]
Julien Lolive [Engineer Inria until November 2012]

PhD Students

Radoniaina Andriatsimandefitra [PhD Student, université de Rennes 1, MESR grant]
Mounir Assaf [PhD Student, université de Rennes 1, CEA grant]
Georges Bossert [PhD Student, Supélec, Cifre Amossys]
Thomas Demongeot [PhD Student, Télécom Bretagne, DGA Grant]
Stéphane Geller [PhD Student, Supélec, DGA Grant]
Ahmed Gmati [PhD Student, université de Rennes 1, MESR grant]
Geoffroy Guéguen [PhD Student, université de Rennes 1, ESIEA Laval]
Christophe Hauser [PhD Student, Supélec, MESR grant]
Christopher Humphries [PhD Student, université de Rennes 1, Inria/DGA grant]
Regina Marin [PhD Student, université de Rennes 1, ARED grant]
Simon Boche [PhD Student, université de Rennes 1, ANR grant, since october 2012]
Paul Lajoie-Mazenc [PhD Student, université de Rennes 1, MESR grant, since october 2012]
Erwan Godefroy [PhD Student, université de Rennes 1, since october 2012, DGA grant]
Pierre Obame [PhD Student, université de Rennes 1, Cifre Orange, since February 2012]

Post-Doctoral Fellow

Ehab El-Salamouny [PostDoc Inria since November 2012]

Administrative Assistant

Loic Lesage [Administrative Assistant, Inria]

2. Overall Objectives

2.1. CIDRE in Brief

In the field of security and distributed systems, the CIDRE team focuses mainly on the three following topics: Intrusion Detection, Privacy Protection, and Trust Management.

3. Scientific Foundations

3.1. Introduction

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

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

By contrast with this traditional conception, we are convinced that by looking at information systems as a combination of possibly revisited basic protocols, each one specified by a set of properties such as synchronization and agreement, security properties should emerge. This vision is shared by others and in particular by Myers *et al.* [56], 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 aim 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 [59], [55]. 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 [54], [58]. 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 [57], 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 with regards 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 evaluating the resulting trade-off between privacy and utility. An engineer (Izabela Moise) is currently working on the development of a distributed version of GEPETO based on the MapReduce paradigm and the Hadoop framework, in order to make it able to deal with datasets composed of millions of mobility traces.

6. New Results

6.1. Intrusion Detection

6.1.1. Intrusion Detection based on an Analysis of the Flow Control

In 2012, we strengthened our research efforts around intrusion detection parameterized by a security policy.

In [22] we formally study information flows that occur during the executions of a system implementing a classical access control mechanism. More precisely, we detail how the generic access control model we proposed defines two sets of illegal information flows: the first set corresponds to the flows resulting from the accesses authorized by the access control policy while the second set corresponds to the information flow policy deduced from the access control policy interpretation. We show that these two sets may coincide for some policies and we propose a mechanism dedicated to illegal information flow detection that can be useful in other cases. Finally, we describe a real implementation for the Linux operating system.

In [38], we extended our previous illegal information flow detector to track network exchanges. A confidentiality policy is defined by labeling sensitive information and defining which information may leave the local system through network exchanges. Furthermore, per application profiles can be defined to restrict the sets of information each application may access and/or send through the network. An example application of this extension in the context of a compromised web browser showed that our implementation can detect a confidentiality violation when the browser attempts to leak private information to a remote host over the network.

In [30], we adapted our detection model to the Android operating system. Mobile phones nowadays evolve as data repositories in which pieces of data belong to different owners and can or must be protected by different security policies. These pieces of data are used on an open environment controlled by a non-specialist user. The dynamic monitoring of information flows is well adapted for protecting information on an embedded system as a mobile phone. Nevertheless the main difficulty relies on the definition of the information flow policy. We proposed a way to define such a policy for the Android operating system.

6.1.2. Detecting Attacks against Data in Web Applications

In [41] we present RRABIDS (Ruby on Rails Anomaly Based Intrusion Detection System) an application level intrusion detection system for applications implemented with the Ruby on Rails framework. This IDS has been developed in the context of a collaborative project funded by ANR and called DALI.

This work aims at detecting attacks against data in the context of web applications. This anomaly based IDS focuses on the modeling of the application profile in the absence of attacks (called normal 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. We showed on simple examples how the approach detects well known categories of web attacks that involve a state violation of the application, such as SQL injections. An assessment phase was performed to evaluate the accuracy of the detection provided by the proposed approach. We learned two lessons during this assessment. First this approach provides excellent results in term of false negatives. Second it demonstrates the importance of the learning phase in terms of false positives.

6.1.3. Visualization of Security Events

After having performed in the begining of the year an extensive state of the art of the current visualisation tools dedicated to security, it now clearly appears that there is an important lack of proposals in the context of security data analytics: most of the current visualization proposals build representations for real-time monitoring and only a few of them really allow the user to crawl its data sources in details. Due to this fact, we decided to focus on visualization for security data analytics.

We also built a new visualisation platform in order to lead experiments. Our new directions and the platform have been presented in [20].

6.1.4. Intrusion Detection System Assessement

In [32], we present Netzob [1], a tool dedicated to semi-automatic network protocol reverse-engineering. Such a tool is useful to understand proprietary or non-documented protocols, which is often the case in security analysis or security product assessments. Netzob leverages different algorithms from the fields of bio-informatics and automata theory to infer both the vocabulary and the grammar of undocumented protocols. The vocabulary is inferred from message sequences previously captured (network packets, function call traces, etc.) whereas the grammar inference needs a working implementation of the protocol, which is executed in a confined environment and is used as an oracle. The inferred model could be used to automatically build a client or server implementation of the protocol to generate realistic network traffic.

6.2. Privacy

6.2.1. Geoprivacy

Recent advances in geolocated capacities, secure and verified positioning techniques, ubiquitous connectivity, as well as mobile and embedded systems, have led to the development of a plethora of Location-Based Services (LBS), personalizing the services they deliver according to the location of the user querying the service. However, beyond the benefits they provide, users have started to be worried about the privacy breaches caused by such systems. Among all the Personally Identifiable Information (PII), learning the location of an individual is one of the greatest threats against privacy. In particular, an inference attack [19], can use mobility data (together with some auxiliary information) to deduce the points of interests characterizing his mobility, to predict his past, current and future locations [34] or even to identify his social network.

[1] http://www.netzob.org

In order to address and mitigate these privacy issues, within the AMORES project [31], we aim at developing an architecture for the provision of privacy-preserving and resilient collaborative services for "mobiquitous" (*i.e.*, mobile and ubiquitous) systems. The project is built around three uses-cases from the area of publication transportation: (1) dynamic carpooling, (2) real-time computation of multimodal transportation itineraries and (3) mobile social networking. Recently, we have introduced the concept of locanym [35], which corresponds to a pseudonym linked to a particular location that could be used as a basis for developing privacy-preserving LBS.

6.2.2. Privacy-enhanced Social Networks

In [49], we have introduced a new research track focusing on the protection of privacy in distributed social networks, which corresponds to the PhD thesis of Regina Paiva Melo Marin. Our first step has been a study of the needs and practices regarding privacy and personal data policies in social networking frameworks. The commonly accepted requirements for general privacy policies are evaluated with respect to the corresponding notions found in European regulations, and then interpreted in the context of social networking applications. One of the main finding of this study is that some of these requirements are not met by the existing social networks (be they widely used or in development, centralized or distributed, focusing on personal data monetization or on user privacy). The concept of *purpose*, as well as the associated notions of minimization, finality and proportionality, in particular, appears to be insufficiently described in the various policy models. Finally, we have proposed a set of minimal requirements that a privacy policy framework designed for distributed social networks should meet for it to be sufficiently expressive with regards to the current regulations.

6.2.3. Privacy Enhancing Technologies

Even though they integrate some blind submission functionalities, current conference review systems, such as EasyChair and EDAS, do not fully protect the privacy of authors and reviewers, in particular from the eyes of the program chair. As a consequence, their use may cause a lack of objectivity in the decision process. To address this issue, we have proposed in collaboration with researchers from the Université de Montréal, P3ERS (for Privacy-Preserving PEer Review System) [17], a distributed conference review system based on group signatures, which aims at preserving the privacy of all participants involved in the peer review process. One of the main ideas of P3ERS is to ensure the privacy of both the authors and the reviewers (and this even from the point of view of the conference provider and the conference chair) by using two different groups of users. In particular, the authors can submit anonymized papers on behalf of the author group to the program chair, who then dispatches the papers according to the declared skills of the reviewer group members in an oblivious manner. In this way, the program chair knows neither the identity of the authors (until a paper is accepted, if it is) nor the correspondence between papers and reviewers.

In [25], we have considered the setting in which the profile of a user is represented in a compact way, as a Bloom filter, and the main objective is to privately compute in a distributed manner the similarity between users by relying only on the Bloom filter representation. In particular, our main objective is to provide a high level of privacy with respect to the profile even if a potentially unbounded number of similarity computations take place, thus calling for a non-interactive mechanism. To achieve this, we have proposed a novel non-interactive differentially private mechanism called BLIP (for BLoom-and-flIP) for randomizing Bloom filters. This approach relies on a bit flipping mechanism and offers high privacy guarantees while maintaining a small communication cost. Another advantage of this non-interactive mechanism is that similarity computation can take place even when the user is offline, which is impossible to achieve with interactive mechanisms. Another contribution of this work is the definition of a probabilistic inference attack, called the "Profile Reconstruction attack", that can be used to reconstruct the profile of an individual from his Bloom filter representation. More specifically, we provided an analysis of the protection offered by BLIP against this profile reconstruction attack by deriving an upper and lower bound for the required value of the differential privacy parameter ϵ.

In order to contribute to solve the personalization/privacy paradox, we have proposed a privacy-preserving architecture for one of the state of the art recommendation algorithm, Slope One [36]. More precisely, we designed SlopPy (for *Slope One with Privacy*), a privacy-preserving version of Slope One in which a user

never releases directly his personal information (*i.e.*, his ratings). Rather, each user first perturbs locally his information by applying a Randomized Response Technique before sending this perturbed data to a semi-trusted entity responsible for storing it. While there is a trade-off to set between the desired privacy level and the utility of the resulting recommendation, our preliminary experiments clearly demonstrate that SlopPy is able to provide a high level of privacy at the cost of a small decrease of utility.

A privacy-preserving identity card is a personal device device that allows its owner to prove some binary statements about himself (such as his right of access to some resources or a property linked to his identity) while minimizing personal information leakage. As a follow-up of previous works, we have discussed a taxonomy of threats against the card. Finally, we also proposed for security and cryptography experts some novel challenges and research directions raised by the privacy-preserving identity card [50].

6.2.4. Privacy and Data Mining

In [44], [33], we have introduced a novel inference attack that we coined as the reconstruction attack whose objective is to reconstruct a probabilistic version of the original dataset on which a classifier was learnt from the description of this classifier and possibly some auxiliary information. In a nutshell, the reconstruction attack exploits the structure of the classifier in order to derive a probabilistic version of dataset on which this model has been trained. Moreover, we proposed a general framework that can be used to assess the success of a reconstruction attack in terms of a novel distance between the reconstructed and original datasets. In case of multiple releases of classifiers, we also gave a strategy that can be used to merge the different reconstructed datasets into a single coherent one that is closer to the original dataset than any of the simple reconstructed datasets. Finally, we gave an instantiation of this reconstruction attack on a decision tree classifier that was learnt using the algorithm C4.5 and evaluated experimentally its efficiency. The results of this experimentation demonstrate that the proposed attack is able to reconstruct a significant part of the original dataset, thus highlighting the need to develop new learning algorithms whose output is specifically tailored to mitigate the success of this type of attack.

6.2.5. Privacy and Web Services

We have proposed [18] a new model of security policy based for a first part on our previous works in information flow policy and for a second part on a model of Myers and Liskov. This new model of information flow serves web services security and allows a user to precisely define where its own sensitive pieces of data are allowed to flow through the definition of an information flow policy. A novel feature of such policy is that they can be dynamically updated, which is fundamental in the context of web services that allow the dynamic discovery of services. We have also presented an implementation of this model in a web services orchestration in BPEL (Business Process Execution Language) [18].

6.3. Trust

6.3.1. Privacy Preserving Digital Reputation Mechanism

Digital reputation mechanisms have recently emerged as a promising approach to cope with the specificities of large scale and dynamic systems. Similarly to real world reputation, a digital reputation mechanism expresses a collective opinion about a target user based on aggregated feedback about his past behavior. The resulting reputation score is usually a mathematical object, *e.g.* a number or a percentage. It is used to help entities in deciding whether an interaction with a target user should be considered. Digital reputation mechanisms are thus a powerful tool to incite users to trustworthily behave. Indeed, a user who behaves correctly improves his reputation score, encouraging more users to interact with him. In contrast, misbehaving users have lower reputation scores, which makes it harder for them to interact with other users. To be useful, a reputation mechanism must itself be accurate against adversarial behaviors. Indeed, a user may attack the mechanism to increase his own reputation score or to reduce the reputation of a competitor. A user may also free-ride the mechanism and estimate the reputation of other users without providing his own feedback. From what has been said, it should be clear that reputation is beneficial in order to reduce the potential risk of communicating with almost or completely unknown entities. Unfortunately, the user privacy may easily be jeopardized by

reputation mechanisms which is clearly a strong argument to compromise the use of such a mechanism. Indeed, by collecting and aggregating user feedback, or by simply interacting with someone, reputation systems can be easily manipulated in order to deduce user profiles. Thus preserving user privacy while computing robust reputation is a real and important issue that we address in ou work [48], [52]. Our proposition combines techniques and algorithms coming from both distributed systems and privacy research domains. Specifically, we propose to self-organize agents over a logical structured graph, and to exploit properties of these graphs to anonymously store interactions feedback. By relying on robust reputation scores functions we tolerate ballot stuffing, bad mouthing and repudiation attacks. Finally, we guarantee error bounds on the reputation estimation score.

6.4. Other Topics Related to Security and Distributed Computing

6.4.1. Network Monitoring and Fault Detection

Monitoring a system is the ability of collecting and analyzing relevant information provided by the monitored devices so as to be continuously aware of the system state. However, the ever growing complexity and scale of systems makes both real time monitoring and fault detection a quite tedious task. Thus the usually adopted option is to focus solely on a subset of information states, so as to provide coarse-grained indicators. As a consequence, detecting isolated failures or anomalies is a quite challenging issue. We propose in [29] to address this issue by pushing the monitoring task at the edge of the network. We present a peer-to-peer based architecture, which enables nodes to adaptively and efficiently self-organize according to their ”health” indicators. By exploiting both temporal and spatial correlations that exist between a device and its vicinity, our approach guarantees that only isolated anomalies (an anomaly is isolated if it impacts solely a monitored device) are reported on the fly to the network operator. We show that the end-to-end detection process, *i.e.*, from the local detection to the management operator reporting, requires a logarithmic number of messages in the size of the network.

6.4.2. Metrics Estimation on Very Large Data Streams

In [27] and [28], we consider the setting of large scale distributed systems, in which each node needs to quickly process a huge amount of data received in the form of a stream that may have been tampered with by an adversary. In this situation, a fundamental problem is how to detect and quantify the amount of work performed by the adversary. To address this issue, we propose AnKLe (for Attack-tolerant eNhanced Kullback-Leibler divergence Estimator), a novel algorithm for estimating the KL divergence of an observed stream compared to the expected one. AnKLe com- bines sampling techniques and information-theoretic methods. It is very efficient, both in terms of space and time complexities, and requires only a single pass over the data stream. Experimental results show that the estimation provided by AnKLe remains accurate even for different adversarial settings for which the quality of other methods dramatically decreases. In [26], considering n as the number of distinct data items in a stream, we show that AnKLe is an (ε, δ)-approximation algorithm with a space complexity $\widetilde{\mathcal{O}}(\frac{1}{\varepsilon} + \frac{1}{\varepsilon^2})$ bits in “most” cases, and $\widetilde{\mathcal{O}}(\frac{1}{\varepsilon} + \frac{n-\varepsilon^{-1}}{\varepsilon^2})$ otherwise. To the best of our knowledge, an approximation algorithm for estimating the Kullback-Leibler divergence has never been analyzed before. We go a step further by considering in [51] the problem of estimating the distance between any two large data streams in small-space constraint. This problem is of utmost importance in data intensive monitoring applications where input streams are generated rapidly. These streams need to be processed on the fly and accurately to quickly determine any deviance from nominal behavior. We present a new metric, the *Sketch ☆-metric*, which allows to define a distance between updatable summaries (or sketches) of large data streams. An important feature of the *Sketch ☆-metric* is that, given a measure on the entire initial data streams, the *Sketch ☆-metric* preserves the axioms of the latter measure on the sketch (such as the non-negativity, the identity, the symmetry, the triangle inequality but also specific properties of the f-divergence or the Bregman one). Extensive experiments conducted on both synthetic traces and real data sets allow us to validate the robustness and accuracy of the *Sketch ☆-metric*.

6.4.3. Robustness Analysis of Large Scale Distributed Systems

In [14] we present an in-depth study of the dynamicity and robustness properties of large-scale distributed systems, and in particular of peer-to-peer systems. When designing such systems, two major issues need to be faced. First, population of these systems evolves continuously (nodes can join and leave the system as often as they wish without any central authority in charge of their control), and second, these systems being open, one needs to defend against the presence of malicious nodes that try to subvert the system. Given robust operations and adversarial strategies, we propose an analytical model of the local behavior of clusters, based on Markov chains. This local model provides an evaluation of the impact of malicious behaviors on the correctness of the system. Moreover, this local model is used to evaluate analytically the performance of the global system, allowing to characterize the global behavior of the system with respect to its dynamics and to the presence of malicious nodes and then to validate our approach. We complete this work by considering in [13], the behavior of a stochastic system composed of several identically distributed, but non independent, discrete-time absorbing Markov chains competing at each instant for a transition. The competition consists in determining at each instant, using a given probability distribution, the only Markov chain allowed to make a transition. We analyze the first time at which one of the Markov chains reaches its absorbing state. When the number of Markov chains goes to infinity, we analyze the asymptotic behavior of the system for an arbitrary probability mass function governing the competition. We give conditions for the existence of the asymptotic distribution and we show how these results apply to cluster-based distributed systems when the competition between the Markov chains is handled by using a geometric distribution.

6.4.4. Secure Multiparty Computation in Dynamic Networks

In [37] in collaboration with researchers from EPFL, we consider the problem of securely conducting a poll in synchronous dynamic networks equipped with a Public Key Infrastructure (PKI). Whereas previous distributed solutions had a communication cost of $O(n^2)$ in an n nodes system, we present SPP (Secure and Private Polling), the first distributed polling protocol requiring only a communication complexity of $O(nlog^3 n)$, which we prove is near-optimal. Our protocol ensures perfect security against a computationally-bounded adversary, tolerates $(1/2?\epsilon)n$ Byzantine nodes for any constant $1/2 > \epsilon > 0$ (not depending on n), and outputs the exact value of the poll with high probability. SPP is composed of two sub-protocols, which we believe to be interesting on their own: SPP-Overlay maintains a structured overlay when nodes leave or join the network, and SPP-Computation conducts the actual poll. We validate the practicality of our approach through experimental evaluations and describe briefly two possible applications of SPP: (1) an optimal Byzantine Agreement protocol whose communication complexity is $\Theta(nlogn)$ and (2) a protocol solving an open question of King and Saia in the context of aggregation functions, namely on the feasibility of performing multiparty secure aggregations with a communication complexity of $o(n^2)$.

6.4.5. Agreement Problems in Unreliable Systems

In distributed systems, replication techniques are used to mask occurrences of accidental and malicious failures. To coordinate efficiently the different replicas, different approaches can be adopted (state machine mechanisms, group communication services, ...). Most solutions are based on agreement protocols. 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. We have proposed a protocol designed to solve several consecutive consensus instances in an asynchronous distributed system prone to crash failures and message omissions. The protocol follows the Paxos approach and integrates two different optimizations to reduce the latency of learning a decision value. As one optimization is risky, dynamics triggering criterion are defined to check at runtime if the context seems to be favorable or not. The proposed protocol 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 [39] focus on the impact of the prediction of collisions (i.e. , the cases where the use of the risky optimization is counterproductive).

We consider also the problem of approximate consensus in mobile ad hoc networks in the presence of Byzantine nodes. Each node begins to participate by providing a real number called its initial value. Eventually

all correct nodes must obtain final values that are different from each other within a maximum value denoted ϵ (convergence property) and must be in the range of initial values proposed by the correct nodes (validity property). Due to nodes' mobility, the topology is dynamic and unpredictable. In [40], [53], we propose an approximate Byzantine consensus protocol which is based on the linear iteration method. Each node repeatedly executes rounds. During a round, a node moves to a new location, broadcasts its current value, gathers values from its neighbors, and possibly updates its value. In our protocol, nodes are allowed to collect information during several consecutive rounds: thus moving gives them the opportunity to gather progressively enough values. An integer parameter Rc is used to define the maximal number of rounds during which values can be gathered and stored while waiting to be used. A novel sufficient and necessary condition guarantees the final convergence of the consensus protocol. At each stage of the computation, a single correct node is concerned by the requirement expressed by this new condition (the condition is not universal as it is the case in all previous related works). Moreover the condition considers both the topology and the values proposed by correct nodes. If less than one third of the nodes are faulty, the condition can be satisfied. We are working on mobility scenarios (random trajectories, predefined trajectories, meeting points) to assert that the condition can be satisfied for reasonable values of Rc.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- **DGA PEA (Exploratory Study Program) contract (2011-2012): « PREVA - Security of the ad hoc routing protocols in the context of future tactical military networks »**

  During the DGA-funded PREVA project ending in January 2013, we analyzed secure ad hoc routing in the context of military tactical networks. We first analyzed which routing protocols were the most suited for each type of tactical networks (Joint and Sub-Joint Tactical Groups, vehicular ad hoc networks, Futur Integrated Soldier Technologies (FIST) troopers and sensor networks assisting the troopers). We also considered the various security technologies (both crypto-based proactive mechanisms and intrusion detection-based reactive mechanims) that could be used to protect each selected ad hoc routing protocols. Finally, we built a demonstrator implementing the various selected protocols and security mechanisms.

  This study is led in cooperation with OPEN, an IT service provider located in Rennes.

- **DGA contract (2012-2013): « CAPALID »**

  The CAPALID project aims at building a state of the art of off-the-shelf solutions for supervision systems in distributed environments. Our work was at first to make a state of the art of the research activities for Intrusion detection systems, correlation systems and visualization systems. On a second phase, the goal was to define an assessment methodology of these types of tools. Finally, this methodology will be applied by Amossys, our partner in the project, to evaluate the best off-the-shelf tools that have been retained in the context of the project. This study is led in cooperation with Amossys, a SME located in Rennes.

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

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

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

7.2. Bilateral Grants with Industry

- **Amossys: « Evaluation of intrusion detection mechanisms »**

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

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

  Pierre Obame is doing his PhD thesis in the context of this cooperation with Orange Labs at Rennes. The theme of this project is to propose a distributed storage system dedicated to users who access Internet via a Digital Subscriber Line (DSL) technology. This system aims at guaranteeing data availability, persistency, and low access latency by fully exploiting millions of home gateways and the hundreds of Points of Presence (POP) of an Internet Service Provider (ISP) infrastructure.

- **DGA-MI: « Security events visualization »**

  The PhD of Christopher Humphries is done in the context of a cooperation with DGA-MI. Due to the generalization of logging systems, security analysts are now overwhelmed by data when they want to obtain more informations. Manual inspection is clearly not possible anymore, and automated systems such as correlators are showing their limits. Visualization is a promising field. Visualization allows to build concise and often aesthetic representations of systems and events. In this project, we aim at proposing ways to evaluate current visualization solutions and to propose new ones dedicated to security events analysis, for instance for forensic purposes.

- **DGA-MI: « Alerts Correlation Taking the Context Into Account»**

  The PhD of Erwan Godefroy is done in the context of a cooperation with DGA-MI. This PhD just started in November 2012.

8. Partnerships and Cooperations

8.1. Regional Initiatives

- **Région Bretagne ARED grant:** the PhD of Regina Marin on privacy protection in distributed social networks is supported by a grant from the Région Bretagne.

- **Labex COMINLAB contract (2012-2015): « POSEIDON »**

  POSEIDON deals with the protection of data in outsourced or mutualized systems such as cloud computing and peer-to-peer networks. While these approaches are very promising solutions to outsource storage space, contents, data and services, they also raise serious security and privacy issues since users lose their sovereignty on their own data, services and systems. Instead of trying to prevent the bad effects of the cloud and of peer-to-peer systems, the main objective of the POSEIDON project is to turn benefit from their main characteristics (distribution, decentralization, multiple authorities, etc.) to improve the security and the privacy of the users' data, contents and services.

  This study is conducted in cooperation with Télécom Bretagne and Université de Rennes 1.

- **Labex COMINLAB contract (2012-2015): « SecCloud »**

  Nowadays attacks targeting the end-user and especially its web browser constitute a major threat. Indeed web browsers complexity has been continuously increasing leading to a very large attack surface. Among all possible threats, we tackle in the context of the SecCloud project those induced by client-side code execution (for example javascript, flash or html5).

  Existing security mechanisms such as os-level access control often only rely on users identity to enforce the security policy. Such mechanisms are not sufficient to prevent client-side browser attacks as the web browser is granted the same privileges as the user. Consequently, a malicious code can

perform every actions that are allowed to the user. For instance, it can read and leak user private data (credit cart numbers, registered passwords, email contacts, etc.) or download and install malware.

One possible approach to deal with such threats is to monitor information flows within the web browser in order to enforce a security information flow policy. Such a policy should allow to define fine-grained information flow rules between user data and distant web sites. This implies to propose an approach and to design and implement a mechanism that can handle both OS-level and browser-level information flows.

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

This study is conducted in cooperation with other Inria Teams (Ascola and Celtique).

8.2. National Initiatives

8.2.1. ANR

- **ANR ARPEGE Project: DALI (2009-2012) - http://dali.kereval.com/**

  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. This project is led by Kereval and involves Supélec, Télécom Bretagne, and the LAAS/ CNRS. Our activity consists in the design and development of a mechanism to discover invariants in web applications. These invariants are weaved in the application source code, in order to be dynamically checked at runtime. The approach has been applied on an e-commerce application. The assessment phase which has been carried out by the LAAS-CNRS demonstrated a good detection rate of our mechanisms. This projet has been evaluated during the ANR « Grand Colloque STIC » January 2012 and has reached an end in June 2012.

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

  Situated in the mobiquitous context characterized by a high mobility of individuals, most of them wearing devices capable of geolocation (smartphones or GPS-equipped cars), the AMORES project is built around three use-cases related to mobility, namely (1) dynamic carpooling, (2) real-time computation of multi-modal transportation itineraries and (3) mobile social networking. For these three use cases, the main objective of the AMORES project is to define and develop geo-communication primitives at the middleware level that can offer the required geo-located services, while at the same time preserving the privacy of users, in particular with respect to their location (notion of geo-privacy). Within this context, we study in particular the problem of anonymous routing and the design of a key generation protocol tied to a particular geographical location. Each of these services can only work through cooperation of the different entities composing the mobile network. Therefore, we also work on the development of mechanisms encouraging entities to cooperate together in a privacy-preserving manner. The envisioned approach consists in the definition of generic primitives such as the management of trust and the incentive to cooperation. This project is joint between the Université de Rennes 1, Supélec, LAAS-CNRS, Mobigis and Tisséo. The research project AMORES received the Innovation Award at the Toulouse Space Show last June. Simon Boche and Paul Lajoie-Mazenc are doing their PhD in the context of this project.

- **ANR INS Project: LYRICS (2011-2014) - http://projet.lyrics.orange-labs.fr/**

  With the fast emergence of the contactless technology such as NFC, mobile phones will soon be able to play the role of e-tickets, credit cards, transit pass, loyalty cards, access control badges, e-voting tokens, e-cash wallets, etc. In such a context, protecting the privacy of an individual becomes a particularly challenging task, especially when this individual is engaged during her daily

life in contactless services that may be associated with his identity. If an unauthorized entity is technically able to follow all the digital traces left behind during these interactions then that third party could efficiently build a complete profile of this individual, thus causing a privacy breach. Most importantly, this entity can freely use this information for some undesired or fraudulent purposes ranging from targeted spam to identity theft. The objective of LYRICS (ANR INS 2011) is to enable end users to securely access and operate contactless services in a privacy-preserving manner that is, without having to disclose their identity or any other unnecessary information related to personal data. Within this project, we work mainly on the privacy analysis of the risks incurred by users of mobile contactless services as well as on the development of the architecture enabling the development of privacy-preserving mobile contactless services. The project is joint between France Télécom, Atos Wordline, CryptoExperts, ENSI Bourges, ENSI Caen, MoDyCo, Oberthur Technologies, NEC Corporation, Microsoft and Université de Rennes 1.

8.2.2. Inria Large-scale Actions

- **CAPPRIS (2012-2016)**

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

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

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

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

  Three major application domains have been identified as interesting experimentation fields for this work: online social networks, location-based services and electronic health record systems. Each of these three domains brings specific privacy-related issues. The aim of the collaboration is to apply the techniques developed to the application domains in a way that promotes the notion of privacy by design, instead of simply considering them as a form of privacy add-ons on the top of already existing technologies. CAPPRIS is a joint project between Inria, CNRS, Université de Rennes 1, Supélec, Université de Namur, Eurecom, and Université de Versailles.

8.2.3. Research mission "Droit et Justice"

- **Droit à l'Oubli (2012-2014)**

  The "right to be forgotten" can be viewed as a consequence and an extension of the right to privacy and to personal data protection, emphasized by the inherent difficulty to erase any given information from the omnipresent digital world. The French ministry of Justice has launched two twin projects (one of which is the DAO project), in order to explore the possible legal definitions of a "right to

be forgotten". Even though there are no legal foundations for such a right in France at the moment, the concept is already known from the general public and is also present in courts. Furthermore, individuals expect to be protected by such a right, thus it is important to understand why, how, in which circumstances and to which extent this new right may apply before envisioning a legal notion defining it. The DAO project involves a major legal component, a sociological survey and a technical study. In a nutshell, the legal part explores the possible boundaries and requirements of a right to be forgotten with respect to labor law, civil statuses, personal data protection, legal prescription and IT law. The sociological survey aims at understanding the root causes making people build a desire for forgetfulness in others. Finally, the objective of the computer science part is to elaborate a state of the art of the techniques that could be used to enforce a right to be forgotten in practice in the digital world. The expected output of the project as a whole is a detailed recommendation about whether an independent legislation proposal for the right to be forgotten would be justified, and how it should be done. The project is joint between Université de Rennes 1, Inria and Supélec.

8.2.4. Competitivity Clusters

The following projects are recognized by the Images & Réseaux cluster:

- DALI (ANR ARPEGE 2008): http://www.images-et-reseaux.com/en/content/dali
- AMORES (ANR INS 2011): http://www.images-et-reseaux.com/en/content/amores

8.3. European Initiatives

8.3.1. Collaborations in European Programs, except FP7

Program: EIT KICs

Project acronym: EIT ICT Labs

Project title: action line « Security, Privacy and Trust in the Information Society »

Duration: 2012-

Coordinator: Sébastien Gambs (until September 2012 and since then Guido Bertoni, STMictoelectronics)

Abstract: Information Technologies have invaded many aspects of people's daily lives, creating new possibilities but also raising concerns in term of privacy and trust. Protecting the privacy of individuals is one of the main challenges of the Information Society but it is difficult to achieve as individuals constantly leave digital traces of their lives, often without even being aware of this. 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. From the technology viewpoint, a number of Privacy Enhancing Technologies (PETs) and Privacy Aware Architectures have been proposed. So far, these technologies have not stimulated a strong public interest and are not widely used yet. However, the European Commission is putting forward the "privacy by design" principle, which integrates the privacy issues in the design phase of a system or application.

Security and trust can be seen as complementary requirements to privacy. Large scale adoption of digital devices, like in eHealth and smart cities, requires trustworthy products and communication. These requirements are not (always) completely understood and off-the-shelf solutions could not fulfill the security, trust and privacy needs. There is a large gap between what is applied, usability requirements and the right level of security. This gap represents a strategic opportunity where European players have a recognized know-how and where leadership should be leveraged and nurtured.

While the action line was originally intended to focus on privacy (created by a joint effort from Sébastien Gambs, Daniel Le Métayer and Claude Castelluccia from Inria Rhône-Alpes), its scope was recently extended to include security and trust thus being renamed as "Security, Privacy and Trust in the Information Society". In 2012, a "location privacy" activity leaded by Sébastien Gambs

was created that involves CIDRE and other partners (namely KTH, Alcatel-Lucent, University of Trento, Inria Rhône-Alpes, Nokia) coming from 3 different nodes of EIT ICT labs. An engineer funded by the project (Izabela Moise) is currently working on the development of a distributed version of GEPETO based on the MapReduce paradigm and the Hadoop framework, in order to make it able to deal with datasets composed of millions of mobility traces. In 2013, this activity will be extended to also address the issues of privacy and security for location-based services, thus being renamed "Security and privacy for location-based services".

8.3.2. Collaborations with Major European Organizations

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.

Our activity focuses on a 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. From November 2011 until November 2012, Julien Lolive has worked on the project as an engineer. Izabela Moise has also joined the Quaero project since October 2012.

8.4. International Initiatives

8.4.1. Inria International Partners

CANADA: Sébastien Gambs was co-supervising Ai Thanh Ho, a PhD student from the Université de Montréal with whom he has been actively collaborating since many 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 successfully defend her PhD thesis in June 2012.

AUSTRALIA: With Queensland University of Technology (QUT, Brisbane) we cooperate to study policy-based intrusion detection problems. 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. From February 2011 to February 2012, Christopher Hauser has worked in Brisbane. His one year visit was supported by a grant from Rennes Métropole.

STIC Algeria (Program Inria/DGRST, 2011-2013): This cooperation project is managed by Adlen Ksentini (member of the Inria Project DIONYSOS, Rennes) and Abdelouahid Derhab (member of CERIST, Centre de Recherche sur l'Information Scientifique et Technique, Alger). This collaboration aims at defining new protocols for data collecting in Wireless Sensor Networks, and evaluate them with the senslab platform. After validating the proposed protocols, CERIST intends to deploy them in the context of the project (Algerian) "Sensirrig", which aims at using sensors for agricultural irrigation. With L. Zeghache and N. Badache (CERIST), we investigate the use of Mobile Transactional Agents.

8.5. International Research Visitors

8.5.1. Visits of International Scientists

CANADA: Jean-Marc Robert, Professor Professor of ETS (École de Technologie Supérieure) at Montreal was visiting us during a period of four months (September 2012 - December 2012). The joint works focus mainly on privacy in pro-active ad hoc routing protocols. Based on the OLSR protocol, we have proposed a privacy preserving ad hoc proactive routing protocol that preserves the anonymity of the participants, and assure the unlinkability of two different packet flows between two given nodes.

8.5.2. Internships

CHINA: Chuanyou Li, PhD student at Southeast University (Nanjing, China) was 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.

9. Dissemination

9.1. Scientific Animation

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 « 7ème Conférence sur la Sécurité des Architectures Réseaux et Systèmes d'Information (SAR-SSI 2012) » held in May 2012 in Cabourg, France (https://sarssi2012.greyc.fr/).
- member of the steering committee of the « 15th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2012) » held in September 2012 in Amsterdam, The Netherlands (http://www.raid2012.org/).
- member of the steering committee of the « Computer & Electronics Security Applications Rendez-vous - Cloud and Security, threat or opportunity ? (C&ESAR 2012) » held in November in Rennes, France (http://www.cesar-conference.org/).
- member of the program committee of the « 5th SETOP International Workshop on Autonomous and Spontaneous Security (SETOP 2012) » held in September 2012 in Pisa, Italy (http://sesar.dti.unimi.it/SETOP2012/).
- member of the program committee of the « 7th International Conference on Risks and Security of Internet and Systems (CRiSIS 2012) » held in October 2012 in Cork, Ireland (http://4c.ucc.ie/crisis2012/).
- member of a DGA's scientific committee.

Emmanuelle Anceaume acts as a

- member of the International Evaluation Panel of the Call 2012 for the topic Context- and Content-Adaptive Communication Networks of the CHIST-ERA, a European Network of Research
- member of the program committee of the « 11th IEEE International Conference on Ubiquitous Computing and Communications (IUCC 2012) » held in June 2012 in Liverpool, England (http://scim.brad.ac.uk/~hmibrahi/IUCC2012/).
- member of the program committee of the « 11th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom-2012) » held in June 2012 in Liverpool, England (http://www.scim.brad.ac.uk/~hmibrahi/TrustCom2012/).

- member of the program committee of the « 7th International Conference on Frontier of Computer Science and Technology (FCST-12) » held in November 2012 in Suzhou, China (http://trust.csu.edu.cn/conference/fcst2012/).
- member of the program committee of the « 9th FTRA International Conference on Secure and Trust Computing, data management, and Applications (STA 2012) » held in September 2012 in Gwangju, Korea (http://www.ftrai.org/sta2012/).
- external reviewer for the IEEE Transactions on Parallel and Distributed Systems journal, the ACM Transactions on Autonomous and Adaptive System journal, and the ACM Transactions on Systems, Man, and Cybernetics (Part A: Systems and Humans).

Christophe Bidan acts as a

- member of the program committee of the « 7th Conference on Network Architectures and Information Systems Security (SAR-SSI 2012) » held in May 2012 in Cabourg, France (https://sarssi2012.greyc.fr/).
- member of the program committee of the « 8th International Conference on Security and Privacy in Communication Networks (SecureComm 2012) » held in September 2012 in Padua, Italy (http://securecomm.org/2012/show/home).
- member of the program committee of the « 5th International Workshop on Autonomous and Spontaneous Security (SETOP 2012) » held in September 2012 in Pisa, Italy (http://sesar.dti.unimi.it/SETOP2012/).

Sébastien Gambs acts as a

- leader of the action line on « Privacy, Security and Trust in the Information Society » from EIT ICT labs (until September 2012).
- 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 editorial board of International Journal of Privacy and Health Information Management (http://www.igi-global.com/journal/international-journal-privacy-health-information/41027).
- co-organizer of a panel on « Location-based services and privacy: are we moving in the right direction ? (6th International Conference on Computers, Privacy and Data Protection - CPDP 2012) » held in January 2012 in Brussels, Belgium (http://www.cpdpconferences.org/thursday26january.html).
- member of the organization committee of the « 3ème Atelier sur la Protection de la Vie Privée (APVP 2012) » held in June 2012 in Ile de Groix, France (http://www.irisa.fr/prive/sgambs/apvp2012.html).
- member of the program committee of the « 3ème Atelier sur la Protection de la Vie Privée (APVP 2012), » held in June 2012 in Ile de Groix, France (http://www.irisa.fr/prive/sgambs/apvp2012.html).
- member of the 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).
- member of the program committee of the « Workshop on Privacy and Anonymity for the Digital Economy (PADE 2012) » held in June 2012 in London, United Kingdom (http://pade12.mytestbed.net/).
- member of the program committee of the « 10th International Conference on Privacy, Security and Trust (PST 2012) » held in July 2012 in Paris, France (http://www.unb.ca/pstnet/pst2012/).
- member of the program committee of the « 1st International Workshop on Citizen Sensor Networks (CitiSen 2012) » held in August 2012 in Montpellier, France (https://sites.google.com/site/citisen2012/).

- member of the program committee of the « 13th Conference on Communications and Multimedia Security (CMS 2012) » held in September 2012 in Canterbury, United Kingdom (http://sec.cs.kent.ac.uk/cms2012/?page=main).
- member of the program committee of the « 7th International Workshop on Data Privacy Management (DPM 2012) » held in September 2012 in Pisa, Italy (http://www-ma4.upc.edu/DPM2012/).
- member of the program committee of the « 5th Symposium on Foundations and Practice of Security (FPS 2012) » held in October 2012 in Montréal, Canada (http://conferences.telecom-bretagne.eu/fps2012/).
- member of the program committee of the « 5th ACM SIGSPATIAL International Workshop on Location-Based Social Networks (LBSN 2012) » held in November 2012 in Redondo Beach, USA (http://www.cs.umb.edu/~gghinita/LBSN12/).
- external reviewer for GeoProcessing 2012 (Conference on Advanced Geographic Information Systems, Applications, and Services), CCS 2012 (19th ACM Conference on Computer and Communications Security), the Neural Computation journal, IEEE Transactions on Parallel and Distributed Systems, Journal of Parallel and Distributed Computing and Information Systems.

Gilles Guette acts as a

- 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 (https://www.sstic.org/2012/news/).

Guillaume Hiet acts as a

- member of the program committee of the « 15th International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2012) » held in September 2012 in Amsterdam, The Netherlands (http://www.raid2012.org/).

Michel Hurfin acts as a

- member of the editorial board of the « Springer Journal of Internet Services and Applications » (http://www.springer.com/computer/communications/journal/13174).
- member of the program committee of the « 3rd International Workshop on Interconnections of Wireless Sensor Networks (IWSN 2012) » held in May 2012 in Hangzhou, China (http://iwsn2012.gforge.uni.lu/index.html).
- member of the program committee of the « 4th International Workshop on Workflow Management in Service and Cloud Computing (WMSC2012) » held in November 2012 in Xiangtan, China (http://kpnm.hnust.cn/confs/wmsc2012).
- 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 Elsevier Journal of Computer and System Sciences (JCSS) and PODC 2012 (31st ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing).
- member of the Inria COST-GTAI (reviewer for ADT submissions and project proposal).

Guillaume Piolle acts as a

- member of the CERNA (*Commission de réflexion sur l'éthique de la recherche en sciences et technologies du numérique d'Allistene*), ethical committee for the French research in digital sciences and technologies.
- member of the organization committee of the « 3ème Atelier sur la Protection de la Vie Privée (APVP 2012), » held in June 2012 in Ile de Groix, France (http://www.irisa.fr/prive/sgambs/apvp2012.html).

- member of the program committee of the « 3ème Atelier sur la Protection de la Vie Privée (APVP 2012), » held in June 2012 in Ile de Groix, France (http://www.irisa.fr/prive/sgambs/apvp2012.html).
- member of the program committee of the « 1st Workshop on Information Hiding Techniques for Internet Anonymity and Privacy (IHTIAP 2012) » held in June 2012 in Venice, Italy (http://www.iaria.org/conferences2012/IHTIAP.html).
- member of the program committee of the « 1st Workshop on Rights and Duties of Autonomous Agents (RDA2 2012) » held in August 2012 in Montpellier, France (https://rda2-2012.greyc.fr/).
- external reviewer for Interstices (online peer-reviewed journal of Inria - http://interstices.info/) and RAID 2012 (15th International Symposium on Research in Attacks, Intrusions and Defenses).

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 2012) » held in June 2012 in Rennes, France (https://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 (https://www.sstic.org/2012/news/).
- member of the program committee of the « 5th SETOP International Workshop on Autonomous and Spontaneous Security (SETOP 2012) » held in September 2012 in Pisa, Italy (http://sesar.dti.unimi.it/SETOP2012/).

Eric Totel acts as a

- external reviewer for RAID 2012 (15th International Symposium on Research in Attacks, Intrusions and Defenses), and CRISIS 2012 (7th International Conference on Risks and Security of Internet and Systems).

Frédéric Tronel acts as a

- 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 (https://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 (https://www.sstic.org/2012/news/).
- external reviewer for RAID 2012 (15th International conference Recent Advances on Intrusion Detection) and PODC 2012 (31st ACM SIGACT-SIGOPS Symposium on Principles of Distributed Computing).

Valérie Viet Triem Tong acts as a

- member of the program committee of the « FTRA International Conference on Advanced IT, engineering and Management (FTRA AIM 2012) » held in February 2012 in Seoul, Korea (http://web.ftrai.org/aim2012/home).
- external reviewer for the IEEE Transactions on Network and Service Management journal (TNSM), the Technique et Science informatiques Journal (TSI), and the British Journal of Applied Science & Technology.

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Ludovic Mé is Professor at Supélec:

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

Master: “Intrusion detection”, 9 hours of lecture, M2 - Master research, Rennes, 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: Ludovic Mé is responsible for the module “Secured information systems”, M2 - third year of the engineer degree, Supélec, 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 Simon Boche, Antoine Rault and Mohammed Ghesmoune from February to June

Gilles Guette is Associate Professor at Université de Rennes 1:

Master: « System and Network Security », 48 hours, M1 - second year of the engineer degree; speciality Automation, ESIR, France

Master: « Supervision of student project », 12 hours, M1 - second year of the engineer degree; speciality Telecommunication and Network, ESIR, France

Master: « Network Security », 40 hours, M2 - third year of the engineer degree; speciality Telecommunication and Network, ESIR, France

Master: « System and Scripting », 24 hours, M2 - third year of the engineer degree; speciality Telecommunication and Network, ESIR, France

Master: « Infrastructure Network », 20 hours, M2 - third year of the engineer degree; speciality Telecommunication and Network, ESIR, France

Master: « Supervision of student project », 20 hours, M2 - third year of the engineer degree; speciality Telecommunication and Network, ESIR, France

Master: « System and Network Security », 24 hours, M2 - third year of the engineer degree; speciality Software engineering, ESIR, France

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

Guillaume Piolle is an Assistant Professor at Supélec:

Licence: « Programming models and languages », 7.5 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: « Logical systems and associated electronics », 36 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: « Modelling, algorithms and programming », 20 hours, M1 - second year of the engineer degree, Supélec, France

Master: « Computer security and privacy », 11.5 hours, M1 - second year of the engineer degree, Supélec, France

Master: « Software development project », 12 hours, M1 - second year of the engineer degree, Supélec, France

Master: « C++ /Qt », 18 hours, M2 - third year of the engineer degree, Supélec, France

Master: « Security policies », 4.5 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: « Network supervision in Java », 18 hours, M2 - third year of the engineer degree, Supélec, France

Master: « Web development », 20 hours, M2 - third year of the engineer degree, Supélec, France

Master: « Symbolic Artificial Intelligence », 4.5 hours, M2 - third year of the engineer degree, Supélec, France

Master: « Law and computing », 11.5 hours, M2 - third year of the engineer degree, Télécom Bretagne and Supélec, France

Master: « Occupations at the law-computing interface », 4 hours, M2 - third year of the engineer degree, Télécom Bretagne, France

PhD : « Privacy and personal data protection », 9 hours, Matisse doctoral school, Rennes, France.

Master: « Legal aspects of computing », 1.5 hours, ENS Cachan (Rectorat de Rennes), Rennes, France.

Master: « Privacy and personal data protection on the Internet », 9 hours, URFIST Ouest – Université Rennes 2, 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: « Computer security », 4 hours, M2 - third year of the engineer degree, Supélec, France

Master: « Computer security and pentesting », 10 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: « Python programming for computer security », 1.5 hours, 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) », 20 hours of lecture, M2 - post-graduate training, Supélec, France

Master: « Security », 17 hours including 9 hours of lecture, M2 - post-graduate training, Supélec, France

In-house training: “Computer networks”, 6 hours including 3 hours of lectures

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 and C++ language », 12 hours including 6 hours of lecture, M2 - third year of the engineer degree, 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

Master: Supervision (50%) of the master thesis of Erwan Godefroy

Master: Supervision (50%) of the master thesis of Pierre Karpman

Frédéric Tronel is Associate Professor at Supélec:

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: « Automatic reasoning », 6 hours including 4.5 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master: « Buffer overflow vulnerabilities (theory and practice) », 15 hours including 3 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master: « Virtualization », 1.5 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master: « Firewalls », 6 hours, M2 - third year of the engineer degree, Supélec, France

Master: « Firewalls », 3 hours, M2 - post-graduate training, Supélec, France

Master: « Makefile », 3 hours, M2 - post-graduate training, Supélec, France

Master: « Calculability in distributed systems », 7.5 hours including 6 hours of lecture, M2 Master research Rennes, France

Master: « Buffer overflow vulnerabilities (theory and practice) », 6 hours including 3 hours of lecture, M2 - third year of the engineer degree, Telecom Bretagne, France

Master: Supervision (50%) of the master thesis of Pierre Karpman

Valérie Viet Triem Tong is Associate Professor at Supélec:

Licence: « Programming », 9 hours, L3 - first year of the engineer degree, Supélec, France

Master: « Computer security », 13.5 hours including 4h30 of lecture, M2 - third year of the engineer degree, Supélec, France

Master: « Game Theory », 20 hours of lecture, M1 - second year of the engineer degree, Supélec, France

Master: « Foundations of computer science », 10.5 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master: « Spontaneous networking », 3 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

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

Emmanuelle Anceaume (CR CNRS):

is co-responsible of the BIB and STAGE modules of the Master Research of the university de Rennes 1.

Michel Hurfin (CR Inria):

Master: Supervision (50%) of the master thesis of Erwan Godefroy

PhD and Post-Doc: in charge of junior researchers at Inria (training through research, relationships with doctoral schools, Support for thematic schools)

9.2.2. Supervision

The defense of the HDR of Eric Totel occurred in december 2012 while the defense of the PhD of Heverson Borba Ribeiro occurred in October 2012. At the end of 2012, fourteen theses are in progress.

HDR: Eric Totel, « Techniques de détection d'erreur appliquées à la détection d'intrusion », Université de Rennes 1 , December 6th 2012.

PhD: Heverson Ribeiro, « Exploiting Rateless Coding in Structured Overlays to Achieve Persistent Storage », université de Rennes 1, October 12th 2011, supervised by Emmanuelle Anceaume and Michel Hurfin.

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: Simon Boche, « Réputation et respect de la vie privée dans les réseaux auto-organisé », started in October 2012, supervised by Christophe Bidan(30%), Gilles Guette (35%) and Nicolas Prigent (35%).

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: 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%).

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 Michel Hurfin (50%) and Sébastien Gambs (50%).

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

PhD in progress: Geoffroy Guéguen, « Métamorphisme viral et grammaires formelles », université de Rennes 1, started in March 2011, supervised by Sébastien Josse (50% - DGA-MI) 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, supervised by 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: Paul Lajoie-Mazenc, « Privacy preserving reputation system in large scale and self organizing systems », started in october 2012, supervised by Emmanuelle Anceaume (50%) and Valérie Viet Triem Tong (50%).

PhD in progress: 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: Pierre Obame, « Dependability issues in large scale systems », started in February 2012, supervised by Emmanuelle Anceaume (50%) and Frédéric Tronel (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). Emmanuelle Anceaume is co-supervising Romaric Ludinard (PhD student from the Inria project Dionysos, Rennes).

9.2.3. Juries

Some members of the team have participated to PhD committees:

- Ludovic Mé was a member of the mid-term PhD committees for 3 PhD students of Télécom Sud Paris (Olivier Levillain, Nabil Hacem, and Gustavo Gonzales Granavillo). Télécom SudParis, April 2012.
- Ludovic Mé was a member of the HDR committee (reviewer) for the HDR of Carlos Aguilar entitled « Sécurité, protection de la vie privée et cryptographie : quelques contributions », Université de Limoges, XLIM, June 2012.
- Christophe Bidan was a member of the PhD committee (reviewer) for the PhD of Aymen Boudguiga entitled « Authentification dans les réseaux maillés sans-fils avec la cryptographie basée sur l'identité », Télécom SudParis, September 2012.
- Ludovic Mé was a member of the PhD committee (reviewer) for the PhD of Sheila Becker entitled « Conceptual Approaches for Securing Networks and Systems », Université du Luxembourg and Institut National Polytechnique de Lorraine, October 2012.
- Christophe Bidan was a member of the PhD committee (reviewer) for the PhD of Rim AKROUT entitled « Analyse de vulnérabilités et évaluation de systèmes de détection d'intrusions pour les applications Web », Université de Toulouse, October 2012.

- Emmanuelle Anceaume was a member of the PhD committee for the PhD of Cyril Cassagnes entitled « Architecture Autonome et Distribuée d'Adressage et de Routage pour la Flexibilité des Communications dans l'Internet », Université de Bordeaux - LaBRI, November 2012.
- Christophe Bidan was a member of the PhD committee (reviewer) for the PhD of Nassima KAMEL entitled « Sécurité des cartes à puce à serveur Web embarqué », Université de Limoges, December 2012.

9.3. Popularization

Sébastion Gambs has participated to the following activities:

- High schools: course on the security topic for the high-school professors involved in the new INS option in Bac S, École Normale Supérieure Cachan antenne de Kerlann, France.
- High schools: 5 presentations in high schools in the context of the event « à la découverte de la recherche ».
- High schools: under the supervision of the association « Math.en.Jeans », a presentation about « Definition and quantification of anonymity » has been done in Rennes and Auray.

Nicolas Prigent has participated to:

- the training of some high-school professors involved in the new INS option in Bac S, École Normale Supérieure Cachan antenne de Kerlann, France.

Guillaume Piolle has participated to:

- the training of some high-school professors involved in the new INS option in Bac S, École Normale Supérieure Cachan antenne de Kerlann, France.

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] H. BORBA RIBEIRO. *L'Exploitation de Codes Fontaines pour un Stockage Persistant des Données dans les Réseaux d'Overlay Structurés*, Université Rennes 1, October 2012, http://hal.inria.fr/tel-00763284.

[12] E. TOTEL. *Techniques de détection d'erreur appliquées à la détection d'intrusion*, Université Rennes 1, December 2012, Habilitation à Diriger des Recherches, http://hal.inria.fr/tel-00763746.

Articles in International Peer-Reviewed Journals

[13] E. ANCEAUME, F. CASTELLA, B. SERICOLA. *Analysis of a large number of Markov chains competing for transitions*, in "International Journal of Systems Science", July 2012, 9 [*DOI :* 10.1080/00207721.2012.704090], http://hal.inria.fr/hal-00736916.

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

[15] R. ANDRIATSIMANDEFITRA, V. VIET TRIEM TONG, L. MÉ. *User Data on Androïd Smartphone Must be Protected*, in "ERCIM News", July 2012, n^{o} 90, 18, http://hal.inria.fr/hal-00735993.

[16] E. AÏMEUR, G. BRASSARD, S. GAMBS. *Quantum speed-up for unsupervised learning*, in "Machine Learning", September 2012, http://hal.inria.fr/hal-00736948.

[17] E. AÏMEUR, G. BRASSARD, S. GAMBS, D. SCHÖNFELD. *P3ERS: Privacy-Preserving PEer Review System*, in "Transactions on Data Privacy", October 2012, http://hal.inria.fr/hal-00737755.

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

[19] S. GAMBS. *Inference attacks on geolocated data*, in "ERCIM News", July 2012, 23, http://hal.inria.fr/hal-00736946.

[20] C. HUMPHRIES, N. PRIGENT, C. BIDAN. *Visualization for Monitoring Network Security Events*, in "ERCIM News", July 2012, n° 90, 31, http://hal.inria.fr/hal-00735995.

Articles in National Peer-Reviewed Journals

[21] Y. DESWARTE, S. GAMBS. *Cyber-attaques et cyber-défenses: problématique et évolution*, in "La Revue de l'Electricité et de l'Electronique", May 2012, n° 2, p. 23-35, http://hal.inria.fr/hal-00736950.

[22] M. JAUME, V. VIET TRIEM TONG, G. HIET. *Spécification et mécanisme de détection de flots d'information illégaux*, in "Technique et Science Informatiques (TSI)", 2012, vol. 31, n° 6, p. 713-742 [*DOI :* 10.3166/TSI.31.713-742], http://hal.inria.fr/hal-00761351.

[23] 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 "Technique et Science Informatiques (TSI)", December 2012, vol. 31, n° 8-9-10, p. 1301-1325 [*DOI :* 10.3166/TSI.31.1301-1325], http://hal.inria.fr/hal-00765487.

Invited Conferences

[24] G. PIOLLE. *Protection de la vie privée : appréhension de concepts éthiques par un agent autonome*, in "Atelier D2A2 "Agents Autonomes et Éthique" à RFIA 2012", Lyon, France, January 2012, http://hal.inria.fr/hal-00682660.

International Conferences with Proceedings

[25] M. ALAGGAN, S. GAMBS, A.-M. KERMARREC. *BLIP: Non-interactive Differentially-Private Similarity Computation on Bloom Filters*, in "14th International Symposium on Stabilization, Safety, and Security of Distributed Systems (SSS 2012)", Toronto, Canada, October 2012, http://hal.inria.fr/hal-00724829.

[26] E. ANCEAUME, Y. BUSNEL. *An Information Divergence Estimation over Data Streams*, in "11th IEEE International Symposium on Network Computing and Applications (IEEE NCA12)", Cambridge, MA, United States, C. ELKS (editor), IEEE, August 2012, vol. 11, Number 72, 11 pages, http://hal.inria.fr/hal-00725097.

[27] E. ANCEAUME, Y. BUSNEL, S. GAMBS. *AnKLe: Detecting Attacks in Large Scale Systems via Information Divergence*, in "Ninth European Dependable Computing Conference (EDCC 2012)", Sibiu, Romania, LNCS, Springer-Verlag, May 2012, 12, http://hal.inria.fr/hal-00677077.

[28] E. ANCEAUME, Y. BUSNEL, S. GAMBS. *AnKLe: détection automatique d'attaques par divergence d'information*, in "14èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel)", La Grande Motte, France, F. MATHIEU, N. HANUSSE (editors), 2012, p. 1-4, 4 pages, http://hal.inria.fr/hal-00688352.

[29] E. ANCEAUME, R. LUDINARD, B. SERICOLA, E. LE MERRER, G. STRAUB. *FixMe: A Self-organizing Isolated Anomaly Detection Architecture for Large Scale Distributed Systems*, in "Proceedings of the 16th International Conference On Principles Of Distributed Systems (OPODIS)", Rome, Italy, December 2012, 12, http://hal.inria.fr/hal-00736922.

[30] R. ANDRIATSIMANDEFITRA, S. GELLER, V. VIET TRIEM TONG. *Designing information flow policies for Android's operating system*, in "IEEE ICC 2012", Ottawa, Canada, June 2012, p. 976-981, http://hal.inria.fr/hal-00736034.

[31] C. ARTIGUES, Y. DESWARTE, J. GUIOCHET, M.-J. HUGUET, M.-O. KILLIJIAN, D. POWELL, M. ROY, C. BIDAN, N. PRIGENT, E. ANCEAUME, S. GAMBS, G. GUETTE, M. HURFIN, F. SCHETTINI. *AMORES: an architecture for mobiquitous resilient systems*, in "ARMOR'12", Sibiu, Romania, April 2012, n^{O} 7, 7, ISBN: 978-1-4503-1150-2 [*DOI :* 10.1145/2222436.2222443], http://hal.inria.fr/hal-00736020.

[32] G. BOSSERT, F. GUIHÉRY, G. HIET. *Netzob : un outil pour la rétro-conception de protocoles de communication*, in "SSTIC 2012", Rennes, France, June 2012, 43, http://hal.inria.fr/hal-00763751.

[33] S. GAMBS, A. GMATI, M. HURFIN. *Reconstruction attack through classifier analysis*, in "DBSEC - 26th Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy - 2012", Paris, France, Springer, July 2012, vol. 7371, p. 274-281, http://hal.inria.fr/hal-00736945.

[34] S. GAMBS, M.-O. KILLIJIAN, M. NUNEZ DEL PRADO CORTEZ. *Next place prediction using mobility Markov chains*, in "MPM - EuroSys 2012 Workshop on Measurement, Privacy, and Mobility - 2012", Bern, Switzerland, April 2012, http://hal.inria.fr/hal-00736947.

[35] S. GAMBS, M.-O. KILLIJIAN, M. ROY, M. TRAORÉ. *Locanyms: Towards Privacy-Preserving Location-Based Services*, in "1st European Workshop on AppRoaches to MObiquiTous Resilience", Sibiu, Romania, May 2012, 6, http://hal.inria.fr/hal-00699742.

[36] S. GAMBS, J. LOLIVE. *SlopPy: Slope One with Privacy*, in "DPM - 7th DPM International Workshop on Data Privacy Management - 2012", Pisa, Italy, September 2012, http://hal.inria.fr/hal-00736949.

[37] S. GAMBS, G. RACHID, H. HAMZA, F. HUC, A.-M. KERMARREC. *Scalable and Secure Polling in Dynamic Distributed Networks*, in "31st International Symposium on Reliable Distributed Systems (SRDS)", Irvine, California, United States, October 2012, http://hal.inria.fr/hal-00723566.

[38] C. HAUSER, F. TRONEL, J. REID, C. FIDGE. *A taint marking approach to confidentiality violation detection*, in "AISC 2012", Melbourne, Australia, CRPIT, Pieprzyk, Josef & Thomborson, Clark (Eds.), February 2012, vol. 125, p. 83-90, http://hal.inria.fr/hal-00736045.

[39] M. HURFIN, I. E. MOISE, J.-P. LE NARZUL, F. MAJORCZYK. *Adaptive Strategies for Speeding Up Sequences of Consensus*, in "26th International Conference on Advanced Information Networking and Applications", Fukuoka, Japan, 2012, p. 435-442, http://hal.inria.fr/hal-00725049.

[40] C. LI, M. HURFIN, Y. WANG. *Brief Announcement: Reaching Approximate Byzantine Consensus in Partially-Connected Mobile Networks*, in "DISC - 26th International Symposium on Distributed Computing", Salvador, Brazil, M. K. AGUILERA (editor), LNCS, Springer, October 2012, vol. 7611, p. 405-406 [*DOI :* 10.1007/978-3-642-33651-5], http://hal.inria.fr/hal-00745112.

[41] R. LUDINARD, E. TOTEL, F. TRONEL, V. NICOMETTE, M. KAANICHE, E. ALATA, R. AKROUT, Y. BACHY. *Detecting Attacks against Data in Web Applications*, in "CRiSIS 2012", Cork, Ireland, October 2012, http://hal.inria.fr/hal-00735997.

[42] L. ZEGHACHE, N. BADACHE, M. HURFIN, I. MOISE. *Providing Reliability for transactional mobile agents*, in "5th International Conference on Advanced Infocomm Technology", Paris, France, V. GUYOT (editor), Springer, July 2012, http://hal.inria.fr/hal-00763197.

National Conferences with Proceeding

[43] T. DEMONGEOT, E. TOTEL, V. VIET TRIEM TONG. *User Defined Control Flow Policy for Web Service Orchestration*, in "C&ESAR 2012", Rennes, France, November 2012, http://hal.inria.fr/hal-00761354.

Conferences without Proceedings

[44] S. GAMBS, A. GMATI, M. HURFIN. *Reconstruction Attack through Classifier Analysis*, in "APVP'12 - 3ième édition Atelier Protection de la Vie Privée", Ile de Groix, France, June 2012, http://hal.inria.fr/hal-00747531.

[45] S. GAMBS, M.-O. KILLIJIAN, M. NUNEZ DEL PRADO CORTEZ. *De-anonymization attack on geolocated datasets*, in "Atelier Protection de la Vie Privée (APVP 2012), 3ième édition", Ile de Groix, France, June 2012, http://hal.inria.fr/hal-00765525.

[46] S. GAMBS, M.-O. KILLIJIAN, M. ROY, M. TRAORÉ. *Locanyms: Towards privacy-preserving location-based services*, in "Atelier Protection de la Vie Privée (APVP 2012), 3ième édition", Ile de Groix, France, June 2012, http://hal.inria.fr/hal-00765530.

[47] S. GAMBS, J. LOLIVE. *SlopPy: Slope One with privacy*, in "Atelier Protection de la Vie Privée (APVP 2012), 3ième édition", Ile de Groix, France, June 2012, http://hal.inria.fr/hal-00765519.

[48] P. LAJOIE MAZENC. *Système de réputation préservant la vie privée*, in "3ième édition Atelier Protection de la vie privée", Groix, France, November 2012, http://hal.inria.fr/hal-00763377.

[49] R. PAIVA MELO MARIN, G. PIOLLE, C. BIDAN. *Privacy Policy Requirements for Distributed Social Network Systems*, in "APVP'12", Groix, France, June 2012, http://hal.inria.fr/hal-00736023.

Scientific Books (or Scientific Book chapters)

[50] Y. DESWARTE, S. GAMBS. *The challenges raised by the privacy-preserving identity card*, in "Cryptography and Security: From Theory to Applications", D. NACCACHE (editor), Lecture Notes in Computer Science, Springer, 2012, vol. 6805, p. 383-404 [*DOI :* 10.1007/978-3-642-28368-0], http://hal.inria.fr/hal-00736944.

Research Reports

[51] E. ANCEAUME, Y. BUSNEL. *Sketch ☆-metric: Comparing Data Streams via Sketching*, IRISA, December 2012, n^{o} 2001, http://hal.inria.fr/hal-00764772.

[52] E. ANCEAUME, G. GUETTE, P. LAJOIE MAZENC, N. PRIGENT, V. VIET TRIEM TONG. *A Privacy Preserving Distributed Reputation Mechanism*, IRISA, October 2012, n^{o} 2000, http://hal.inria.fr/hal-00763212.

[53] C. LI, M. HURFIN, Y. WANG. *Reaching Approximate Byzantine Consensus in Partially-Connected Mobile Networks*, Inria, May 2012, n^{o} RR-7985, 17, http://hal.inria.fr/hal-00703111.

References in notes

[54] 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.

[55] 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.

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

[57] 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.

[58] 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. 299–306.

[59] 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.