IN PARTNERSHIP WITH:
Institut national des sciences appliquées de Lyon

Activity Report 2013

Team PRIVATICS

Privacy Models, Architectures and Tools for the Information Society

RESEARCH CENTER
Grenoble - Rhône-Alpes

THEME
Security and Confidentiality

Table of contents

Team PRIVATICS

Keywords: Privacy, Security, Cryptography, Networks, Formal Methods

Creation of the Team: 2013 January 01.

1. Members

Research Scientists

Claude Castelluccia [Team Leader, Inria, Senior Researcher, HdR]
Mohamed Ali Kaafar [Inria, Researcher, from Aug 2013]
Cédric Lauradoux [Inria, Researcher]
Daniel Le Métayer [Inria, Senior Researcher, HdR]
Vincent Roca [Inria, Researcher]

Faculty Members

Mathieu Cunche [INSA Lyon, Associate Professor]
Marine Minier [INSA Lyon, Associate Professor, HdR]

Engineers

Gergely Acs [Inria]
James-Douglass Lefruit [Inria]

PhD Students

Ludovic Jacquin [Inria, until Sep 2013]
Jagdish Achara [Inria]
Thibaud Antignac [Inria]
Abdelberi Chaabane [Inria, granted by ANR ARESA2 project3]
Jessye Dos Santos [CEA, from Oct 2013]
Hicham Hossayni [CEA, from Feb 2013 until Sep 2013]
Amrit Kumar [Univ. Grenoble I, from Nov 2013]
Ferdaouss Mattoussi [Inria, granted by Alcatel-Lucent Bell Labs]
Lukasz Olejnik [Inria]
Minh-Dhung Tran [Univ. Grenoble I]
Dong Wang [Inria]

Post-Doctoral Fellows

Denis Butin [Inria, granted by FP7 PARIS project]
Christophe Lazaro [Inria, granted by FP7 PARIS project3]
Kazuhisa Matsuzono [Inria, granted by ANR ARSSO project, from Feb 2013 until Nov 2013]

Administrative Assistant

Helen Pouchot [Inria]

Other

Levent Demir [Inria, Intern, from Mar 2013 until Sep 2013]

2. Overall Objectives

2.1. Context

The promises of new technologies: Many advances in new technologies are very beneficial to the society and provide services that can drastically improve life's quality. A good example is the emergence of reality mining. Reality mining is a new discipline that infers human relationships and behaviors from information collected by cell-phones. Collected information include data collected by the sensors, such as location or physical activities, as well as data recorded by the phones themselves, such as call duration and dialed numbers. Reality mining could be used by individuals to get information about themselves, their state or performances ("quantified self"). More importantly, it could help monitoring health. For example, the motions of a mobile phone might reveal changes in gait, which could be an early indicator of ailments or depression. The emergence of location-based or mobile/wireless services is also often very beneficial. These systems provide very useful and appreciated services, and become almost essential and inevitable nowadays. For example, RFID cards allow users to open doors or pay their metro tickets. GPS systems help users to navigate and find their ways. Some services tell users where their friends are or provide services personalized to their current location (such as indicating the closest restaurant or hotel). Some wireless parking meters send users a text message when their time is running out. The development of smart grids, smart houses, or more generally smart spaces/environments, can also positively contribute to the well-being of the society. Smart-grids and smart houses attempt to minimize energy consumption by monitoring users' energy consumptions and applying adequate actions. These technologies can help reducing pollution and managing energy resources.

Privacy threats of new technologies: While the potential benefits provided by these systems are numerous, they also pose considerable privacy threats that can potentially turn new technologies into a nightmare. Most of these systems leave digital traces that can potentially be used to profile or monitor users. Content on the Internet (documents, emails, chats, images, videos etc) is often disseminated and replicated on different peers or servers. As a result, users lose the control of their content as soon as they release it. Furthermore most users are unaware of the information that is collected about them beyond requested data. It was shown that consumption data provided by smart meters to electricity providers is so accurate that it can be used to infer physical activities (e.g. when the house occupant took a shower or switched-on TV). Also, a picture taken by a user may reveal additional contextual information inferred from the background or the style of any associated text. For example, photos and videos taken with smart phones or cameras contain geo-location information. This may be considered as a potential source of information leakage and may lead to a privacy breach if used for location tracking or in conjunction with data retrieved from OSN (Online Social Networks). The risk becomes higher as the border between OSN and LBS (Location Based Services) becomes fuzzier. For instance, OSN such as FourSquare and Gowalla are designed to encourage users to share their geolocated data. Information posted on social applications such as T witter can be used to infer whether or not an individual is at home. Other applications, such as Google Latitude, allow users to track the movements of their friends' cellphones and display their position on a map. In addition to social applications, there are other public sources of information that can be exploited by potential adversaries, such as the free geographic data provided by Google Maps, Yahoo! Maps and Google Earth. The danger is to move into a surveillance society where all our online and physical activities are recorded and correlated. Some companies already offer various services that gather different types of information from users. The combination and concentration of all these information provide a powerful tool to accurately profile users. For example, Google is one of the main third-party aggregators and tracks users across most web sites [30]. In addition, it also runs the most popular search engine and, as such, stores web histories of most users (i.e. their search requests), their map searches (i.e. their requests to the Google Map service), their images and so on [8]. Web searches have been shown to often be sensitive. Furthermore, Google is also going into the mobile and energy business, which will potentially allow it to correlate online profile with physical profiles.

The "internet of the future" should solve these privacy problems. How- ever, privacy is not something that occurs naturally online, it must be deliberately designed. This architecture of Privacy must be updated and reconsidered as the concept of privacy evolves and new technologies appear.

2.2. Highlights of the Year

The project Mobilitics has made significant advances in the context the Inria-CNIL convention in 2013. Major improvements have been made in the software, which include new capabilities and improved analysis (even for encrypted streams) for the two major systems that are iOS 6.2 and Android 4.1. A first phase of experiments for iOS took place in early 2013 with volunteers from the CNIL. It resulted in a press conference (April 2013) and a large media exposure. A second phase of experiments will take place in 2014 for Android. More targeted work on the our side also led to advances in understanding the ecosystem of mobile applications and the flows of personal information.

We have published at CODASPY 2013 [33] a new formal framework for the analysis of architectural choices. The privacy by design approach has already been put into practice in different application areas. We believe that the next challenge today is to go beyond individual cases and to provide methodologies to explore the design space in a systematic way. As a first step in this direction, we focus on the data minimization principle and consider different options using decentralized architectures in which actors do not necessarily trust each other. We propose a framework to express the parameters to be taken into account (the service to be performed, the actors involved, their respective requirements, etc.) and an inference system to derive properties such as the possibility for an actor to detect potential errors (or frauds) in the computation of a variable. This inference system can be used in the design phase to check if an architecture meets the requirements of the parties or to point out conflicting requirements.

Even if our main goal is to develop general techniques with a potentially broad impact, Privatics will consider different and various concrete case studies to ensure the relevance and significance of its results. We plan to work on several case studies related to the Internet, online social networks (OSN), mobile services and smart spaces/environments (such as smart grids, smart houses,..), which correspond to challenging application domains with great impact on society.

3. Application Domains

3.1. Domain 1: Privacy in smart environments.

Privacy in smart environments. One illustrative example is our latest work on privacy-preserving smart-metering [2]. Several countries throughout the world are planning to deploy smart meters in house-holds n the very near future. Traditional electrical meters only measure total consumption on a given period of time (i.e., one month or one year). As such, they do not provide accurate information of when the energy was consumed. Smart meters, instead, monitor and report consumption in intervals of few minutes. They allow the utility provider to monitor, almost in real-time, consumption and possibly adjust generation and prices according to the demand. Billing customers by how much is consumed and at what time of day will probably change consumption habits to help matching energy consumption with production. In the longer term, with the advent of smart appliances, it is expected that the smart grid will remotely control selected appliances to reduce demand. Although smart metering might help improving energy management, it creates many new privacy problems. Smart-meters provide very accurate consumption data to electricity providers. As the interval of data collected by smart meters decreases, the ability to disaggregate low-resolution data increases. Analysing high-resolution consumption data, Non-intrusive Appliance Load Monitoring (NALM) can be used to identify a remarkable number of electric appliances (e.g., water heaters, well pumps, furnace blowers, refrigerators, and air conditioners) employing exhaustive appliance signature libraries. We developed DREAM, DiffeRentially privatE smArt Metering, a scheme that is private under the differential privacy model and therefore provides strong and provable guarantees. With our scheme, an (electricity) supplier can periodically collect data from smart-meters and derive aggregated statistics while learning only limited information about the activities of individual households. For example, a supplier cannot tell from a user's trace when he watched TV or turned on heating.

3.2. Domain 2: Big Data and Privacy

We believe that another important problem will be related to privacy issues in big data. Public datasets are used in a variety of applications spanning from genome and web usage analysis to location-based and recommendation systems. Publishing such datasets is important since they can help us analyzing and understanding interesting patterns. For example, mobility trajectories have become widely collected in recent years and have opened the possibility to improve our understanding of large-scale social networks by investigating how people exchange information, interact, and develop social interactions. With billion of handsets in use worldwide, the quantity of mobility data is gigantic. When aggregated, they can help understand complex processes, such as the spread of viruses, and build better transportation systems. While the benefits provided by these datasets are indisputable, they unfortunately pose a considerable threat to individual privacy. In fact, mobility trajectories might be used by a malicious attacker to discover potential sensitive information about a user, such as his habits, religion or relationships. Because privacy is so important to people, companies and researchers are reluctant to publish datasets by fear of being held responsible for potential privacy breaches. As a result, only very few of them are actually released and available. This limits our ability to analyze such data to derive information that could benefit the general public. It is now an urgent need to develop Privacy-Preserving Data Analytics (PPDA) systems that collect and transform raw data into a version that is immunized against privacy attacks but that still preserves useful information for data analysis. This is one of the objectives of Privatics. There exists two classes of PPDA according to whether the entity that is collecting and anonymizing the data is trusted or not. In the trusted model, that we refer to as Privacy-Preserving Data Publishing (PPDP), individuals trust the publisher to which they disclose their data. In the untrusted model, that we refer to as Privacy-Preserving Data Collection (PPDC), individuals do not trust the data publisher. They may add some noise to their data to protect sensitive information from the data publisher.

Privacy-Preserving Data Publishing: In the trusted model, individuals trust the data publisher and disclose all their data to it. For example, in a medical scenario, patients give their true information to hospitals to receive proper treatment. It is then the responsibility of the data publisher to protect privacy of the individuals' personal data. To prevent potential data leakage, datasets must be sanitized before possible release. Several proposals have been recently proposed to release private data under the Differential Privacy model [25, 56, 26, 57, 50]. However most of these schemes release a "snapshot" of the datasets at a given period of time. This release often consists of histograms. They can, for example, show the distributions of some pathologies (such as cancer, flu, HIV, hepatitis, etc.) in a given population. For many analytics applications, "snapshots" of data are not enough, and sequential data are required. Furthermore, current work focusses on rather simple data structures, such as numerical data. Release of more complex data, such as graphs, are often also very useful. For example, recommendation systems need the sequences of visited websites or bought items. They also need to analyse people connection graphs to identify the best products to recommend. Network trace analytics also rely on sequences of events to detect anomalies or intrusions. Similarly, traffic analytics applications typically need sequences of visited places of each user. In fact, it is often essential for these applications to know that user A moved from position 1 to position 2, or at least to learn the probability of a move from position 1 to position 2. Histograms would typically represent the number of users in position 1 and position 2, but would not provide the number of users that moved from position 1 to position 2. Due to the inherent sequentiality and high-dimensionality of sequential data, one major challenge of applying current data sanitization solutions on sequential data comes from the uniqueness of sequences (e.g., very few sequences are identical). This fact makes existing techniques result in poor utility. Schemes to privately release data with complex data structures, such as sequential, relational and graph data, are required. This is one the goals of Privatics. In our current work, we address this challenge by employing a variable-length n-gram model, which extracts the essential information of a sequential database in terms of a set of variable-length n - grams [15]. We then intend to extend this approach to more complex data structures.

Privacy-Preserving Data Collection: In the untrusted model, individuals do not trust their data publisher. For example, websites commonly use third party web analytics services, such as Google Analytics to obtain aggregate traffic statistics such as most visited pages, visitors' countries, etc. Similarly, other applications, such as smart metering or targeted advertising applications, are also tracking users in order to derive aggregated

information about a particular class of users. Unfortunately, to obtain this aggregate information, services need to track users, resulting in a violation of user privacy. One of our goals is to develop Privacy-Preserving Data Collection solutions. We propose to study whether it is possible to provide efficient collection/aggregation solutions without tracking users, i.e. without getting or learning individual contributions.

4. Software and Platforms

4.1. Mobilitics

Mobilitics is a joint project, started in 2012 between Inria and CNIL, which targets privacy issues on smartphones. The goal is to analyze the behavior of smartphones applications and their operating system regarding users private data, that is, the time they are accessed or sent to third party companies usually neither with user's awareness nor consent.

In the presence of a wide range of different smartphones available in terms of operating systems and hardware architecture, Mobilitics project focuses actually its study on the two more widespread mobile platforms which are IOS(Iphone) and Android.

Indeed, both versions of Mobilitics software should provide these common requirements: Be able to capture any event about private data access such as User location, Device Unique Identifier, Address Book... Store these events in a local database on the phone for offline analysis Send this local database to Mobilitics server for privacy leakage statistics

A Mobilitics prototype for Iphone has been developed since January 2012 at Privatics. It has already embedded the features listed above and much more. However, a separate prototype for Android has been also developed since September 2012 fulfilling the same equirements listed above because IOS and Android are different in either software or hardware level.

Indeed, some live experiments have been conducted by CNIL with Mobilitics prototype for IOS with the help of volunteers equipped with iphones which they have used for a period of four(4) months(September 2012-January 2013). As a result, some visualization tools have been developed for the data collected in order to showcase private data leakage by the apps which the participants of the experiment have used. Therefore, a press conference has been held by CNIL in Paris in April 2013 during which Mobilitics results for Iphone have been published onto several French newspapers (see Section 8.3)

Likewise, some live experiments will be conducted on Android this year in February 2014 for at least three(3) months with volunteers equipped with Galaxy Nexus smartphones on which Mobilitics will be deployed. As a consequence, a press release by CNIL will be scheduled for the publication of the results obtained for Android with a perspective of comparing Google privacy policy to Apple one.

5. New Results

5.1. Online Social Networks Tracking

Participants: Mohamed Ali Kaafar, Abdelberi Chaabane.

Behavioural advertisement, profiling, adver-gaming and social advertisement illustrate how user personal information and social relations have been integrated to the market model. In other words, user information is *commodified*: the user identity becomes a commodity to be sold and bought. This radical change raises several privacy questions and leads to clamouring for better understanding, regulation and protection of user privacy. Within this context, there is both a long-term and a short-term dimension to our work. For the sort term, I showed that OSN can present a real threat to user privacy as the *full* control of user data – both access and dissemination – is hard to achieve. For the long term, our work calls for a better educational approach to privacy as well as a stricter regulation.

5.2. Behavioural advertisement

Participants: Mohamed Ali Kaafar, Abdelberi Chaabane.

Online Social Networks Tracking. I examined web user tracking capabilities of the three major global OSNs. I studied the mechanisms which enable these services to persistently and accurately follow users web activity, and evaluate to which extent this phenomena is spread across the web. Through a study of the top 10K websites, our findings indicate that OSN tracking is diffused among almost all website categories, independently from the content and the audience. I also evaluated the tracking capabilities in practice and demonstrated – by analysing a real traffic traces – that OSNs can reconstruct a significant portion of users web profile and browsing history. I finally provided insights into the relation between the browsing history characteristics and the OSN tracking potential, highlighting the high risk properties. This work shows that web tracking in combination with personal information from social networks represents a serious privacy violation that shifts the tracking from a virtual tracking (i.e. the user is virtual) to a real "physical" tracking (i.e. based on user personal information).

5.3. Selling Off Privacy at Auction

Participants: Claude Castelluccia, Lukasz Olejnik, Cédric Lauradoux, Minh-Dung Tran.

The first one is a privacy analysis of Real-Time Bidding (RTB) and Cookie Matching (CM). RTB is a technology that allows ad buyers (advertisers) and ad sellers (publishers) to buy and sell ad spaces at real-time auctions through ad exchanges. In RTB, when user visits a publisher page, the ad impression (i.e. one ad display in an ad space) and the user information are immediately broadcast by the ad exchange to a number of bidders (i.e. advertisers or their representatives) for them to bid for the chance to serve ads to this user. CM protocol allows the ad exchange and the bidder to synchronize their cookies of the same user, thus facilitating their exchange of user data.

In [41], we characterize and quantify the potential user web history leakage from ad exchanges to bidders in RTB as a result of exchanging user data. We also discuss and quantify the extent to which companies can potentially collude to increase their tracked user profiles using CM. In addition, we leverage a design characteristic of RTB to observe the winning price of each RTB auction. By analyzing these prices, we show how advertisers evaluate the value of user privacy. This work (titled Selling Off Privacy at Auction) will be presented in NDSS 2014, San Diego, USA in February, 2014.

5.4. Wi-Fi and privacy

Participants: Cédric Lauradoux, Mathieu Cunche, Levent Demir.

Active service discovery in Wi-Fi involves wireless stations broadcasting their Wi-Fi fingerprint, i.e. the SSIDs of their preferred wireless networks. The content of those Wi-Fi fingerprints can reveal different types of information about the owner. In [5], we focus on the relation between the fingerprints and the links between the owners. Our hypothesis is that social links between devices owners can be identified by exploiting the information contained in the fingerprint. More specifically we propose to consider the similarity between fingerprints as a metric, with the underlying idea: similar fingerprints are likely to be linked. We have studied the performances of several similarity metrics on a controlled dataset and then apply the designed classifier to a dataset collected in the wild. Our study is based on a dataset collected in Sydney, Australia, composed of fingerprints belonging to more than 8000 devices.

Extending this problem, we present a set of attacks that allow an attacker to link a Wi-Fi device to its owner identity. We present two methods that, given an individual of interest, allow identifying the MAC address of its Wi-Fi enabled portable device. Those methods do not require a physical access to the device and can be performed remotely, reducing the risks of being noticed. We present in [4], [35] scenarios in which the knowledge of an individual MAC address could be used for mischief.

5.5. Sensor security and privacy

Participants: Claude Castelluccia, Marine Minier, Cédric Lauradoux, Mathieu Cunche.

Wireless sensor networks (WSNs) are composed of a large number of low-cost, low-power, and multi-functional sensor nodes that communicate at short distance through wireless links. They are usually deployed in an open and uncontrolled environment where attackers may be present. Due to the use of low-cost materials, hardware components are not tamper-resistant and an adversary could access to a sensor's internal state.

In [7], we consider packet pollution attack. Packet pollution attack is considered as the most threatening attack model against network coding based sensor networks. A widely held belief says that, in a single source multi-destination dissemination scenario, the total number of polluted packets in the network will grow with the length of the transmission path, and the decoding failure (DF) rate at the further destination nodes are relatively lower. In this work, we first obtain an opposite result by analyzing the pollution attack in multicast scenarios, and find out a convergence trend of pollution attack by network coding system, and quantify the network resiliency against the pollution attacks which happen at any place along the source-destination paths. Then, the analysis result is proved by our simulations on two most widely deployed buffer strategies, Random-In Random-Out (RIRO) and First-in First-Out (FIFO). Finally, it is proved that RIRO has a much advanced security feature than FIFO in constraining the pollution attack gradually, and almost vanished in the end.

An adversary can easily capture even a single node and inserts duplicated nodes at any location in the network. If no specific detection mechanisms are established, the attacker could lead many insidious attacks such as subverting data aggregation protocols by injecting false data, revoking legitimate nodes and disconnecting the network if the replicated nodes are judiciously placed in the network. In [8], we first introduce the algorithm already published in PIMRC 2009 that describes a new hierarchical distributed algorithm for detecting node replication attacks using a Bloom filter mechanism and a cluster head selection. This mechanism could be efficiently used in a WSN as soon as the network is built with a clustering algorithm creating a three tiers hierarchy. We extend the results of our previous results by a theoretical discussion on the bounds of our algorithm. We also perform extensive simulations of our algorithm for random topologies and we compare those results with other proposals of the literature. Finally we show the effectiveness of our algorithm and its energy efficiency.

Finding entropy sources is a major issue to design non-deterministic random generators for headless devices. Our goal in [22] is to evaluate a collection of sensors (e.g. thermometer, accelerometer, magnetometer) as potential sources of entropy. A challenge in the analysis of these sources is the estimation of min-entropy. We have followed the NIST recommendations to obtain pessimistic estimations from the dataset collected during our campaign of experiments. The most interesting sensors of our study are: the accelerometer, the magnetometer, the vibration sensor and the internal clock. Contrary to previous results, we observe far less entropy than it was expected before. Other sensors which measures phenomena with high inertia such as the temperature or air pressure provide very little entropy.

In [12], we propose a key certification protocol for wireless sensor networks that allows nodes to autonomously exchange their public keys and verify their authenticity using one-way accumulators. We examine and compare different accumulator implementations for our pro- tocol on the Sun SPOT platform. We observe that our protocol performs best with accumulators based on Elliptic Curve Cryptography (ECC): ECC-based accumulators have roughly the same speed as Secure Bloom filters, but they have a smaller memory footprint.

5.6. Buidling blocks

Participant: Marine Minier.

In [17], we develop a complete library of lightweight block ciphers dedicated to security applications in wireless sensor networks (WSNs). Choosing best algorithms in terms of energy-efficiency and of small memory requirements is a real challenge because the sensor networks must be autonomous. We study on a dedicated platform of sensors most of the recent lightweight block ciphers as well as some conventional block ciphers. First, we describe the design of the chosen block ciphers with a security summary and we then present some implementation tests performed on our platform. The library is available online: http://bloc.project.citi-lab.fr/library.html.

In [23], we present two related key impossible differential attacks against 14 rounds of Piccolo-80 and 21 rounds of Piccolo-128 without the whitening layers. Piccolo is a new lightweight block cipher proposed by SONY at CHES 2011. The attack against Piccolo-80 has a time and data complexity of $2^{68.19}$ whereas the time/data complexity of the attack against Piccolo-128 is $2^{117.77}$.

While Generalized Feistel Networks have been widely studied in the literature as a building block of a block cipher, we propose in [13] a unified vision to easily represent them through a matrix representation. We then propose a new class of such schemes called Extended Generalized Feistel Networks well suited for cryptographic applications. We instantiate those proposals into two particular constructions and we finally analyze their security.

We also obtain, in [24] a result concerning an integral distinguisher on the SHA-3 finalist Grøstl-512 v3.

5.7. Formal and legal issues of privacy

Participants: Thibaud Antignac, Denis Butin, Daniel Le Métayer.

- **Privacy by design** The privacy by design approach is often praised by lawyers as well as computer scientists as an essential step towards a better privacy protection. The general philosophy of privacy by design is that privacy should not be treated as an afterthought but rather as a first-class requirement during the design of a system. The approach has been applied in different areas such as smart metering, electronic traffic pricing, ubiquitous computing or location based services. More generally, it is possible to identify a number of core principles that are widely accepted and can form a basis for privacy by design. For example, the Organization for Economic Co-operation and Development (OECD) has put forward principles such as the consent, limitation of use, data quality, security and accountability. One must admit however that the take-up of privacy by design in the industry is still rather limited. This situation is partly due to legal and economic reasons: as long as the law does not impose binding commitments, ICT providers and data collectors do not have sufficient incentives to invest into privacy by design. The situation on the legal side might change in Europe though because the regulation proposed by the European Commission in January 2012 (to replace the European Directive 95/46/EC), which is currently under discussion, includes binding commitments on privacy by design.

  But the reasons for the lack of adoption of privacy by design are not only legal and economic: even though computer scientists have devised a wide range of privacy enhancing tools, no general methodology is available to integrate them in a consistent way to meet a set of privacy requirements. The next challenge in this area is thus to go beyond individual cases and to establish sound foundations and methodologies for privacy by design. As a first step in this direction, we have focused on the data minimization principle which stipulates that the collection should be limited to the pieces of data strictly necessary for the purpose, and we have proposed a framework to reason about the choices of architecture and their impact in terms of privacy. The first strategic choices are the allocation of the computation tasks to the nodes of the architecture and the types of communications between the nodes. For example, data can be encrypted or hashed, either to protect their confidentiality or to provide guarantees with respect to their correctness or origin. The main benefit of a centralized architecture for the "central" actor is that he can trust the result because he keeps full control over its computation. However, the loss of control by a single actor in decentralized architectures can be offset by extra requirements ensuring that errors (or frauds) can be detected *a posteriori*. In order to help the designer grasp the combination of possible options, our framework provides means to express the parameters to be taken into account (the service to be performed, the actors involved, their respective requirements, etc.) and an inference system to derive properties such as the possibility for an actor to detect potential errors (or frauds) in the computation of a variable. This inference system can be used in the design phase to check if an architecture meets the requirements of the parties or to point out conflicting requirements.
- **Accountability**

The principle of accountability, which was introduced three decades ago in the OECD guidelines, has been enjoying growing popularity over the last few years as a solution to mitigate the loss of control by increasing transparency of data processing. At the European level, the Article 29 Working Group published an opinion dedicated to the matter two years ago and the principle is expected to be enshrined in the upcoming European data protection regulation. But the term "accountability" is used with different meanings by different actors and the principle itself has been questioned by some authors as providing deceptive protections and also possibly introducing new risks in terms of privacy. We have studied the different interpretations of the notion of accountability following a multidisciplinary approach and we have argued that *strong accountability* should be a cornerstone of future data protection regulations. By *strong accountability* we mean a principle of accountability which

- applies not only to policies and procedures, but also to practices, thus providing means to oversee the effective processing of the personal data, not only the promises of the data controller and its organisational measures to meet them;
- is supported by precise binding commitments enshrined in law;
- involves audits by independent entities.

Strong accountability should benefit all stakeholders: data subjects, data controllers, and even data protection authorities whose workload should be considerably streamlined.

But accountability is a requirement to be taken into account from the initial design phase of a system because of its strong impact on the implementation of the log architecture. Using real-world scenarios, we have shown that decisions about log architectures are actually nontrivial. We have addressed the question of what information should be included in logs to make their a posteriori compliance analysis meaningful. We have shown how log content choices and accountability definitions mutually affect each other and incites service providers to rethink up to what extent they can be held responsible. These different aspects are synthesized into guidelines to avoid common pitfalls in accountable log design. This analysis is based on case studies performed on our implementation of the PPL policy language.

- **Verification of privacy properties** The increasing official use of security protocols for electronic voting deepens the need for their trustworthiness, hence for their formal verification. The impossibility of linking a voter to her vote, often called voter privacy or ballot secrecy, is the core property of many such protocols. Most existing work relies on equivalence statements in cryptographic extensions of process calculi. We have proposed the first theorem-proving based verification of voter privacy which overcomes some of the limitations inherent to process calculi-based analysis. Unlinkability between two pieces of information is specified as an extension to the Inductive Method for security protocol verification in Isabelle/HOL. New message operators for association extraction and synthesis are defined. Proving voter privacy demanded substantial effort and provided novel insights into both electronic voting protocols themselves and the analysed security goals. The central proof elements have been shown to be reusable for different protocols with minimal interaction.
- **Privacy and discrimination**

  The interactions between personal data protection, privacy and protection against discriminations are increasingly numerous and complex. For example, there is no doubt that misuses of personal data can adversely affect privacy and self-development (for example, resulting in the unwanted disclosure of personal data to third parties, in identity theft, or harassment through email or phone calls), or lead to a loss of choices or opportunities (for example, enabling a recruiter to obtain information over the Internet about political opinions or religious beliefs of a candidate and to use this information against him). It could even be suggested that privacy breaches and discriminations based on data processing are probably the two most frequent and the most serious types of consequences of personal data breaches. We have studied these interactions from a multidisciplinary (legal and technical) perspective and argued that an extended application of the application of non-discrimination regulations could help strengthening data protection. We have have analysed and

compared personal data protection, privacy and protection against discriminations considering both the types of data concerned and the *modus operandi* (*a priori* versus *a posteriori* controls, actors in charge of the control, etc.). From this comparison, we have drawn some conclusions with respect to their relative effectiveness and argued that *a posteriori* controls on the use of personal data should be strengthened and the victims of data misuse should get compensations which are significant enough to represent a deterrence for data controllers. We have also advocated the establishment of stronger connections between anti-discrimination and data protection laws, in particular to ensure that any data processing leading to unfair differences of treatments between individuals is prohibited and can be effectively punished.

6. Bilateral Contracts and Grants with Industry

6.1. Bilateral Contracts with Industry

6.1.1. XDATA

Title: XDATA.

Type: FUI.

Duration: April 2013 - April 2015.

Coordinator: Data Publica

Others partners: Inria, Orange, EDF, LaPoste, Hurance, Cinequant, IMT.

See also: http://www.xdata.fr/.

Abstract: The X-data project is a “projet investissements d’avenir” on big data with Data Publica (leader), Orange, La Poste, EDF, Cinequant, Hurence and Inria (Indes, Privatics and Zenith) . The goal of the project is to develop a big data plaftform with various tools and services to integrate open data and partners’s private data for analyzing the location, density and consuming of individuals and organizations in terms of energy and services. In this project, the Zenith team leads the workpackage on data protection and anonymization.

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. Privamov’

Title: Privamov’

Type: Labex IMU.

Duration: September 2013 - 2015.

Coordinator: LIRIS.

Others partners: EVS-ITUS, Inria Urbanets.

Abstract: The objective of this project is to provide researchers the IMU community traces of urban mobility allowing further their research and validate their assumptions and models. Indeed , many communities need to know the modes of urban transport : sociologists, philosophers , geographers, planners or computer scientists. If these traces are an important feature for researchers or industrial, they are more for users who have helped to build: attacks jeopardize the privacy of users. Anonymization techniques developed within the project will make available to the greatest number of these traces, while ensuring that the entire process (from collection to data analysis) will be made in respect of the privacy of users involved.

7.1.2. SCCyPhy

Title: SCCyPhy

Type: Labex Persyval.

Duration: September 2013 - 2015.

Coordinator: Institut Fourier.

Others partners: Inria MOAIS, Verimag, CEA/LETI, LIG, GIPSA-Lab, TIMA.

Abstract: A main motivation of this action-team is to provide a structure to the Grenoble community in computer security and cryptography in the spirit of the PERSYVAL-lab Labex. Our emphasize, within the PCS workpackage, is around complementary areas of research with high impact for science and technology, with the following target applications: embedded systems (including smartphones and sensors network), at both software and hardware levels, distributed architectures (including “cloud” and “sky”), privacy and protection of information systems against cyberattacks of various origins.

7.2. National Initiatives

7.2.1. ANR

7.2.1.1. BIOPRIV

Title: Application of privacy by design to biometric access control.

Type: ANR.

Duration: April 2013 - March 2017.

Coordinator: Morpho (France).

Others partners: Morpho (France), Inria (France), Trusted Labs (France).

See also: http://planete.inrialpes.fr/biopriv/.

Abstract: The objective of BIOPRIV is the definition of a framework for privacy by design suitable for the use of biometric technologies. The case study of the project is biometric access control. The project will follow a multidisciplinary approach considering the theoretical and technical aspects of privacy by design but also the legal framework for the use of biometrics and the evaluation of the privacy of the solutions.

7.2.1.2. BLOC

Title: Analysis of block ciphers dedicated to constrained environments.

Type: ANR.

Duration: October 2013 - September 2015.

Coordinator: INSA-Lyon (France).

Others partners: CITI Laboratory XLIM Laboratory, University of Limoges, Inria Secret, CryptoExperts (PME).

See also: http://bloc.project.citi-lab.fr/.

Abstract: BLOC aims at studying the design and analysis of block ciphers dedicated to constrained environments. The four milestones of BLOC are: security models and proofs, cryptanalysis, design and security arguments and performance analyzes and implementations of lightweight block ciphers. The aims of the project are the following ones: Security models and proofs Cryptanalysis Design C library of lightweight block ciphers We also aim at providing at the end of the project a lightweight block cipher proposal.

7.2.1.3. pFlower

Title: Parallel Flow Recognition with Multi-Core Processor.

Type: ANR.

Duration: March 2011 - September 2014.

Coordinator: LISTIC Université de Savoie.

Others partners: ICT-CAS Insititute of Computing Technology (China), LISTIC Université de Savoie.

Abstract: The main objective of this project is to take advantage of powerful parallelism of multi-thread, multi-core processors, to explore the parallel architecture of pipelined-based flow recognition, parallel signature matching algorithms.

7.2.2. Other

7.2.2.1. MOBILITICS

Title: MOBILITICS

Type: joint project.

Duration: January 2012 - Ongoing.

Coordinator: CNIL.

Others partners: CNIL.

Abstract: Platform for mobile devices privacy evaluation. This project strives to deploy an experimental mobile platform for studying and analyzing the weaknesses of current online (smartphone) applications and operating systems and the privacy implications for end-users. For instance, one of the objectives is to understand trends and patterns collected when they are aimed at obtaining general knowledge that does not pertain to any specific individual. Examples of such tasks include learning of commuting patterns, inference of recommendation rules, and creation of advertising segments.

7.2.2.2. MOBILITICS

Title: MOBILITICS

Type: joint project.

Duration: January 2012 - Ongoing.

Coordinator: CNIL.

Others partners: CNIL.

Abstract: Platform for mobile devices privacy evaluation. This project strives to deploy an experimental mobile platform for studying and analyzing the weaknesses of current online (smartphone) applications and operating systems and the privacy implications for end-users. For instance, one of the objectives is to understand trends and patterns collected when they are aimed at obtaining general knowledge that does not pertain to any specific individual. Examples of such tasks include learning of commuting patterns, inference of recommendation rules, and creation of advertising segments.

Inria Mobilitics (2011-2012): as a joint national project with CNIL (the French national committee of Information freedom).

Collaborative Action CAPRIS (2011-2014): the Collaborative Action on the Protection of Privacy Rights in the Information Society (CAPRIS), is an Inria national project, which goal is to tackle privacy-related challenges and provide solutions to enhance the privacy protection in the Information Society. His main tasks are the identification of existing and future threats to privacy, and the design of appropriate measures to assess and quantify privacy.

7.3. European Initiatives

7.3.1. FP7 Projects

7.3.1.1. PRIPARE

Title: Preparing industry to privacy-by-design by supporting its application in research.

Type: COOPERATION (ICT).

Instrument: Support Action (SA).

Duration: October 2013 - September 2015.

Coordinator: Trialog (France).

Others partners: American University of Paris (France), Atos (Spain), Fraunhofer SIT (Germany), Galician Research and Development Center in Advanced Telecommunications (Spain), Inria (France), KU Leuven (Belgium), Trialog (France), Trilateral Research (UK), Universidad Politecnica de Madrid (Spain), University of Ulm (Netherlands), Waterford Institute of Technology (UK).

Abstract: the general goal of PRIPARE is to facilitate the application of privacy by design. To this aim, PRIPARE will support the practice of privacy by design by the ICT research community (to prepare for industry practice) and foster risk management culture through educational material targeted to a diversity of stakeholders. The project will specify a privacy by design software and systems engineering methodology combining a multidisciplinary expertise involving legal, engineering and business viewpoints. The project will also provide best practices material and educational material focusing on risk management of privacy for different target audiences (general public, policy makers, users, ICT students and professional). The project will also pave the way for future research by identifying gaps and providing recommendations for a research agenda for privacy by design.

7.3.1.2. PARIS

Title: Privacy preserving infrastructure for surveillance.

Type: COOPERATION (ICT).

Instrument: Specific Targeted Research Project (STREP).

Duration: January 2013 - December 2015.

Coordinator: Trialog (France).

Others partners: AIT (Austria), Inria (France), KU Leuven (Belgium), Trialog (France), Universidad de Malaga (Spain), Université de Namur (Belgium), Thales (France), Visual Tools (Spain).

See also: http://www.paris-project.org/.

Abstract: PARIS will define and demonstrate a methodological approach for the development of surveillance infrastructure which enforces the right of citizens for privacy, justice and freedom and takes into account the evolving nature of such rights (e.g. aspects that are acceptable today might not be acceptable in the future), and the social and ethical nature of such rights (e.g. perception of such rights varies). The methodological approach will be based on two pillars, first a theoretical framework for balancing surveillance and data protection which fully integrates the concept of accountability, and secondly an associated process for the design of surveillance systems which takes from the start privacy (i.e. Privacy by Design) and accountability (i.e. Accountability by Design).

7.3.2. Collaborations in European Programs, except FP7

7.3.2.1. FI-WARE

Title: Future Internet Ware.

Type: COOPERATION (ICT).

Defi: PPP FI: Technology Foundation: Future Internet Core Platform.

Instrument: Integrated Project (IP).

Duration: May 2011 - April 2014.

Coordinator: Telefonica. (Spain)

Others partners: SAP (Germany), IBM (Israel, Switzerland), Inria (France), Thales Communications (France), Telecom Italia (Italy), France Telecom (France), Nokia Siemens Networks (Germany, Hungary, Finland), Deutsche Telekom (Germany), Technicolor (France), Ericsson (Sweden), Atos Origin (Spain), Ingeneria Informatica (Italy), Alcatel-Lucent (Italy, Germany), Siemens (Germany), Intel (Ireland), NEC (United Kingdom), Fraunhofer Institute (Germany), University of Madrid (Spain), University of Duisburg (Germany), University of Roma La Sapienza (Italy), University of Surrey (United Kingdom).

See also: http://www.fi-ware.eu/.

Abstract: The goal of the FI-WARE project is to advance the global competitiveness of the EU economy by introducing an innovative infrastructure for cost-effective creation and delivery of services, providing high QoS and security guarantees. FI-WARE is designed to meet the demands of key market stakeholders across many different sectors, e.g., healthcare, telecommunications, and environmental services. The project unites major European industrial actors in an unique effort never seen before. The key deliverables of FI-WARE will deliver an open architecture and implementation of a novel service infrastructure, building upon generic and reusable building blocks developed in earlier research projects. This infrastructure will support emerging Future Internet (FI) services in multiple Usage Areas, and will exhibit significant and quantifiable improvements in the productivity, reliability and cost of service development and delivery - building a true foundation for the Future Internet.

7.4. International Initiatives

7.4.1. Inria International Labs

Title: Secure and Private Distributed Data Storage and Publication in the Future Internet

Inria principal investigator: Claude Castelluccia

International Partners (Institution - Laboratory - Researcher):

University of California Berkeley (United States) - Electrical Engineering and Computer Science Department - Edward Lee

University of California Irvine (United States) - Donald Bren School of Information and Computer Sciences - Gene Tsudik

Duration: 2012 - 2014

See also: http://planete.inrialpes.fr/cloudy-associated-team/

Cloud computing is a form of computing where general purpose clients (typically equipped with a web browser) are used to access resources and applications managed and stored on a remote server. Cloud applications are increasingly relied upon to provide basic services like e-mail clients, instant messaging and office applications. The customers of cloud applications benefit from outsourcing the management of their computing infrastructure to a third-party cloud provider. However, this places the customers in a situation of blind trust towards the cloud provider. The customer has to assume that the "cloud" always remains confidential, available, fault-tolerant, well managed, properly backed-up and protected from natural accidents as well as intentional attacks. An inherent reason for today's limitations of commercial cloud solutions is that end users cannot verify that servers in the cloud and the network in between are hosting and disseminating tasks and content without deleting, disclosing or modifying any content. This project seeks to develop novel technical solutions to allow customers to verify that cloud providers guarantee the confidentiality, availability and fault-tolerance of the stored data and infrastructure.

7.5. International Research Visitors

7.5.1. Visits to International Teams

Mohamed Ali Kaafar, spending a sabbatical at NICTA Australia in Sydney (since February 2012)

Subject: Online Privacy Enhancing Technologies: measuring the risks and designing countermeasures

8. Dissemination

8.1. Scientific Animation

8.1.1. Organization

Claude Castelluccia : WISEC 2014.

Mathieu Cunche : WISEC 2014.

Cédric Lauradoux : Colloque CAPPRIS-AFDIT, 11/09/2013, Lyon, http://planete.inrialpes.fr/capprisafdit.

Daniel Le Métayer : Colloque CAPPRIS-AFDIT, 11/09/2013, Lyon, http://planete.inrialpes.fr/capprisafdit.

Vincent Roca : SAR-SSI 2014.

8.1.2. Program committee

Claude Castelluccia : PETS 2013, WISEC 2013, POST 2013, SESOC 2013.

Mathieu Cunche : WCNC 2014.

Cédric Lauradoux : ACNS 2013, Cardis 2013, GreHack 2013, WISEC 2014.

Daniel Le Métayer : CPDP 2013, APF 2013, APVP 2013, WOSSAP 2013, SAR-SSI 2013.

Vincent Roca : SPACOMM 2014, SNDS 2014, SSCC 2013.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Undergraduate course : Vincent Roca, On Wireless Communications, 12h, L1, Polytech' Grenoble, France.

Undergraduate course : Vincent Roca, On Network Communications (24h), L1, IUT-2 (UPMF University) Grenoble, France.

Undergraduate course : Marine Minier, Probabilities, 50h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Signal Processing, 50h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Analysis, 50h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Introduction to Cryptography, 30h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Information Theory, 30h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, Micromachine, 20h, L3, INSA-Lyon, France.

Undergraduate course : Mathieu Cunche, Introduction to computer science, 120h, L1, INSA-Lyon, France.

Master : Claude Castelluccia, Wireless Security, 20h, M2, Ensimag/University of Grenoble, France.

Master : Claude Castelluccia, Wireless Security, 15h, M2, Ensimag/INPG, France.

Master : Marine Minier, Security for wireless networks, 10h, M2, INSA-Lyon, France.

Master : Mathieu Cunche, Wireless Security, 2h, M2, INSA-Lyon, France.

8.2.2. Supervision

PhD in progress : Jagdish Achara, Mobile devices and operating systems from a privacy point of view, October 2013, Vincent Roca and Claude Castelluccia.

PhD in progress : Thibaud Antignac, New solutions for a better privacy, September 2011, Daniel Le Métayer.

PhD in progress : Abdelberi Chaabane, Threats against privacy on Internet: evaluation and solutions, September 2010, Mohamed Ali Kaafar and Claude Castelluccia.

PhD in progress : Jessye Dos Santos, Wireless physical tracking, October 2013, Cédric Lauradoux and Claude Castelluccia.

PhD in progress : Amrit Kumar, Privacy and multiparty computation, November 2013, Cédric Lauradoux.

PhD in progress : Ferdaouss Mattoussi, Design and optimizations of AL-FEC: GLDPC-Staircase Codes, September 2010, Vincent Roca and Claude Castelluccia.

PhD in progress : Lukasz Olejnik, Internet Tracking and Profiling, October 2011, Claude Castelluccia.

PhD in progress : Vincent Primault, Privacy and geolocated services, November 2013, Cédric Lauradoux.

PhD in progress : Gael Thomas, Algebraic Automata in Symetric Cryptography, November 2011, Marine Minier.

PhD in progress : Minh-Dung Tran, Privacy-Preserving Ad systems, September 2011, Claude Castelluccia and Mohamed Ali Kaafar.

PhD in progress : Dong Wang, titre (provisoire) du mémoire, date du début de la thèse, Mohamed Ali Kaafar.

8.2.3. Juries

HdR : Marc-Olivier Killijian, Towards Resilient and Private Mobiquitous Systems, Toulouse, 20/02/2013, Claude Castelluccia.

PhD : Ahmed Benfarah, Security of a UWB-IR link, INSA-Lyon, 10/07/2013, Cédric Lauradoux.

PhD : Ludovic Jacquin, Efficiency/Security trade-off for High Bandwidth Internet Gateway, Grenoble, 20/11/2013, Vincent Roca and Claude Castelluccia.

PhD : Mohammad Nabil ALAGGAN, Private Peer-to-peer similarity computation in personalized collaborative platforms, Rennes, 16/12/2013, Daniel Le Métayer.

PhD : Sophie Guicherd, Le régime juridique applicable aux dysfonctionnements du logiciel, 05/12/2013, Daniel Le Métayer.

8.3. Popularization

Claude Castelluccia and Daniel Le Métayer, La vie privée, un obstacle à l'économie numérique ?, LeMonde.fr, 03.09.2013, http://www.lemonde.fr/economie/article/2013/08/25/la-vie-privee-un-obstacle-a-l-economie-numerique_3466139_3234.html.

Mathieu Cunche, Smartphone, Wi-Fi et vie privée : comment votre smartphone peut se révéler être votre pire ennemi [35], October 2013, MISCMAG.

Mathieu Cunche, Quand les terminaux mobiles jouent les mouchards de poche, Podcast Interstices, September 2013, https://interstices.info/jcms/ni_74624/quand-les-terminaux-mobiles-jouent-les-mouchards-de-poche.

Cédric Lauradoux and Levent Demir, Guesswork [40], October 2013, MISCMAG.

Mobilitics project, Paris Metro Tracks and Trackers: Why is the RATP App leaking my private data?

Mobilitics project, Voyage au cœur des smartphones et des applications mobiles avec la CNIL et Inria, 09/04/2013, bit.ly/M3cWCi.

9. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] L. JACQUIN. , *Compromis performance/sécurité des passerelles très haut débit pour Internet.*, Université de Grenoble, November 2013, http://hal.inria.fr/tel-00911075

[2] V. ROCA. , *Codes AL-FEC et protocoles de diffusion robuste de contenus : composants pour des services performants et passant à l'échelle*, Université de Grenoble, April 2014, version 1.0, 30 décembre 2013, http://hal.inria.fr/tel-00925955

Articles in International Peer-Reviewed Journals

[3] A. CHAABANE, E. DE CRISTOFARO, M. A. KAAFAR, E. UZUN. *Privacy in Content-Oriented Networking: Threats and Countermeasures*, in "ACM Computer Communication Review", July 2013, pp. 167–174, http://hal.inria.fr/hal-00939179

[4] M. CUNCHE. *I know your MAC address: targeted tracking of individual using Wi-Fi*, in "Journal of Computer Virology and Hacking Techniques", December 2013 [*DOI :* 10.1007/s11416-013-0196-1], http://hal.inria.fr/hal-00923467

[5] M. CUNCHE, M. A. KAAFAR, R. BORELI. *Linking wireless devices using information contained in Wi-Fi probe requests*, in "Pervasive and Mobile Computing", 2013 [*DOI :* 10.1016/J.PMCJ.2013.04.001], http://hal.inria.fr/hal-00816374

[6] L. OLEJNIK, C. CASTELLUCCIA, A. JANC. *On the Uniqueness of Web Browsing History Patterns*, in "Annales des Télécommunications", September 2013 [*DOI :* 10.1007/s12243-013-0392-5], http://hal.inria.fr/hal-00917042

[7] Y. ZHANG, M. MINIER. *How network coding system constrains packet pollution attacks in wireless sensor networks*, in "IJGUC - International Journal of Grid and Utility Computing", 2013, vol. 4, n^{o} 2/3, pp. 197-203, http://hal.inria.fr/hal-00918953

[8] W. ZNAIDI, M. MINIER, S. UBÉDA. *Hierarchical Node Replication Attacks Detection in Wireless Sensor Networks*, in "IJDSN - International Journal of Distributed Sensor Networks", 2013, vol. 2013, 12 p. p. [*DOI :* 10.1155/2013/745069], http://hal.inria.fr/hal-00918969

Articles in Non Peer-Reviewed Journals

[9] J. ACHARA, C. CASTELLUCCIA, J.-D. LEFRUIT, V. ROCA, F. BAUDOT, G. DELCROIX. *Mobilitics: Analyzing Privacy Leaks in Smartphones*, in "ERCIM Newsletter", April 2013, http://hal.inria.fr/hal-00917417

[10] M. CUNCHE, M. A. KAAFAR, R. BORELI. *Revealing Social Links Between Owners of Wi-Fi Enabled Smartphones*, in "ERCIM News", April 2013, n^{o} 93, pp. 33-34, http://hal.inria.fr/hal-00818202

International Conferences with Proceedings

[11] J. ACHARA, J.-D. LEFRUIT, V. ROCA, C. CASTELLUCCIA. *Detecting Privacy Leaks in the RATP App: how we proceeded and what we found*, in "GREHACK 2013", Grenoble, France, Guillaume Jeanne, November 2013, to appear also in Springer Journal of Computer Virology and Hacking Techniques (JCVHT), http://hal.inria.fr/hal-00872967

[12] J. Y. BAE, C. CASTELLUCCIA, C. LAURADOUX, F. ROUSSEAU. *Distributed Key Certification using Accumulators for Wireless Sensor Networks*, in "International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services - MOBIQUITOUS 2013", Tokyo, Japan, Springer, December 2013, http://hal.inria.fr/hal-00915741

[13] T. P. BERGER, M. MINIER, G. THOMAS. *Extended Generalized Feistel Networks using Matrix Representation*, in "Selected Areas in Cryptography 2013", Burnaby, British Columbia, Canada, L. R. KNUDSEN, H. WU (editors), Lecture Notes in Computer Science, Springer, 2013, vol. 7707, pp. 355-371, http://hal.inria.fr/hal-00913881

[14] D. BUTIN, M. CHICOTE, D. LE MÉTAYER. *Log Design for Accountability*, in "DUMA13 - 4th International Workshop on Data Usage Management - 2013", San Francisco, United States, May 2013 [*DOI :* 10.1109/SPW.2013.26], http://hal.inria.fr/hal-00799100

[15] D. BUTIN, D. GRAY, G. BELLA. *Towards Verifying Voter Privacy Through Unlinkability*, in "ESSoS13 - International Symposium on Engineering Secure Software and Systems - 2013", Rocquencourt, France, Lecture Notes in Computer Science, Springer, March 2013, pp. 91-106 [*DOI :* 10.1007/978-3-642-36563-8_7], http://hal.inria.fr/hal-00766201

[16] C. CASTELLUCCIA, S. GRUMBACH, L. OLEJNIK. *Data Harvesting 2.0: from the Visible to the Invisible Web*, in "The Twelfth Workshop on the Economics of Information Security", Washington, DC, United States, Allan Friedman, June 2013, http://hal.inria.fr/hal-00832784

[17] M. CAZORLA, K. MARQUET, M. MINIER. *Survey and Benchmark of Lightweight Block Ciphers for Wireless Sensor Networks*, in "SECRYPT 2013 - Proceedings of the International Conference on Security and Cryptography", Reykjavik, Iceland, SciTePress, 2013, pp. 543-548, http://hal.inria.fr/hal-00918974

[18] A. CHAABANE, Y. DING, R. DEY, M. ALI KAAFAR, K. ROSS. *A Closer Look at Third-Party OSN Applications: Are They Leaking Your Personal Information?*, in "Passive and Active Measurement conference", Springer, March 2014, http://hal.inria.fr/hal-00939175

[19] M. CUNCHE. *I know your MAC Address: Targeted tracking of individual using Wi-Fi*, in "International Symposium on Research in Grey-Hat Hacking - GreHack", Grenoble, France, November 2013, http://hal.inria.fr/hal-00858324

[20] M. CUNCHE, C. LAURADOUX, M. MINIER, R. BORELI. *Private and Resilient Data Aggregation*, in "IEEE Conference on Local Computer Networks - LCN", Sydney, Australia, IEEE, October 2013, http://hal.inria.fr/hal-00915770

[21] G. GÖSSLER, D. LE MÉTAYER. *A General Trace-Based Framework of Logical Causality*, in "FACS - 10th International Symposium on Formal Aspects of Component Software - 2013", Nanchang, China, 2013, http://hal.inria.fr/hal-00924048

[22] C. LAURADOUX, H. HOSSAYNI, C. HENNEBERT. *Entropy harvesting from physical sensors*, in "ACM Conference on Security and Privacy in Wireless and Mobile Networks, WISEC'13", Budapest, Hungary, ACM, April 2013 [*DOI :* 10.1145/2462096.2462122], http://hal.inria.fr/hal-00915722

[23] M. MINIER. *On the security ofPiccolo lightweight block cipher against related-key impossible differentials*, in "Progress in Cryptology - INDOCRYPT 2013", Mumbay, India, Springer, 2013, vol. 8250, pp. 308-318 [*DOI :* 10.1007/978-3-319-03515-4_21], http://hal.inria.fr/hal-00918965

[24] M. MINIER, G. THOMAS. *An Integral Distinguisher on Grøstl-512 v3*, in "14th International Conference on Cryptology in India", Bombay, India, G. PAUL, S. VAUDENAY (editors), Lecture Notes in Computer Science, Springer International Publishing, 2013, vol. 8250, pp. 50-59, Print ISBN : 978-3-319-03514-7 [*DOI :* 10.1007/978-3-319-03515-4_4], http://hal.inria.fr/hal-00913902

[25] L. OLEJNIK, C. CASTELLUCCIA. *Towards Web-based Biometric Systems Using Personal Browsing Interests*, in "The 8th International Conference on Availability, Reliability and Security (ARES 2014)", Regensburg, Germany, September 2013, pp. 274-280 [*DOI :* 10.1109/ARES.2013.36], http://hal.inria.fr/hal-00917046

[26] V. ROCA, M. CUNCHE, C. THIENOT, J. DETCHART, J. LACAN. *RS + LDPC-Staircase Codes for the Erasure Channel: Standards, Usage and Performance*, in "9th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2013)", Lyon, France, A. BENSLIMANE (editor), IEEE, August 2013, http://hal.inria.fr/hal-00850118

[27] D. WANG, H. PARK, G. XIE, S. MOON, M. A. KAAFAR, S. KAVÉ. *A genealogy of information spreading on microblogs: A Galton-Watson-based explicative model*, in "Proceedings IEEE INFOCOM, 2013", TOrino, Italy, April 2013, pp. 2391 - 2399 [*DOI :* 10.1109/INFCOM.2013.6567044], http://hal.inria.fr/hal-00945461

National Conferences with Proceedings

[28] M. CUNCHE, L. DEMIR, C. LAURADOUX. *Anonymization for Small Domains: the case of MAC address*, in "Atelier sur la Protection de la Vie Privée - APVP 2013", Les Loges en Josas, France, June 2013, http://hal.inria.fr/hal-00915789

Scientific Books (or Scientific Book chapters)

[29] D. BUTIN, M. CHICOTE, D. LE MÉTAYER. *Strong Accountability: Beyond Vague Promises*, in "Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges", S. GUTWIRTH, R. LEENES, P. DE HERT (editors), Springer, 2014, pp. 343-369 [*DOI :* 10.1007/978-94-007-7540-4_16], http://hal.inria.fr/hal-00917350

Research Reports

[30] D. BUTIN, D. LE MÉTAYER. , *Log Analysis for Data Protection Accountability (Extended Version)*, Inria, December 2013, n^{o} RR-8432, 18 p. , http://hal.inria.fr/hal-00921156

[31] M. CUNCHE, C. LAURADOUX, M. MINIER. , *Private and Resilient Data Aggregation*, Inria, July 2013, n^{o} RR-8330, http://hal.inria.fr/hal-00842914

[32] G. GÖSSLER, D. LE MÉTAYER. , *A General Trace-Based Framework of Logical Causality*, Inria, October 2013, n^{o} RR-8378, http://hal.inria.fr/hal-00873665

[33] D. LE MÉTAYER. , *Privacy by Design: a Formal Framework for the Analysis of Architectural Choices (extended version)*, Inria, February 2013, n° RR-8229, 24 p. , http://hal.inria.fr/hal-00788584

Scientific Popularization

[34] M. CUNCHE. *Quand les terminaux mobiles jouent les mouchards de poche*, in "Podcast Interstices", September 2013, http://hal.inria.fr/hal-00918398

[35] M. CUNCHE. *Smartphone, Wi-Fi et vie privée : comment votre smartphone peut se révéler être votre pire ennemi*, in "Multi-system & Internet Security Cookbook (MISC)", October 2013, n° 8, http://hal.inria.fr/hal-00874078

Other Publications

[36] J. ACHARA, C. CASTELLUCCIA, J.-D. LEFRUIT, V. ROCA. *Privacy and Smartphones*, in "CAPPRIS project reunion", Lyon, France, September 2013, http://hal.inria.fr/hal-00915771

[37] J. ACHARA, C. CASTELLUCCIA, J.-D. LEFRUIT, V. ROCA. *Smartphones: Privacy Standpoint*, in "Workshop on security and privacy for location-based services - EIT ICT Labs", Saarbrücken, Germany, December 2013, 30 p. , http://hal.inria.fr/hal-00915756

[38] L. DEMIR. , *Wi-Fi tracking : what about privacy*, M2 SCCI Security, Cryptologyand Coding of Information - UFR IMAGGrenoble, September 2013, 25 p. , http://hal.inria.fr/hal-00859013

[39] L. JACQUIN, V. ROCA, J.-L. ROCH. , *ICMP: an Attack Vector against IPsec Gateways*, 2013, http://hal.inria.fr/hal-00879997

[40] C. LAURADOUX, L. DEMIR. , *Guesswork*, October 2013, Multi-system & Internet Security Cookbook (MISC), http://hal.inria.fr/hal-00915782

[41] L. OLEJNIK, T. MINH-DUNG, C. CASTELLUCCIA. , *Selling Off Privacy at Auction*, December 2013, http://hal.inria.fr/hal-00915249

[42] V. ROCA, J. ACHARA, J.-D. LEFRUIT, C. CASTELLUCCIA. *The Mobilitics Inria-CNIL project: privacy and smartphones*, in "8ème Conférence sur la Sécurité des Architectures Réseaux et des Systèmes d'Information (SARSSI 2013)", Mont-de-Marsan, France, September 2013, http://hal.inria.fr/hal-00915884

[43] V. ROCA, J. ACHARA, J.-D. LEFRUIT, C. CASTELLUCCIA. *The Mobilitics Inria-CNIL project: privacy and smartphones*, in "Métroscope : l'observatoire scientifique d'Internet", Paris, France, July 2013, http://hal.inria.fr/hal-00915905

[44] V. ROCA, B. ADAMSON. , *FCAST: Object Delivery for the Asynchronous Layered Coding (ALC) and NACK-Oriented Reliable Multicast (NORM) Protocols*, July 2013, Internet Engineering Task Force (IETF) Request for Comments 6968 (RFC 6968), http://hal.inria.fr/hal-00844825

[45] V. ROCA, K. MATSUZONO. *Not so random RLC AL-FEC codes*, in "IETF88 - NWCRG meeting", Vancouver, Canada, November 2013, http://hal.inria.fr/hal-00879834