IN PARTNERSHIP WITH:
CNRS

Université Rennes 1

SUPELEC (Rennes)

Activity Report 2013

Project-Team CIDRE

Confidentialité, Intégrité, Disponibilité et Répartition

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

RESEARCH CENTER
Rennes - Bretagne-Atlantique

THEME
Distributed Systems and middleware

Table of contents

Project-Team CIDRE

Keywords: Security, Privacy, Distributed Systems, Visualization

Creation of the Project-Team: 2011 July 01.

1. Members

Research Scientists

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

Faculty Members

Ludovic Mé [Team leader, SUPELEC, Professor, HdR]
Christophe Bidan [SUPELEC, Professor, HdR]
Sébastien Gambs [Univ. Rennes I, Associate Professor, Inria, Research Chair]
Gilles Guette [Univ. Rennes I, Associate Professor]
Guillaume Hiet [SUPELEC, Assistant Professor]
Guillaume Piolle [SUPELEC, Assistant Professor]
Nicolas Prigent [SUPELEC, Assistant Professor]
Eric Totel [SUPELEC, Professor, HdR]
Frédéric Tronel [SUPELEC, Associate Professor]
Valérie Viet Triem Tong [SUPELEC, Associate Professor]

Engineers

Guillaume Brogi [Inria, from Jan. 2013]
David Lanoe [Univ. Rennes I, from Sep. 2013]
Thomas Letan [SUPELEC, from Sep. 2013]
Izabela Moise [Inria, OSEO Anvar, until May. 2013]

PhD Students

Radoniaina Andriatsimandefitra [Univ. Rennes I, MESR grant]
Mounir Assaf [SUPELEC, CEA contract]
Simon Boche [Univ. Rennes I, ANR project AMORES]
Georges Bossert [SUPELEC, Amossys CIFRE, until Oct. 2013]
Thomas Demongeot [Télécom Bretagne, DGA]
Ahmed Gmati [Université de Rennes I, MESR grant, until June 2013]
Erwan Godefroy [SUPELEC, Inria/DGA]
Antoine Guellier [Univ. Rennes I, MESR grant, from Sep. 2013]
Geoffroy Guéguen [Univ. Rennes I, DGA]
Mouna Hkimi [Univ. Rennes I, Inria CORDI-S grant, from Nov. 2013]
Christopher Humphries [SUPELEC, Inria/DGA]
Paul Lajoie-Mazenc [Univ. Rennes I, MESR grant]
Julien Lolive [Telecom Bretagne, Comin Labs labex/Région Bretagne grant]
Pierre Obame Meye [Univ. Rennes I, France Telecom CIFRE]
Regina Paiva Melo Marin [SUPELEC, Région Bretagne grant]
Deepak Subramanian [SUPELEC, Comin Labs labex/Région Bretagne grant, from Mar. 2013]
Stéphane Geller [SUPELEC, DGA grant]

Post-Doctoral Fellows

Ehab Elsalamouny [Inria, until Oct. 2013]
Maria Cristina Onete [Univ. Rennes I, from Sep. 2013]

Visiting Scientists

Frédéric Majorczyk [DGA]
Miguel Nunez Del Prado Cortez [CNRS, until Dec. 2013]
Jean-François Lalande [ENSI Bourges, Associate Professor, délégation Inria from Sep. 2013]

Others

Simon Bouget [SUPELEC, Intern ENS Cachan, from Feb. 2013 until Jun 2013]
Antoine Guellier [SUPELEC, Intern INSA, from Feb. 2013 until Sep 2013]
David Lanoe [SUPELEC, Intern Univ. Rennes I, from Feb. 2013 until Sep 2013]
Thomas Letan [SUPELEC, Intern INSA, from Feb 2013 until Jul. 2013]
Thomas Saliou [SUPELEC, Intern ENS Cachan, from May 2013 until Jul. 2013]
Eric Asselin [SUPELEC, Intern Univ. Limoges, from Mar. 2013 until Sep. 2013]
Oualid Koucham [SUPELEC, Intern SUPELEC, from Apr. 2013 until Sep. 2013]
Lydie Mabil [Inria, Administrative assistant]

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.

2.2. Highlights of the Year

As highlights of the year, we wish to mention four best paper awards.

Mounir Assaf PhD thesis focusses on the verification of security properties in C programs. While investigating the domain, Mounir Assaf has created a static analysis for programs written in an imperative language with pointer aliases whose objective is to verify a property called Terminating-Insensitive Non Interference (TINI). Briefly speaking, this property guarantees that the content of secret variables of a program do not leak into public ones. Hence, this property is of paramount importance for the security of some critical software components. This work has conducted to the publication of two articles. The first one appeared in (IFIP SEC 2013, a renowned international conference in the domain of security), while the second one has been published in [45] (SAR-SSI 2013), a national conference dedicated to the spreading of work in progress to the French speaking security community. Both papers received the best paper award.

Stephane Geller has proposed a language (namely BSPL) for specifying and composing information flow policies. Such policies detail how a piece of data owned by an application is allowed to disseminate in an operating system. Thomas Saliou, Radoniaina Andriatsimandefitra and Valerie Viet Triem Tong have experimented the relevance of this language. They have proposed a semi-automatic way to compute such policies. They have also show that when such policies are enforced it is possible to detect if an application is infected by a malware. This work has led to the publication of an article in an international conference of the security domain . This article received the best student paper award of the conference.

In , we propose an inference attack called the de-anonymization attack, by which an adversary tries to infer the identity of a particular individual behind a set of mobility traces. The implementation of this attack is based on a mobility model called Mobility Markov Chain (MMC), which is built out from the mobility traces observed during the training phase and is used to perform the attack during the testing phase. Experiments led on real datasets demonstrate that the attack is both accurate and resilient to sanitization mechanisms such as downsampling. This paper has received the IEEE best student paper award at the conference TrustCom 2013.
BEST PAPERS AWARDS :
[27] **Program Transformation for Non-interference Verification on Programs with Pointers in SEC**. M. ASSAF, J. SIGNOLES, F. TRONEL, E. TOTEL.
[25] **Information Flow Policies vs Malware in IAS - Information assurance and security - 2013**. R. ANDRIATSIMANDEFITRA, T. SALIOU, V. VIET TRIEM TONG.

[31] **De-anonymization attack on geolocated datasets in The 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-13)**. S. GAMBS, M.-O. KILLIJIAN, M. NUNEZ DEL PRADO CORTEZ.

3. Research Program

3.1. Our perspective

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

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

By contrast with this traditional conception, we are convinced that by looking at information systems as a combination of possibly revisited basic protocols, each one specified by a set of properties such as synchronization and agreement, security properties should emerge. This vision is shared by others and in particular by Myers *et al.* [57], whose objectives are to explore new methods for constructing distributed systems that are trustworthy in the aggregate even when some nodes in the system have been compromised by malicious attackers.

In accordance with this vision, the first main characteristic of the CIDRE group is to gather researchers from the two aforementioned communities, in order to address intentional failures, using foundations and approaches coming from both communities.

The second main characteristic of the CIDRE group lies in the scope of the systems it considers. Indeed, we consider three complementary levels of study:

- The Node Level: The term node either refers to a device that hosts a network client or service or to the process that runs this client or service. Node security management must be the focus of a particular attention, since from the user point of view, security of his own devices is crucial. Sensitive information and services must therefore be locally protected against various forms of attacks. This protection may take a dual form, namely prevention and detection.
- The Group Level: Distributed applications often rely on the identification of sets of interacting entities. These subsets are either called groups, clusters, collections, neighborhoods, spheres, or communities according to the criteria that define the membership. Among others, the adopted criteria may reflect the fact that its members are administrated by a unique person, or that they share the same security policy. It can also be related to the localization of the physical entities, or the fact that they need to be strongly synchronized, or even that they share mutual interests. Due to the vast number of possible contexts and terminologies, we refer to a single type of set of entities, that we call set of nodes. We assume that a node can locally and independently identify a set of nodes and modify the composition of this set at any time. The node that manages one set has to know the identity of each of its members and should be able to communicate directly with them without relying on a third party. Despite these two restrictions, this definition remains general enough to include as particular cases most of the examples mentioned above. Of course, more restrictive behaviors can be specified by adding other constraints. We are convinced that security can benefit from the existence and the identification of sets of nodes of limited size as they can help in improving the efficiency of the detection and prevention mechanisms.

- The Open Network Level: In the context of large-scale distributed and dynamic systems, interaction with unknown entities becomes an unavoidable habit despite the induced risk. For instance, consider a mobile user that connects his laptop to a public Wifi access point to interact with his company. At this point, data (regardless it is valuable or not) is updated and managed through non trusted undedicated entities (i.e., communication infrastructure and nodes) that provide multiple services to multiple parties during that user connection. In the same way, the same device (e.g., laptop, PDA, USB key) is often used for both professional and private activities, each activity accessing and manipulating decisive data.

The third characteristic of the CIDRE group is to focus on three different aspects of security, namely trust, intrusion detection, and privacy as well as on the bridges that exist between these aspects. Indeed, we believe that to study new security solutions for nodes, set of nodes and open network levels, one must take into account that it is now a necessity to interact with devices whose owners are unknown. To reduce the risk 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 fundamental individual 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 [60], [56]. 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], [59]. 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.

To complement these two approaches, we started two years ago to study the impact that visualization could have in the context of security and particularly how it could improve intrusion detection and forensics analysis.

We finally 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 apply the defensive programming approach (coming from the dependability field) to data corruption detection. The challenge is to determine which invariant/properties must be and can be verified either at runtime or statically. Regarding illegal flow detection, we try to extend this method to build anti-viruses by determining viruses signatures.

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

3.3. Privacy

In our world of ubiquitous technologies, each individual constantly leaves digital traces related to his activities and interests which can be linked to his identity. The protection of privacy is one of the greatest challenge that lies ahead and also an important condition for the development of the Information Society. Moreover, due to legality and confidentiality issues, 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). This directive is currently being revised into a regulation (probably released in 2014) that is going to strengthen the privacy rights of individuals and puts forward the concept of "privacy-by-design", which integrates the privacy aspects into the conception phase of a service or product. The data sovereignty principle states that data related to an individual belong to him and that he should stay in control of how this data is used and for which purpose. This principle can be seen as an extension of many national legislations on medical data that consider that a patient record belongs to the patient, and not to the doctors that create or update it, nor to the hospital that stores it. In the CIDRE project, we 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 management and privacy, geo-privacy, distributed systems 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 design privacy preserving identification scheme, automated reasoning on privacy policies [58], and policy-based adaptive PETs.
- at the set of nodes level, we augment distributed algorithms (i.e., routing) with privacy properties such as anonymity, unlinkability, and unobservability.
- at the open distributed system level, we target both geo-privacy concerns (that typically occur in location-based services) and privacy issues in social networks. In the former case, we adopt a sanitization approach while in the latter one we 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 studies automated trust management systems at all the three identified levels:

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

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

1. at node level, we 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 be forgotten (i.e., the right to data erasure).

4. Application Domains

4.1. Application Domains

With the infiltration of computers and software in almost all aspects of our modern life, security can nowadays be seen as an absolutely general concern. As such, the results of the research targeted by CIDRE apply to a wide range of domains. It is clear that critical systems, where 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 or cloud services, social networks, location-based services, etc.) can also benefit from results obtained by CIDRE, especially with respect to privacy. In addition, 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 and Platforms

5.1. Intrusion Detection

Members of the team have developed several intrusion detectors and security tools.

Blare implements our approach of illegal information flow detection at the OS level for a single node **and** a set of nodes. Two implementations have been realized: a first one for standard Linux distributions and a second one dedicated to Android operating systems (smartphones, tablets, etc). These implementations imply modification of the standard OS kernel; 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. Thanks to the work conducted by Christophe Hauser during its PhD [34], it is now possible to extend this information flow monitoring between a set of cooperating nodes. This is made possible by using dedicated tags carried out by IPv4 packets header (CIPSO tags).

However, 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.

Both **Blare** and **JBlare** development have been supported by an Inria ADT grant since January 2013. Thanks to this grant, Guillaume Brogi has been hired as an engineer to improve the development process of these tools and their quality. He also participates in the dissemination of these tools to the scientific community and potential industrial partners. Blare tools source code and documentation are now available on a dedicated Web site [1].

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.

Netzob is an open-source tool for reverse engineering, traffic generation and fuzzing of communication protocols. It helps security experts to infer both the message format and the state machine of a protocol using passive and active inference approaches. The model can afterward be used to simulate realistic traffic. This tool is developed by AMOSSYS company and Cidre members. Netzob source code and documentation are available on a dedicated Web site [2]

BSPL policy manager is a tool that aims to charge a security policy in a Android device. Policies are fine-grained information flow policies written in BSPL (Blare Security Policies Languages). Such policies precisely describe how a piece of data owned by an application is allowed to disseminate in the operating system. The BSPL policy manager permits to load a policy, checks if the policy is consistent or not. The policy manager permits to compose policies coming with different applications to obtain the policy of the whole device. A policy defined by the manager is enforced by Blare.

5.2. Privacy

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

[1] https://www.blare-ids.org/

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

paradigm and the Hadoop framework that is able to analyze datasets composed of millions of mobility traces in a few minutes [30].

GNOME (Geoprivacy eNhancing tOol for MobilE) is an application for Android smartphone whose main objectives are to (1) to help the user to understand which type of personal information can be learnt from his mobility traces through inference attacks as well as (2) to allow him to decide if he want to sanitize his location data before it is released to a third party (for instance this data could be perturbed according to the desired level of privacy of the user). In addition of the inference attacks such as the extraction of the points of interests and the construction of the mobility model, different mechanisms for generating fake yet realistic mobility traces have been implemented. In particular, one of this method leverages on the mobility model learnt while the second one perturbs the location based on a location variant of differential privacy, a well-established privacy model. These fake mobility traces, that are hard to distinguish from real ones, can be fed to applications running on the smartphone instead of his real location upon request of the user. This application is actually available as a beta release and experiments are actually being conducted with real users in order to test the functionalities of the application. This application has been developed by David Lanoë, an engineer hired as part of the "security and privacy for location-based services" EIT ICT labs activity.

6. New Results

6.1. Intrusion Detection

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

In 2013, we continue to strengthen our research efforts around intrusion detection parameterized by a security policy.

In [33], we have proposed a language for specifying and composing fine-grained information flow policies. The language used a XML-syntax and has a formal semantic. BSPL enables to precisely specify the expected behavior of applications relatively to their sensitive pieces of information. More precisely it permits to specify where a piece of data owned by an application is allowed to disseminate: in which files or processes.

In [25], we have experimented the previous language (BSPL). We have developed a policy manager for android devices. The manager is able to check the consistency of a policy and to compose two consistent policies. We have also proposed a semi-automatic method for computing information flow policies of applications. We have thus computed some examples of policies and shown that these policies are rich enough to permit benign execution of an application without raising useless alerts and sufficiently restrictive to detect malicious actions induced by a malware.

In [40], we have proposed a new data-structure called System Flow Graph (or SFG in short) that offers a compact representation of how pieces of data flow inside a system. For a given application, the system flow graph describes its external behavior. We have shown that this new data structure suits to represent malware behavior and permits to give an early diagnostic in case of intrusion.

In [36] we have collaborated with Mathieu Jaume from Université de Paris 6 describes a formal framework to draw a correspondence between two types of policy definitions - policies that are defined by properties over states of a system and those that are described by properties over executions of a system.

In [34] and in C.Hauser's PhD desertion, we have extended previous work on kBlare (an IDS that detect illegal flows of information at the kernel level) so as to follow information flows at the network level. To that end, a set of nodes administrated by a single entity can be configured according to a distributed security policy expressed in terms of legal information flows. The different operating systems (kBlare) at each node cooperate by tagging each network packet with a tag that describes the information content of the payload. This way, it is possible to detect illegal information flow of information at the network level. This can be used to detect attacks against confidentiality or integrity of the overall system.

6.1.2. Terminating-Insensitive Non-Interference Verification based on an Information Flow Control

In 2010-2011, we started an informal collaboration with colleagues from CEA LIST laboratory. In 2012, this collaboration has turn into a reality by the funding of a PhD student (Mounir Assaf). This PhD thesis is about the verification of security properties of programs written in an imperative language with pointer aliasing (a subset of C language) by techniques borrowed from the domain of static analysis. One of the property of interest for the security field is called Terminating-Insensitive Non-Interference. Briefly speaking, when verified by a program, this property ensures that the content of any secret variable can not leak into public ones (for any terminating execution). However, this property is too strict in the sense that a large number of programs although perfectly secure are rejected by classical analyzers.

In 2013, Mounir Assaf has studied novel approaches that combine static and dynamic information flow monitoring. These approaches are promising since they enable permissive (accepting a large subset of executions) yet sound (rejecting all insecure executions) enforcement of non-interference. We have investigated a dynamic information flow monitor for a language supporting pointers. Our flow-sensitive monitor relies on prior static analysis in order to soundly enforce non-interference. We have also proposed a program transformation that preserves the behavior of initial programs and soundly inlines our security monitor. This program transformation enables both dynamic and static verification of non-interference in a language supporting pointers. This work has been published in [27] and [45].

6.1.3. Visualization of Security Events

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

ELVis [35] has been presented in VizSec 2013 (part of Vis 2013) in October in Atlanta. A working prototype is currently being tuned in order to perform field trials with our partners in DGA-MI. Next year, we are planing to perform research on how various log files can be combined in the same representation. In the PANOPTESEC project, we will also perform some research on visualization for security monitoring in the context of SCADA systems.

6.2. Privacy

6.2.1. Geoprivacy

With the advent of GPS-equipped devices, a massive amount of location data is being collected, raising the issue of the privacy risks incurred by the individuals whose movements are recorded. In [31], we focus on a specific inference attack called the de-anonymization attack, by which an adversary tries to infer the identity of a particular individual behind a set of mobility traces. More specifically, we propose an implementation of this attack based on a mobility model called Mobility Markov Chain (MMC). A MMC is built out from the mobility traces observed during the training phase and is used to perform the attack during the testing phase. We design several distance metrics quantifying the closeness between two MMCs and combine these distances to build de-anonymizers that can re-identify users in an anonymized geolocated dataset. Experiments conducted on real datasets demonstrate that the attack is both accurate and resilient to sanitization mechanisms such as downsampling. This paper has received the IEEE best student paper award at the conference TrustCom 2013.

In [30], we propose to adopt the MapReduce paradigm in order to be able to perform a privacy analysis on large scale geolocated datasets composed of millions of mobility traces. More precisely, we design and implement a complete MapReduce-based approach to GEPETO. GEPETO (for GEoPrivacy-Enhancing TOolkit) is a flexible software that can be used to visualize, sanitize, perform inference attacks and measure the utility of a particular geolocated dataset. The main objective of GEPETO is to enable a data curator (e.g., a company, a governmental agency or a data protection authority) 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. Most of the algorithms used to conduct an inference attack (such as sampling, k-means and DJ-Cluster) represent good candidates to be abstracted in the MapReduce formalism. These algorithms have been implemented with Hadoop and evaluated on a real dataset. Preliminary results show that the MapReduced versions of the algorithms can efficiently handle millions of mobility traces.

6.2.2. Privacy-enhanced Social Networks

In [38], we have proposed a systematic methodology for evaluating the quality of the privacy proposed by a social networking platform. It is based on an analysis grid organizing a correspondence between a number of design features and properties having an impact on privacy, and a level of distribution. For each property, we consider three possible distribution levels: centralized, decentralized and fully decentralized. For security properties, in particular, we have defined those distribution levels with the help of three different attacker models: an attacker has the ability to compromise either one entity in the system, a pre-defined subset of entites in the system, or the whole set of peers in the system. We argument on the idea that the more powerful the attacker model needed to compromise a property for all users in the system, the higher the privacy level linked to this property. A formal evaluation tool based on lattice structures is then proposed to compare social network systems based on this analysis grid. An example evaluation is also provided, with the thorough analysis of several well-known systems of various kinds, notably leading to the conclusion that some privacy-oriented social networking architectures, presented by their authors as fully distributed, showed centralized characteristics for many privacy-related properties.

6.2.3. Privacy Enhancing Technologies

The development of NFC-enabled smartphones has paved the way to new applications such as mobile payment (m-payment) and mobile ticketing (m-ticketing). However, often the privacy of users of such services is either not taken into account or based on simple pseudonyms, which does not offer strong privacy properties such as the unlinkability of transactions and minimal information leakage. In [26], we introduce a lightweight privacy-preserving contactless transport service that uses the SIM card as a secure element. Our implementation of this service uses a group signature protocol in which costly cryptographic operations are delegated to the mobile phone.

6.2.4. Privacy and Web Services

We have proposed [55] a new model of security policy based for a first part on our previous works in information flow policy and for a second part on a model of Myers and Liskov. This new model of information flow serves web services security and allows a user to precisely define where its own sensitive pieces of data are allowed to flow through the definition of an information flow policy. A novel feature of such policy is that they can be dynamically updated, which is fundamental in the context of web services that allow the dynamic discovery of services. We have also presented an implementation of this model in a web services orchestration in BPEL (Business Process Execution Language).

6.2.5. Privacy-preserving Ad-hoc Routing

6.2.5.1. Proactive Protocol

In [39], we have proposed a *proactive* ad hoc routing protocol that preserves the anonymity of the source and of the destination of the packet flows, and assures the unlinkability of flows between any pair of participants to local observers and to global attackers to a lesser extend. Our solution is based on OLSR and combines Bloom filters and ephemeral identifiers. More specifically, the routing process allows any node to discover the topology of the ad hoc network. Once such a topology is known, a source node can establish beforehand a path to reach any destination node. To conceal the identity of the source and destination nodes, the path may not be the shortest ones nor terminate at the destination node. Then, by including the ephemeral public identifiers of the intermediate nodes into a Bloom filter, the source node is able to specify the nodes that have to rebroadcast packets. Thus, when receiving a packet, a node has simply to check, using its ephemeral private identifier, whether it has to rebroadcast the packet, without knowing the source, the destination, nor the previous and next hop.

6.2.5.2. Reactive Protocol

In [42], we have proposed a classification of privacy preserving properties that ensure privacy in ad hoc network routing. We also proposed a taxonomy of adversary's model to analyse existing privacy preserving ad hoc routing protocols. To improve these protocols and to try address all privacy preserving properties, we proposed NoName [42], a novel privacy-preserving ad hoc routing protocol. Based on trapdoor, virtual switching and partially disjoint multipath using Bloom filter, NoName ensures anonytmity of the source, of the destination and of intermediate nodes. It also ensures unlinkability between source and message and between destination and message.

In [43], we have proposed another anonymous *proactive* ad hoc routing protocol, called APART, based on Gentry's fully homomorphic cryptography. Even though this technology is currently quite inefficient from a computational perspective, especially for an application in ad-hoc networks, the protocol APART is merely a proof of concept showing that an anonymous proactive protocol is possible thanks to it. The main idea is that each node maintains a routing table that contains only encrypted data. When a source node want to communicate with a destination node, it cooperates with its neighbors to discover the node that is the next hop to the destination node. This is done in such a way that the source node does not know the entry in its routing table that corresponds to the destination, and the next hop does only know that it has to rebroadcast the messages coming from that source.

6.2.6. Right to be forgotten

The right to be forgotten has become an investigation topic in itself within the field of privacy protection. In [46], we present the joint research project funded by the ministry of justice between our team and researchers in law and sociology, in order to examine the current state, in society and in technology, of the notion of a right to be forgotten, to identify the forthcoming computing tools capable of implementing the notion, and to evaluate the relevance of an autonomous legislation to define it and regulate it. In association with this study and in the light of the identified state-of-the-art, we have proposed in [47] a new technique to implement a right to be forgotten in the manner of a degradation of the quality of published data in time, associated with a fully distributed ephemeral publication technology. We show how this technique could fit various use cases in geosocial networks.

6.3. Trust

Digital reputation mechanisms have indeed emerged as a promising approach to cope with the specificities of large scale and dynamic systems. Similarly to real world reputation, a digital reputation mechanism expresses a collective opinion about a target user based on aggregated feedback about his past behavior. The resulting reputation score is usually a mathematical object (*e.g.* a number or a percentage). It is used to help entities in deciding whether an interaction with a target user should be considered. Digital reputation mechanisms are thus a powerful tool to incite users to behave trustworthily. Indeed, a user who behaves correctly improves his reputation score, encouraging more users to interact with him. In contrast, misbehaving users have lower reputation scores, which makes it harder for them to interact with other users. To be useful, a reputation mechanism must itself be accurate against adversarial behaviors. Indeed, a user may attack the mechanism to increase his own reputation score or to reduce the reputation of a competitor. A user may also free-ride the mechanism and estimate the reputation of other users without providing his own feedback. From what has been said, it should be clear that reputation is beneficial in order to reduce the potential risk of communicating with almost or completely unknown entities. Unfortunately, the user privacy may easily be jeopardized by reputation mechanisms which is clearly a strong argument to compromise the use of such a mechanism. Indeed, by collecting and aggregating user feedback, or by simply interacting with someone, reputation systems can be easily manipulated in order to deduce user profiles. Thus preserving user privacy while computing robust reputation is a real and important issue that we address in our work [51], [23].

6.4. Other Topics Related to Security and Distributed Computing

6.4.1. Network Monitoring and Fault Detection

Monitoring a system consists in collecting and analyzing relevant information provided by the monitored devices, so as to be continuously aware of the system state (situational awareness). However, the ever growing complexity and scale of systems makes both real time monitoring and fault detection a quite tedious task. Thus the usually adopted option is to focus solely on a subset of information states, so as to provide coarse-grained indicators. As a consequence, detecting isolated failures or anomalies is a quite challenging issue. We propose in [24], [44] 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 [12], we consider the setting of large scale distributed systems, in which each node needs to quickly process a huge amount of data received in the form of a stream that may have been tampered with by an adversary (*i.e.*, data items ordering can be manipulated by an omniscient adversary [13]). In this situation, a fundamental problem is how to detect and quantify the amount of work performed by the adversary. To address this issue, we propose AnKLe (for Attack-tolerant eNhanced Kullback- Leibler divergence Estimator), a novel algorithm for estimating the KL divergence of an observed stream compared to the expected one. AnKLe combines sampling techniques and information-theoretic methods. It is very efficient, both in terms of space and time complexities, and requires only a single pass over the data stream. Experimental results show that the estimation provided by AnKLe remains accurate even for different adversarial settings for which the quality of other methods dramatically decreases. Considering n as the number of distinct data items in a stream, we show that AnKLe is an (ε, δ)-approximation algorithm with a space complexity $\widetilde{\mathcal{O}}(\frac{1}{\varepsilon} + \frac{1}{\varepsilon^2})$ 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 [21] 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 the continuation of [53] which proposed an in-depth study of the dynamicity and robustness properties of large-scale distributed systems, in [22], we analyze 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 Uniform Sampling in Dynamic Systems

In [21], we consider the problem of achieving uniform node sampling in large scale systems in presence of a strong adversary. We first propose an omniscient strategy that processes on the fly an unbounded and arbitrarily biased input stream made of node identifiers exchanged within the system, and outputs a stream that preserves Uniformity and Freshness properties. We show through Markov chains analysis that both properties hold despite any arbitrary bias introduced by the adversary. We then propose a knowledge-free strategy and show through extensive simulations that this strategy accurately approximates the omniscient one. We also evaluate its resilience against a strong adversary by studying two representative attacks (flooding and targeted attacks). We quantify the minimum number of identifiers that the adversary must insert in the input stream to prevent uniformity. To our knowledge, such an analysis has never been proposed before.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

- **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. We first realized a state of the art of the research activities for intrusion detection systems (probes), correlation systems and visualization systems. On a second phase, we defined an assessment methodology of these types of tools. Finally, this methodology was 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.

- **HP contract (2013-2014): “Firmware Security”**

  The work we have conducted on the automatic instrumentation of C programs in order to detect intrusions has led to the implementation of the approach within the Frama-C framework under the form of a plugin called SIDAN (see above). A part of this contract for HP consists in adapting and improving this plugin for a real-word code provided by HP, in order to harden their source code.

  Another aspect of this work consists in developing a knew intrusion detection mechanism at the hardware level to protect the firmware (i.e. BIOS or UEFI) level. This mechanism must take into account industrial constraints provided by HP. Thomas Letan has been hired as an engineer to design and implement a proof-of-concept of such mechanism. In 2013, he focused his work on studying state-of-the-art and comparing existing approaches using metrics adapted to HP constraints.

7.2. Bilateral Grants with Industry

- **Amossys: "Evaluation of Intrusion Detection Mechanisms"**

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

- **Orange Labs: "Data Persistence and Consistency in ISP Infrastructures"**

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

- **DGA-MI: "Security Events Visualization"**

  The PhD of Christopher Humphries on visualization is done in the context of a cooperation with DGA-MI. The objective is to propose new visulization mechnisms dedicated to the analysis of security events, for instance for forensic purposes. The tool ELVis presented earlier in this documents is the most recent contribution to this contract. It should be extended this year to allow the unified manipulation of multiple data sources.

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

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

8. Partnerships and Cooperations

8.1. Regional Initiatives

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

- **Labex COMINLAB contract (2012-2015): "POSEIDON"**

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

This project is conducted in cooperation with Télécom Bretagne and Université de Rennes I. The PhD of Julien Lolive (co-supervised by Sébastien Gambs and Caroline Fontaine), which deals with the entwining of identification and privacy mechanisms, is funded by the POSEIDON project.

- **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). Deepak Subramanian is doing his PhD in the context of this project.

- **Labex COMINLAB contract (2013-2016): "DeSceNt"**

  In DeSceNt, we propose to investigate how decentralized home-based networks of plug computers can support personal clouds according to sound architectural principles, mechanisms, and programming abstractions. To fulfill this vision we see three core scientific challenges, which we think must be overcome. The first challenge, decentralized churn-poor design, arises from the nature of plug federations, which show much lower levels of churn than traditional peer-to-peer environments. The second challenge, quasi-causal consistency, is caused by the simultaneous needs to produce a highly scalable environment (potentially numbering millions of users), that also offers collaborative editing capabilities of mutable data-structures (to offer rich social interactions). The third and final challenge, intuitive data structures for plug programming, arises from the need by programmers for intuitive and readily reusable data-structures to rapidly construct rich and robust decentralized personal cloud applications.

  This study is conducted in cooperation with other teams (GDD Team (University of Nantes), EPI ASAP)

8.2. National Initiatives

8.2.1. ANR

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

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

8.2.2. Inria Project Labs

- **CAPPRIS (2012-2016)**

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

  - The design of appropriate metrics to assess and quantify privacy, primarily by extending and integrating the various possible definitions existing for the generic privacy properties such as anonymity, pseudonymity, unlinkability and unobservability, as well as notions coming from information theory or databases such as the recent but promising concept of differential privacy;
  - The definition and the understanding of the fundamental principles underlying “privacy by design”, with the hope of deriving practical guidelines to implement notions such as data

minimization, proportionality, purpose specification, usage limitation, data sovereignty and accountability directly in the formal specifications of our information systems;

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

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

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 I, Inria and Supélec.

8.2.4. Competitivity Clusters

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

8.3. European Initiatives

8.3.1. FP7 Projects

The **PANOPTESEC** project started on the 1st of November 2013. It deals with the automated and assisted security management of SCADA system. The main objective of PANOPTESEC is to provide an integrated solution that will allow to efficiently monitor SCADA systems, detect intrusions and react to them. To that end, it encompasses many of the research topics that are addressed by the CIDre team: alerts aggregation and correlation, policy-aware intrusion detection, architecture-aware intrusion detection, automated trust management, trust-based automated reaction and visualization. The CIDre team is envolved in the project on all of these aspects. The partners are REHA, Alcatel-Lucent Bell Labs France, Epistematica, The university of Rome, the university of Hamburg, the institut Mines-Telecom, ACEA and Supelec.

8.3.2. Collaborations in European Programs, except FP7

Program: EIT ICT labs

Project acronym: “Privacy, security and trust in information society” action line

Project title: “Security and privacy for location-based services” activity

Duration: January 2012 - December 2013

Coordinator: Sébastien Gambs

Other partners: KTH (Sweden), Privatics Inria team (France), Alcatel-Lucent (France), University of Trento (Italy), DFKI (Germany).

Abstract: The main objective of this activity is to address the issues of privacy and security for location-based services. More precisely, the main outcomes of this activity are (1) secure and privacy-preserving implementations of location-based services (for instance traffic monitoring), (2) tools to raise the public awareness about the privacy issues in such context but also to help a user to prevent/limit privacy leaks (thus contributing to the protection of privacy), (3) demonstrators to secure the position of an individual and (4) the application of the results and findings of the activity to other thematic Action Lines of EIT ICT labs.

9. Dissemination

9.1. Scientific Animation

Frédéric Tronel and Nicolas Prigent are members of the organization and program committees of the French symposium SSTIC about security of information and communications technologies (Symposium sur la Sécurité des Technologies de l’Information et de la Communication). This symposium is held each year in Rennes and gathers more than 400 people coming from academic, industrial and governmental sectors.

Emmanuelle Anceaume served as a reviewer for the following conferences:

- IEEE/ACM International Conference on Ubiqutious Computing and Communications (IUCC). 2013 (Australia).
- International Symposium on Security and Multimodality in Pervavise Environments (SMPE). 2013 (Spain).
- International Conference on Secure and Trust Computing, data management, and Applications (STA). 2013 (Japan).
- International Conference on Pervasive and Embedded Computing and Communication Systems (PECCS), 2013 (Spain).

Christophe Bidan is a member of the Selection and Validation Committee (CSV - Comité de Sélection et de Validation) of the Images & Réseaux cluster, of the advisory board the security activities of the DGA-MI (Direction Générale de l’Armement - Maîtrise de l’Information). Christophe Bidan served as a reviewer for the following conferences:

- SecureComm - International Conference on Security and Privacy in Communication Networks 2013.
- SETOP - International Workshop on Autonomous and Spontaneous Security 2013.
- IIT - International Conference on Innovations in Information Technology 2013.

Sébastien Gambs acts as:

- 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).
- member of the program committee of the « 5th International Workshop on SEcurity and SOCial Networking (SESOC 20123) » held in March 2013 in San Diego, USA.
- member of the program committee of the « Workshop on Privacy and Anonymity for the Digital Economy (PADE 2013) » held in June 2013 in Sydney, Australia (http://pade-lcn2013.conference.nicta.com.au/?page_id=14).
- member of the program committee of the « 11th International Conference on Privacy, Security and Trust (PST 2013) » held in July 2013 in Tarragona, Spain (http://unescoprivacychair.urv.cat/pst2013/).
- member of the program committee of the « 14th Conference on Communications and Multimedia Security (CMS 2013) » held in September 2013 in Magdeburg, Germany (http://www.cms2013.de/).
- member of the program committee of the « 8th International Workshop on Data Privacy Management (DPM 2013) » held in September 2013 in Egham, UK (http://research.icbnet.ntua.gr/DPM2013/).
- member of the program committee of the « 6th Symposium on Foundations and Practice of Security (FPS 2013) » held in October 2013 in La Rochelle, France (http://conferences.telecom-bretagne.eu/fps/2013/).
- member of the program committee of the « 8th International Conference on Risks and Security of Internet and Systems (CRiSIS 2013) » held in October 2013 in La Rochelle, France (http://secinfo.msi.unilim.fr/crisis2013/).
- member of the program committee of the « 4th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN 2013) » held in October 2013 in Niagara Falls, Canada (http://cs-conferences.acadiau.ca/euspn-13/).
- external reviewer for PETS 2013 (13th Privacy Enhancing Technologies Symposium), Transactions on Mobile Computing, IEEE Transactions on Parallel and Distributed Systems, Journal of Parallel and Distributed Computing, Journal of Systems and Software and Information Systems.

Gilles Guette is member of the program committee of the symposium SSTIC. He also served as a reviewer for the following conferences:

- National conference SARSSI 2013.
- National conference SSTIC 2013.

Ludovic Mé is a member of the steering committee of RAID (International Symposium on Research in Attacks, Intrusions and Defenses, ex-Recent Advances in Intrusion Detection), of the French conference SAR-SSI, and of the conference C&ESAR organized by the DGA. He served from 2011 to 2013 the scientific board of the CSFRS ("High Council for Strategic Education and Research"). He served this year as a reviewer for the ANRT organization, and for a few journals.

Guillaume Piolle served as a reviewer for the Internal Journal of Information Security. He is a member of CERNA, the ethics committee of Allistene, serving as a common reference point for French institutions undertaking research in information technologies. He also served as a reviewer for the following conferences:

- IIT - International Conference on Innovations in Information Technology 2013;
- SARSSI - National conference on Security of Information Systems and Network Architectures 2013.

Nicolas Prigent served as a reviewer for the SSTIC 2013 conference. He also was the PC chair of SAR-SSI 2013.

Frédéric Tronel served as a reviewer for the following conferences:

- International conference Principles of Distributed Computing (PODC 2013) (as an external reviewer).
- National conference SSTIC 2013.

Valérie Viet Triem Tong served as a reviewer for the following conferences:

- International journal Science of Computer Programming.
- International conference ICC 2014.

Guillaume Hiet served as a reviewer for the following organizations :

- Fonds de recherche du Québec – Nature et technologies
- ANRT
- ANR (INS)

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

Christophe Bidan is Professor at Supélec :

Licence : “Models and programming languages”, lab work (8h), L3 - first year of the engineer degree, Supélec, France

Licence : “Foundations of computer science, data structures and algorithms.”, lectures (18h), tutorial (6h) and lab work (12h), L3 - first year of the engineer degree, Supélec, France

Licence: “Software engineering”, tutorial (6h) and lab work (12h), L3 - first year of the engineer degree, Supélec.

Licence: “Information System”, tutorial (6h), M1 - second year of the engineer degree, Supélec.

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

Master : “Applied / Advanced Cryptography”, lectures (12h) and lab work (24h), 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 : “Supervision of student project”, 1 project, M2 research degree of University of Rennes I.

Sébastien Gambs is Associate Professor at Université de Rennes I:

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

Master: “Topics on Authentication”, 16 hours of lectures, M2 - Master Pro SSI, Université de Rennes I, France.

Gilles Guette is Associate Professor at University of Rennes I :

Master : “Network Architecture and Security”, 48 hours including 16 hours of lecture, M1 - second year of the engineer degree, ESIR, France

Master : “Network Administration”, 42 hours including 14 hours of lecture, M1 - second year of the engineer degree, ESIR, France

Master : “Network and System Tools”, 24 hours including 4 hours of lecture, M1 - second year of the engineer degree, ESIR, France

Master : “Access Network”, 6 hours including 2 hours of lecture, M1 - second year of the engineer degree, ESIR, France

Master : “Network and System Security”, 18 hours including 6 hours of lecture, M2 - third year of the engineer degree, ESIR, France

Master : “Network Security”, 12 hours including 12 hours of lecture, M2 - third year of the engineer degree, ESIR, France

Master : “Infrastructure Network”, 20 hours including 4 hours of lecture, M2 - third year of the engineer degree, ESIR, France

Master : “Supervision of student project”, 1 projects, M1 - Master in Computer Science, ISTIC, France

Master : “Supervision of student project”, 1 projects, M1 - second year of the engineer degree, ESIR, France

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

Ludovic Mé is Professor at Supélec:

Licence: “Software Engineering”, 15h, L3 - first year of the engineer degree, Supélec, France

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

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

Master: “Supervision of student project”, 1 project, 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: Ludovic Mé is responsible for the module “Secured information systems”, M2 - third year of the engineer degree, Supélec, France

Doctorat: “Introduction to Information Systems Security”, 18 hours, Université de Rennes I, France

Guillaume Hiet is Assistant-Professor at Supélec:

Licence: “Models and programming languages”, 11 hours, L3 - first year of the engineer degree, Supélec, France

Licence: “Foundations of computer science, data structures and algorithms”, 15 hours, L3 - first year of the engineer degree, Supélec, France

Master: “Computer security and privacy for the engineer”, 10 hours including 4,5 hours of lecture, M1 - second year of the engineer degree, Supélec, France

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

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

Master: “Introduction to Linux”, lab work (3h), M2 - master CS (Cyber Security), Supélec, France

Master: “Java Security”, lecture (3h), M2 - master CS (Cyber Security), Supélec, France

Master: “Linux Security”, lab work (6h), M2 - master CS (Cyber Security), Supélec, France

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

Master: “Intrusion Detection”, lecture (6h) and lab work (6h), M2 - master CS (Cyber Security), Supélec, France

Master: “Intrusion Detection”, lecture (3h) and lab work (6h), M2 - third year of the engineer degree, M2 research degree of University of Rennes I, Supélec

Master: “Intrusion Detection”, lecture (8h) and lab work (12h), M2 - master 2 degree, University of Rennes I, France

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

Master: “Intrusion Detection”, 6 hours of lecture, M2, Université de Limoges, France

Master: “Firewall”, lecture (4h), M2 - master 2 degree, University of Rennes I, 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

Guillaume Piolle is Assistant Professor at Supélec:

Licence: “Programming models and languages”, 14 hours, L3 - first year of the engineer degree, Supélec, France

Licence: “Foundations of computing, data structures and algorithms”, 15 hours, L3 - first year of the engineer degree, Supélec, France

Licence: “Logical systems and electronics”, 16 hours, L3 - first year of the engineer degree, Supélec, France

Licence: “Software engineering”, 22 hours, L3 - first year of the engineer degree, Supélec, France

Master: “Modelling, algorithms and programming”, 17 hours including 9 hours of lecture, M1 - second year of the engineer degree, Supélec, France

Master: “Computer security and privacy for the engineer”, 10,5 hours including 7,5 hours of lecture, M1 - second year of the engineer degree, Supélec, France

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

Master: “Network access protection”, 6 hours, M2 - third year of the engineer degree, Supélec, France

Master: “Network supervision in Java”, 3 hours, M2 - third year of the engineer degree, Supélec, France

Master: “Symbolic artificial intelligence”, 3 hours of lecture, M2 - third year of the engineer degree, Supélec, France

Master: “C++/Qt”, 15 hours, M2 - third year of the engineer degree, Supélec, France

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

Master: “Introduction to privacy protection”, 4 hours of lecture, M2, joint degree between University of Saint-Étienne, École Nationale Supérieure des Mines de Saint-Étienne, France, and University of Alicante, Spain

Master: “Legal aspects of computing”, 1 hour of lecture, course for computing high school teachers, Académie de Rennes, France

Master: “Law and computing”, 4 hours of lecture, M2, master in Cybersecurity, joint degree between Supélec and École Nationale Supérieure des Télécommunications de Bretagne, France

Nicolas Prigent is Assistant Professor at Supélec:

Master: “Operating systems”, lectures (10h30), M2 - third year of the engineer degree, Supélec.

Master: “Automatic reasoning”, lectures (3h00) and lab work (1h30), M2 - third year of the engineer degree, Supélec.

Master: “Python for security”, lectures (3h00) and lab work (3h00), M2 - third year of the engineer degree, Supélec.

Master: “Advanced Java”, lectures (3h00) and lab work (3h00), M2 - third year of the engineer degree, Supélec.

Master: “Pentest”, lab work (9h00), M2 - third year of the engineer degree, Supélec.

Master: “MS-Windows”, lectures (6h00) and lab work (6h00), M2 - third year of the engineer degree, Supélec.

Master: “Preparation to iCTF, operational security”, lab work (20h00), M2 - third year of the engineer degree, Supélec.

Licence: “Programming models and languages”, 14 hours, L3 - first year of the engineer degree, Supélec.

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

Master: “Supervision of student project”, 3 projects, M3 - third year of the engineer degree, Supélec, France.

Eric Totel is 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 CS (Cyber Security), 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”, 9 hours including 7.5 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 : “Intrusion Detection”, 6 hours of lecture, M2 - M2 - master CS (Cyber Security), Supélec, France

Master : “Intrusion Detection”, 8 hours of lecture, M2 - master 2 degree, University of Rennes I, France

Master : “Intrusion Detection”, 4 hours of lecture, M2 - master 2 degree, University of Rennes I, France

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

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

Frédéric Tronel is Associate Professor at Supélec:

Licence: “Software engineering”, lectures (15h), tutorial (6h) and lab work (12h), L3 - first year of the engineer degree, Supélec.

Master: “Operating systems”, lectures (10h30), M2 - third year of the engineer degree, Supélec .

Master: “Compilers”, lectures (9h), lab work (12h), M2 - third year of the engineer degree, Supélec.

Master: “Automatic reasoning”, lectures (4h30) and lab work (1h30), M2 - third year of the engineer degree, Supélec.

Master: “Buffer overflow vulnerabilities (theory and practice)”, lecture (3h) and lab work (12h), M2 - third year of the engineer degree, Supélec.

Master: “Buffer overflow vulnerabilities (theory and practice)”, lectures (3h) and lab work (3h), M2 - third year of the engineer degree, Telecom Bretagne.

Master: “Firewall”, tutorial (3h), lab work (3h), M2 - third year of the engineer degree, Supélec.

Master: “Calculability in distributed systems”, lecture (6h), M2 research degree jointly with University of Rennes I and Supélec.

Valérie Viet Triem Tong is associate Professor at Supélec :

Licence : “Models and programming languages”, Lab work (10h), L3 - first year of the engineer degree, Supélec, France

Licence : “Foundations of computer science, data structures and algorithms.”, tutorial (3h) and lab work (6h), L3 - first year of the engineer degree, Supélec, France

Licence : “Programming with Java”, Lectures and lab work (12h), M1- International student in second year of the engineer degree (NplusI program), Supélec, France

Master: “Game Theory”, Lectures and lab work (20h), M1 - second year of the engineer degree, Supélec.

Master: “Projects in computer science ”, coordination of the projects for all students second year of the engineer degree (60 students at Rennes), Supélec.

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

Master : “Applied / Advanced Cryptography”, lectures (3h) and lab work (3h), M2 - third year of the engineer degree, Supélec, France.

Master: “Intrusion Detection”, Lectures (3h), M2 - third year of the engineer degree, M2 research degree of University of Rennes I, Supélec.

Master: “Automatic reasoning”, lectures (4h30), M2 - third year of the engineer degree, Supélec.

Master: “Security of program using proof assistants”, Lectures and lab work (10h30), M2 - third year of the engineer degree, Supélec.

9.2.2. Supervision

PhD: Christophe Hauser, “Détection d’intrusions dans les systèmes distribués par propagation de teinte au niveau noyau – A basis for intrusion detection in distributed systems using kernel-level data tainting”, Université de Rennes I (France) and Queensland University of Technology (Brisbane, Australia) joint PhD, June 2013, 19th, supervised by Ludovic Mé (20%) and Frédéric Tronel (80%).

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%). The Phd was defended with success on the 19th of December 2013.

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: 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 I, started in March 2011, supervised by Sébastien Josse (50% - DGA-MI) and Ludovic Mé (50%).

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

PhD in progress: Mouna Hkimi “, Détection d’intrusion dans les systèmes distribués: Application au cloud computing”, started in October 2013, supervised by Eric Totel (50%) and Michel Hurfin (50%).

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: Julien Lolive, “Entwining identification and privacy mechanisms”, Télécom-Bretagne, started in December 2012, supervised by Caroline Fontaine (50% - Télécom-Bretagne) and Sébastien Gambs (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%).

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

Some members of the team also participate to the supervision of external PhD students. Sébastien Gambs is co-supervising Raghavendran Balu (PhD student for Texmex, Inria Rennes), Mohammad Nabil Al-Aggan (PhD student from ASAP, Inria Rennes, who defended his thesis on December 2013), Miguel Nunez del Prado Cortez (PhD student from LAAS-CNRS, Toulouse, who defended his thesis on December 2013), and Moussa Traore (PhD student from LAAS-CNRS, Toulouse). Emmanuelle Anceaume is co-supervising Romaric Ludinard (PhD student from the Inria project Dionysos, Rennes). Valérie Viet Triem Tong participates to the "supervision committee" of Quentin Jerome Phd Student from the University of Luxembourg. Christophe Bidan is supervising Kun He (PhD student from the IRT B-Com).

9.2.3. Juries

- Ludovic Mé was a member of the mid-term PhD committees for a PhD student at Ecole des Mines de Nantes (Florent de Kerchove). Ecole des Mines de Nantes, June 2013.
- Ludovic Mé was a member of the PhD committee (reviewer) for the PhD of Gabriel Serme entitled “Modularisation de la sécurité informatique dans les systèmes distribués”, Télécom Paris Tech, November 2013.
- Ludovic Mé was a member of the PhD committee (president of the jury) for the PhD of Mohammad Alaggan entitled “Private peer-to-peer similarity computation in personalized collaborative platforms”, Université de Rennes I, December 2013.

- Ludovic Mé was a member of the PhD committee (examinateur) for the PhD of Gustavo Gonzalez Granadillo entitled "Optimization of Cost-based Threat Response for Security Information and Event Management Systems", Télécom SudParis et Université Pierre et Marie Curie, December 2013.
- Christophe Bidan was a member of the PhD committee (president of the jury) for the PhD of Aude Plateaux entitled "Solutions opérationnelles d'une transaction électronique sécurisée et respectueuse de la vie privée", Université de Caen Basse-Normandie, November 2013.
- Christophe Bidan was a member of the PhD committee (examiner) for the PhD of Ludovic Jacquin entitled "Compromis performance/sécurité des passerelles très haut débit pour Internet", Université de Grenoble, November 2013.
- Christophe Bidan was a member of the PhD committee (reviewer) for the PhD of Mohamed Amine Riahla entitled "Contributions au routage et l'anonymat des échanges dans les réseaux dynamiques", Université de Limoges, March 2013.

9.3. Popularization

[17] represents an effort to communicate to the community of engineers and company officials the reflexions and evolutions taking place in academia in the domain of personal data protection, in the fields of both computer science and law. The adopted perspective is to shed some light on the evolutions of the requirements, procedures and policies applying to public or private organizations, putting them in correspondence with the evolution of technical and legal risks, societal motivations and computing tools.

10. Bibliography

Major publications by the team in recent years

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

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

[3] M. Ben Ghorbel-Talbi, F. Cuppens, N. Cuppens-Boulahia, D. Le Métayer, G. Piolle. *Delegation of Obligations and Responsibility*, in "Future Challenges in Security and Privacy for Academia and Industry - 26th IFIP TC 11 International Information Security Conference (SEC2011)", J. Camenisch, S. Fischer-Hübner, Y. Murayama, A. Portmann, C. Rieder (editors), IFIP AICT, Springer, 2011, vol. 354, pp. 197–209

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

[5] S. Gambs, B. Kégl, E. Aïmeur. *Privacy-preserving boosting*, in "Data Mining and Knowledge Discovery", 2007, vol. 14, n^{o} 1, pp. 131-170

[6] G. Hiet, V. Viet Triem Tong, L. Mé, B. Morin. *Policy-based intrusion detection in web applications by monitoring Java information flows*, in "International Journal of Information and Computer Security", 2009, vol. 3, n^{o} 3/4, pp. 265–279

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

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

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

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

Publications of the year

Doctoral Dissertations and Habilitation Theses

[11] C. HAUSER. , *Détection d'intrusions dans les systèmes distribués par propagation de teinte au niveau noyau*, Université Rennes 1, June 2013, http://hal.inria.fr/tel-00932618

Articles in International Peer-Reviewed Journals

[12] E. ANCEAUME, Y. BUSNEL. *A Distributed Information Divergence Estimation over Data Streams*, in "IEEE Transactions on Parallel and Distributed Systems", 2013, 10 p. , http://hal.inria.fr/hal-00804437

[13] E. ANCEAUME, Y. BUSNEL, S. GAMBS. *On the Power of the Adversary to Solve the Node Sampling Problem*, in "Transactions on Large-Scale Data- and Knowledge-Centered Systems (TLDKS)", December 2013, vol. 8290, pp. 102-126 [*DOI :* 10.1007/978-3-642-45269-7_5], http://hal.inria.fr/hal-00926485

[14] E. ANCEAUME, F. CASTELLA, R. LUDINARD, B. SERICOLA. *Markov Chains Competing for Transitions: Application to Large-Scale Distributed Systems*, in "Methodology and Computing in Applied Probability", June 2013, vol. 15, n^{o} 2, pp. 305–332 [*DOI :* 10.1007/s11009-011-9239-6], http://hal.inria.fr/hal-00650081

[15] E. ANCEAUME, F. CASTELLA, B. SERICOLA. *Analysis of a large number of Markov chains competing for transitions*, in "International Journal of Systems Science", March 2014, vol. 45, n^{o} 3, pp. 232–240 [*DOI :* 10.1080/00207721.2012.704090], http://hal.inria.fr/hal-00736916

[16] E. AÏMEUR, G. BRASSARD, S. GAMBS. *Quantum speed-up for unsupervised learning*, in "Machine Learning", February 2013, vol. 90, n^{o} 2, pp. 261-287 [*DOI :* 10.1007/s10994-012-5316-5], http://hal.inria.fr/hal-00736948

Articles in National Peer-Reviewed Journals

[17] G. PIOLLE. *La protection des données personnelles, un enjeu organisationnel et technique*, in "Flux", March 2013, n^{o} 274, VIII p. , http://hal.inria.fr/hal-00845803

Invited Conferences

[18] L. Mé. *Faire face aux cybermenaces : détecter (les attaques) et former (des experts en SSI)*, in "11ème Symposium sur la Sécurité des Technologies de l'Information et des Communications (SSTIC 2013)", Rennes, France, June 2013, http://hal.inria.fr/hal-00926075

[19] G. Piolle. *La vie privée sur Internet, une question de confiance ?*, in "Journée Web et Confiance", Lyon, France, January 2013, http://hal.inria.fr/hal-00777430

International Conferences with Proceedings

[20] E. Anceaume, Y. Busnel. *Sketch *-metric: Comparing Data Streams via Sketching*, in "12th IEEE International Symposium on Network Computing and Applications (IEEE NCA 2013)", Boston, United States, D. Avresky (editor), August 2013, vol. 12, 11 p. [*DOI :* 10.1109/NCA.2013.11], http://hal.inria.fr/hal-00926685

[21] E. Anceaume, Y. Busnel. *Sketch -metric: Comparing Data Streams via Sketching*, in "The 12th IEEE International Symposium on Network Computing and Applications (IEEE NCA13)", Boston, France, IEEE (editor), August 2013, 8 p. , http://hal.inria.fr/hal-00764772

[22] E. Anceaume, Y. Busnel, B. Sericola. *Uniform Node Sampling Service Robust against Collusions of Malicious Nodes*, in "43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN 2013)", Budapest, Hungary, June 2013, vol. 43, 249 p. , http://hal.inria.fr/hal-00804430

[23] E. Anceaume, G. Guette, P. Lajoie Mazenc, N. Prigent, V. Viet Triem Tong. *A Privacy Preserving Distributed Reputation Mechanism*, in "International Conference on communications (ICC)", Budapest, France, June 2013, 6 p. , http://hal.inria.fr/hal-00763212

[24] E. Anceaume, E. Le Merrer, R. Ludinard, B. Sericola, G. Straub. *A Self-organising Isolated Anomaly Detection Architecture for Large Scale Systems*, in "Nem-Summit", France, October 2013, 12 p. , http://hal.inria.fr/hal-00907374

[25] *Best Paper*
R. Andriatsimandefitra, T. Saliou, V. Viet Triem Tong. *Information Flow Policies vs Malware*, in "IAS - Information assurance and security - 2013", Yassmine Hammamet, Tunisia, 2013, http://hal.inria.fr/hal-00909406.

[26] G. Arfaoui, S. Gambs, P. Lacharme, J.-F. Lalande, L. Roch, J.-C. Paillès. *A Privacy-Preserving Contactless Transport Service for NFC Smartphones*, in "Fifth International Conference on Mobile Computing, Applications and Services", Paris, France, LNICST, Springer, November 2013, http://hal.inria.fr/hal-00875098

[27] *Best Paper*
M. Assaf, J. Signoles, F. Tronel, E. Totel. *Program Transformation for Non-interference Verification on Programs with Pointers*, in "SEC", Auckland, New Zealand, L. Janczewski, H. Wolfe, S. Shenoi (editors), IFIP Advances in Information and Communication Technology, Springer Berlin Heidelberg, April 2013, vol. 405, pp. 231-244 [*DOI :* 10.1007/978-3-642-39218-4_18], http://hal.inria.fr/hal-00814671.

[28] C. Bidan, D. Boucard, M. Chapon, P. Cloitre, G. Donias, G. Guette, T. Plesse, N. Prigent, S. Tarrapey. *Preventive and corrective security solutions for routing in military tactical ad hoc networks*, in "MCC 2013", Saint Malo, France, October 2013, pp. 149-165, http://hal.inria.fr/hal-00919218

[29] E. Elsalamouny, V. Sassone. *An HMM-based reputation model*, in "Advances in Security of Information and Communication Networks", Cairo, Egypt, Springer Berlin Heidelberg, 2013, vol. 381, pp. 111-121 [*DOI :* 10.1007/978-3-642-40597-6_9], http://hal.inria.fr/hal-00831401

[30] S. Gambs, M.-O. Killijian, I. Moise, M. Nunez Del Prado Cortez. *MapReducing GEPETO or Towards Conducting a Privacy Analysis on Millions of Mobility Traces*, in "2013 IEEE International Symposium on Parallel & Distributed Processing, Workshops and Phd Forum", Cambridge, United States, May 2013, pp. 1937-1946 [*DOI :* 10.1109/IPDPSW.2013.180], http://hal.inria.fr/hal-00911238

[31] *Best Paper*
S. Gambs, M.-O. Killijian, M. Nunez Del Prado Cortez. *De-anonymization attack on geolocated datasets*, in "The 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom-13)", Melbourne, Australia, July 2013, 9 p. , Prix IEEE Best Student Paper Award, http://hal.inria.fr/hal-00718763.

[32] S. Gambs, M.-O. Killijian, M. Nunez Del Prado Cortez, M. Traoré. *Towards a recommender system for bush taxis*, in "3rd Conference on the Analysis of Mobile Phone Datasets (NetMob'13)", Boston, United States, May 2013, http://hal.inria.fr/hal-00911241

[33] S. Geller, V. Viet Triem Tong, L. Mé. *BSPL: A Language to Specify and Compose Fine-grained Information Flow Policies*, in "SECUREWARE - 7th International Conference on Emerging Security Information, Systems and Technologies", Barcelona, Spain, 2013, http://hal.inria.fr/hal-00909400

[34] C. Hauser, F. Tronel, C. Fidge, L. Mé. *Intrusion detection in distributed systems, an approach based on taint marking*, in "IEEE ICC2013 - IEEE International Conference on Communications", Budapest, Hungary, July 2013, http://hal.inria.fr/hal-00840338

[35] C. Humphries, N. Prigent, C. Bidan, F. Majorczyk. *ELVIS: Extensible Log VISualization*, in "VIZSEC", ATLANTA, United States, October 2013, http://hal.inria.fr/hal-00875668

[36] M. Jaume, R. Andriatsimandefitra, V. Viet Triem Tong, L. Mé. *Secure states versus Secure executions: From access control to flow control*, in "ICISS - 9th International Conference on Information Systems Security - 2013", Kolkata, India, 2013, http://hal.inria.fr/hal-00909395

[37] P. Meye, P. Raïpin-Parvédy, F. Tronel, E. Anceaume. *Toward a distributed storage system leveraging the DSL infrastructure of an ISP*, in "11th IEEE Consumer Communications and Networking Conference", United States, January 2014, 2 p. , http://hal.inria.fr/hal-00924051

[38] R. Paiva Melo Marin, G. Piolle, C. Bidan. *An Analysis Grid for Privacy-related Properties of Social Network Systems*, in "SOCIALCOM 2013", Washington D.C., United States, IEEE Computer Society, September 2013, pp. 520-525 [*DOI :* 10.1109/PASSAT/SocialCom.2013.79], http://hal.inria.fr/hal-00908339

[39] J.-M. Robert, C. Bidan. *A proactive routing protocol for wireless ad hoc networks assuring some privacy*, in "HotWiSec '13", Budapest, Hungary, September 2013, pp. 25-30 [*DOI :* 10.1145/2463183.2463190], http://hal.inria.fr/hal-00920036

National Conferences with Proceedings

[40] R. Andriatsimandefitra, V. Viet Triem Tong, L. Mé. *Diagnosing intrusions in Android operating system using system flow graph*, in "Workshop Interdisciplinaire sur la Sécurité Globale", Troyes, France, January 2013, http://hal.inria.fr/hal-00875211

[41] N. Aubert, M. Ali Ayachi, C. Bidan, N. Prigent. *The Hecate Attack*, in "SAR-SSI 2013", Mont de Marsan, France, September 2013, pp. 205-215, http://hal.inria.fr/hal-00919227

[42] S. Boche, G. Guette, C. Bidan, N. Prigent. *NoName, un protocole de routage ad hoc respectant la vie privée*, in "SAR-SSI 2013", Mont de Marsan, France, September 2013, pp. 122-134, http://hal.inria.fr/hal-00919178

[43] A. Guellier, C. Bidan, N. Prigent. *Protocole Ad hoc Proactif Anonyme à Base de Cryptographie Homomorphique*, in "SAR-SSSI 2013", Mont-de-Marsan, France, September 2013, 11 p. , http://hal.inria.fr/hal-00881049

Conferences without Proceedings

[44] E. Anceaume, E. Le Merrer, R. Ludinard, B. Sericola, G. Straub. *FixMe : détection répartie de défaillances isolées*, in "15èmes Rencontres Francophones sur les Aspects Algorithmiques des Télécommunications (AlgoTel)", Pornic, France, N. Nisse, F. Rousseau, Y. Busnel (editors), May 2013, pp. 1-4, http://hal.inria.fr/hal-00818650

[45] M. Assaf, J. Signoles, F. Tronel, E. Totel. *Moniteur hybride de flux d'information pour un langage supportant des pointeurs*, in "SARSSI - 8ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information", Mont de Marsan, France, September 2013, http://hal.inria.fr/hal-00909293

[46] A. Blandin-Obernesser, M. Boizard, S. Gambs, G. Piolle. *Le droit à l'oubli : Présentation du projet DAO*, in "4ème Atelier sur la Protection de la Vie Privée (APVP'13)", Les Loges en Josas, France, June 2013, http://hal.inria.fr/hal-00845780

[47] S. Bouget, S. Gambs, G. Piolle. *Dégradation de données par publication éphémère*, in "4ème Atelier sur la Protection de la Vie Privée (APVP'13)", Les Loges en Josas, France, June 2013, http://hal.inria.fr/hal-00845567

Research Reports

[48] E. Anceaume, Y. Busnel. , *CoMMEDIA: Separating Scaramouche from Harlequin to Accurately Estimate Items Frequency in Distributed Data Streams*, June 2013, 16 pages, http://hal.inria.fr/hal-00847764

[49] R. Andriatsimandefitra, V. Viet Triem Tong, T. Saliou. , *Information Flow Policies vs Malware*, September 2013, http://hal.inria.fr/hal-00862468

[50] M. Assaf, J. Signoles, F. Tronel, E. Totel. , *Moniteur hybride de flux d'information pour un langage supportant des pointeurs*, Inria, July 2013, n^{o} RR-8326, 25 p. , http://hal.inria.fr/hal-00841048

Other Publications

[51] E. Anceaume, G. Guette, P. Lajoie Mazenc, T. Sirvent, V. Viet Triem Tong. , *Extending Signatures of Reputation*, June 2013, International Summer School with proceedings, http://hal.inria.fr/hal-00907394

[52] C. Humphries, N. Prigent, C. Bidan, F. Majorczyk. , *Vers une catégorisation par objectif des outils de visualisation pour la sécurité*, September 2013, Poster, http://hal.inria.fr/hal-00919211

References in notes

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

[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] 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

[56] 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

[57] A. Myers, F. Schneider, K. Birman. , *Nsf project security and fault tolerance, nsf cybertrust grant 0430161*, 2004, http://www.cs.cornell.edu/Projects/secft/

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

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

[60] 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