IN PARTNERSHIP WITH:
Institut national des sciences appliquées de Lyon

Activity Report 2016

Project-Team PRIVATICS

Privacy Models, Architectures and Tools for the Information Society

IN COLLABORATION WITH: Centre of Innovation in Telecommunications and Integration of services

RESEARCH CENTER
Grenoble - Rhône-Alpes

THEME
Security and Confidentiality

Table of contents

Project-Team PRIVATICS

Creation of the Team: 2013 January 01, updated into Project-Team: 2014 July 01

Keywords:

Computer Science and Digital Science:

1. - Architectures, systems and networks
1.1. - Architectures
1.2. - Networks
1.3. - Distributed Systems
1.4. - Ubiquitous Systems
3. - Data and knowledge
4. - Security and privacy
4.1. - Threat analysis
4.3. - Cryptography
4.8. - Privacy-enhancing technologies

Other Research Topics and Application Domains:

9. - Society and Knowledge
9.8. - Privacy
9.9. - Risk management
9.10. - Ethics

1. Members

Research Scientists

Claude Castelluccia [Team leader, Inria, Senior Researcher, HDR]
Cédric Lauradoux [Inria, Researcher]
Daniel Le Metayer [Inria, Senior Researcher, HDR]
Vincent Roca [Inria, Researcher, HDR]

Faculty Members

Mathieu Cunche [INSA Lyon, Associate Professor]
Marine Minier [Univ. Lorraine, Associate Professor, HDR]

Engineers

Sofiane Lagraa [Inria]
Belkacem Teibi [Inria]

PhD Students

Jagdish Achara [Inria, until Nov 2016]
Levent Demir [INCAS-ITSEC, granted by CIFRE]
Jessye Dos Santos [CEA]
Amrit Kumar [Univ. Grenoble I, until Nov 2016]
Celestin Matte [INSA Lyon]
Victor Morel [Inria, from Oct 2016]

Post-Doctoral Fellows

Mohammad Alaggan [Inria]
Sourya Joyee de [Inria]

Gabor Gulyas [Inria]
Ali Kassem [Inria]
Pablo Rauzy [Inria, until Aug 2016]

Visiting Scientist

Gergely Acs [Budapest University of Technology and Economics]

Administrative Assistant

Helen Pouchot-Rouge-Blanc [Inria]

Others

Margaux Canet Sola [Inria, Intern M1, from Feb 2016 until Aug 2016]
Julie Catania [Inria, Intern M1, from Feb 2016 until Jun 2016]
Jose Paul Dominguez [University of Savoie, Intern M2, until Sep 2016]
Zoltan Kovacs [Inria, Intern M2, from Jul 2016 until Aug 2016]
Luca Melis [University College London, PhD Student]
Aurelien Monnet Paquet [Inria, Intern M1, from Feb 2016 until Jun 2016]
Mary-Andrea Rakotomanga [Inria, Intern M1, until Jul 2016]
Alessandro Tedesco [Inria, Intern M2, from Feb 2016 until Jul 2016]

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 Twitter 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. However, 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.

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 in 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. Highlights of the Year

4.1. Highlights of the Year

In 2014, Jagdish Prasad Achara, Mathieu Cunche and Vincent Roca published with Aurelien Francillon from Eurecom a study on the Wi-Fi permissions used by mobile applications and their privacy implications. Two years after our research was published, the Federal Trade Commission (FTC) reached a $950,000 settlement with InMobi for tracking millions of consumers' locations, including children, without their knowledge. The FTC allege that InMobi abused the WiFi State information on the Android system to track the location of people without their consent, which is exactly what we showed in our research. Its policy prevents the FTC of releasing the sources of its investigations, therefore there is no way to affirm that our research triggered this investigation or was used during this investigation. We can only be sure that we identified a privacy issue that was serious enough to justify an investigation of the FTC and a penalty of $950,000. In addition to this, the company is under surveillance for their privacy behaviour for the next 20 years.

4.1.1. Awards

The software `MyTrackingChoices` designed by Claude Castellucia and Jagdish Prasad Achara from Privatics in collaboration with Javier Parra (former member of Privatics and now at Universitat Politecnica de Catalunya) was awarded 'Data protection by design' award by the Catalan Data Protection Authority.

5. New Software and Platforms

5.1. FECFRAME

FEC Framework following RFC 6363 specifications (https://datatracker.ietf.org/doc/rfc6363/)
KEYWORDS: Error Correction Code - Content delivery protocol - Robust transmission
FUNCTIONAL DESCRIPTION

This sofware implements the FECFRAME IETF standard (RFC 6363) co-authored by V. ROCA, and is compliant with 3GPP specifications for mobile terminals. It enables the simultaneous transmission of multimedia flows to one or several destinations, while being robust to packet erasures that happen on wireless networks (e.g., 4G or Wifi). This software relies on the OpenFEC library (the open-source http://openfec.org version or the commercial version) that provides the erasure correction codes (or FEC) and thereby offer robustness in front of packet erasures.

- Author: Vincent Roca
- Contact: Vincent Roca
- URL: http://openfec.org/

5.2. Mobilitics

FUNCTIONAL DESCRIPTION

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 mostly used mobile platforms, IOS (Iphone) and Android. Both versions of the Mobilitics software: (1) capture any access to private data, any modification (e.g., ciphering or hashing of private data), or transmission of data to remote locations on the Internet, (2) store these events in a local database on the phone for offline analysis, and (3) provide the ability to perform an in depth database analysis in order to identify personnal information leakage.

- Authors: Jagdish Achara, James-Douglass Lefruit, Claude Castelluccia, Vincent Roca, Gwendal Le Grand, Geoffrey Delcroix, Franck Baudot and Stéphane Petitcolas
- Contact: Claude Castelluccia
- URL: https://team.inria.fr/privatics/mobilitics/

5.3. MyTrackingChoices

KEYWORDS: Privacy - User control

FUNCTIONAL DESCRIPTION

This extension lets you control how you are being tracked on the Internet. It allows you to choose the categories (e.g., health, adult) of the websites where you don't want to be tracked on. When you browse the web, your visited webpages will be categorized on the fly and, depending on your choices, the extension will block the trackers (webpage by webpage) or not.

Existing anti-tracking (Ghostery, Disconnect etc.) and ad-blocking (AdBlock Plus etc.) tools block almost ALL trackers and as a result, ads. This has a negative impact on the Internet economy because free services/content on the Internet are fuelled by ads. As a result, websites are starting to block access to their content if they detect use of Ad-blockers or they ask users to move to a subscription-based model (where users have to pay to get access to the website).

This extension is testing another approach: It is trying to find a trade-off between privacy and economy, that would allow users to protect their privacy while still accessing to free content.

It is based on the assumption that most people are not against advertisements, but want to keep control over their data. We believe that some sites are more sensitive than others. In fact, most people don't want to be tracked on "sensitive" websites (for example related to religion, health,. . .), but don't see any problem to be tracked on less sensitive ones (such as news, sport,. . .). This extension allows you to take control and specify which on which categories of sites you don't want to be tracked on! Furthermore, the extension also gives you the option to block the trackers on specific websites.

- Contact: Claude Castelluccia
- URL: https://addons.mozilla.org/FR/firefox/addon/mytrackingchoices/

5.4. OMEN+

FUNCTIONAL DESCRIPTION

Omen+ is a password cracker following our previous work. It is used to guess possible passwords based on specific information about the target. It can also be used to check the strength of user password by effectively looking at the similarity of that password with both usual structures and information relative to the user, such as his name, birth date...

It is based on a Markov analysis of known passwords to build guesses. The previous work Omen needs to be cleaned in order to be scaled to real problems and to be distributed or transfered to the security community (maintainability): eventually it will become an open source software. The main challenge of Omen+ is to optimize the memory consumption.

- Participants: Pierre Rouveyrol and Claude Castelluccia
- Contact: Claude Castelluccia

5.5. OPENFEC

FUNCTIONAL DESCRIPTION

OpenFEC is an open-source C-language implementation of several Application-Level Forward Erasure Correction (AL-FEC) codecs, namely: 2D-parity, Reed-Solomon (RFC 5510) and LDPC-Staircase (RFC 5170) codes. The OpenFEC project also provides a complete performance evaluation tool-set, capable of automatically assessing the performance of various codecs, both in terms of erasure recovery and encoding/decoding speed or memory consumption.

- Participants: Mathieu Cunche, Jonathan Detchart, Julien Laboure, Christophe Neumann, Vincent Roca, Jérome Lacan and Kevin Chaumont
- Contact: Vincent Roca
- URL: http://openfec.org/

6. New Results

6.1. MobileAppScrutinator: A Simple yet Efficient Dynamic Analysis Approach for Detecting Privacy Leaks across Mobile OSs

Participants: Jagdish Achara, Vincent Roca, Claude Castelluccia.

Smartphones, the devices we carry everywhere with us, are being heavily tracked and have undoubtedly become a major threat to our privacy. As " Tracking the trackers " has become a necessity, various static and dynamic analysis tools have been developed in the past. However, today, we still lack suitable tools to detect, measure and compare the ongoing tracking across mobile OSs. To this end, we propose MobileAppScrutinator [24], based on a simple yet efficient dynamic analysis approach, that works on both Android and iOS (the two most popular OSs today). To demonstrate the current trend in tracking, we select 140 most representative Apps available on both Android and iOS AppStores and test them with MobileAppScrutinator. In fact, choosing the same set of apps on both Android and iOS also enables us to compare the ongoing tracking on these two OSs. Finally, we also discuss the effectiveness of privacy safeguards available on Android and iOS. We show that neither Android nor iOS privacy safeguards in their present state are completely satisfying.

6.2. MyTrackingChoices: Pacifying the Ad-Block War by Enforcing User Privacy Preferences

Participants: Jagdish Achara, Claude Castelluccia.

Free content and services on the Web are often supported by ads. However, with the proliferation of intrusive and privacy-invasive ads, a significant proportion of users have started to use ad blockers. As existing ad blockers are radical (they block all ads) and are not designed taking into account their economic impact, ad-based economic model of the Web is in danger today. In this paper, we target privacy-sensitive users and provide them with fine-grained control over tracking. Our working assumption is that some categories of web pages (for example, related to health, religion, etc.) are more privacy-sensitive to users than others (education, science, etc.). Therefore, our proposed approach consists in providing users with an option to specify the categories of web pages that are privacy-sensitive to them and block trackers present on such web pages only. As tracking is prevented by blocking network connections of third-party domains, we avoid not only tracking but also third-party ads. Since users will continue receiving ads on web pages belonging to non-sensitive categories, our approach essentially provides a trade-off between privacy and economy. To test the viability of our solution, we implemented it as a Google Chrome extension, named MyTrackingChoices (available on Chrome Web Store). Our real-world experiments with MyTrackingChoices [23] show that the economic impact of ad blocking exerted by privacy-sensitive users can be significantly reduced.

6.3. Security or privacy?

Participants: Amrit Kumar, Cédric Lauradoux.

Security softwares such as anti-viruses, IDS or filters help Internet users to protect their privacy from hackers. The cost of this protection is that the users privacy is stripped away by the companies providing these security solutions. Currently, Internet users can choose between no security with the risk of being hacked or use security software and lose all personal data to security companies. As a example of this dilemma, we analyze the solution proposed by Google and Yandex for Safe Browsing [8] and shows that their privacy policies do not match the reality: Google can perform tracking.

6.4. Near-Optimal Fingerprinting with Constraints

Participants: Gabor Gulyas, Gergely Acs, Claude Castelluccia.

Several recent studies have demonstrated that people show large behavioural uniqueness. This has serious privacy implications as most individuals become increasingly re-identifiable in large datasets or can be tracked while they are browsing the web using only a couple of their attributes, called as their fingerprints. Often, the success of these attacks depend on explicit constraints on the number of attributes learnable about individuals, i.e., the size of their fingerprints. These constraints can be budget as well as technical constraints imposed by the data holder. For instance, Apple restricts the number of applications that can be called by another application on iOS in order to mitigate the potential privacy threats of leaking the list of installed applications on a device. In [15], we address the problem of identifying the attributes (e.g., smartphone applications) that can serve as a fingerprint of users given constraints on the size of the fingerprint. We give the best fingerprinting algorithms in general, and evaluate their effectiveness on several real-world datasets. Our results show that current privacy guards limiting the number of attributes that can be queried about individuals is insufficient to mitigate their potential privacy risks in many practical cases.

6.5. Data anonymization Evaluation

Participants: Claude Castelluccia, Gergely Acs, Daniel Le Metayer.

Anonymization is a critical issue because data protection regulations such as the European Directive 95/46/EC and the European General Data Protection Regulation (GDPR) explicitly exclude from their scope anonymous information" and personal data rendered anonymous"1. However, turning this general statement into effective criteria is not an easy task. In order to facilitate the implementation of this provision, the Working Party 29 (WP29) has published in April 2014 an Opinion on Anonymization Techniques. This Opinion puts forward three criteria corresponding to three risks called respectively "singling out", "linkability" and "inference". In this work, we first evaluated these criteria and showed that they are neither necessary nor effective to decide upon the robustness of an anonymization algorithm. Then we proposed an alternative approach relying on the notions of acceptable versus unacceptable inferences in [4] and we introduced differential testing, a practical way to implement this approach using machine learning techniques.

6.6. Wi-Fi and privacy

Participants: Mathieu Cunche, Celestin Matte.

- **Geolocation spoofing attack** We present several novel techniques to track (unassociated) mobile devices by abusing features of the Wi-Fi standard. This shows that using random MAC addresses, on its own, does not guarantee privacy. First, we show that information elements in probe requests can be used to fingerprint devices. We then combine these fingerprints with incremental sequence numbers, to create a tracking algorithm that does not rely on unique identifiers such as MAC addresses. Based on real-world datasets, we demonstrate that our algorithm can correctly track as much as 50% of devices for at least 20 minutes. We also show that commodity Wi-Fi devices use predictable scrambler seeds. These can be used to improve the performance of our tracking algorithm. Finally, we present two attacks that reveal the real MAC address of a device, even if MAC address randomization is used. In the first one, we create fake hotspots to induce clients to connect using their real MAC address. The second technique relies on the new 802.11u standard, commonly referred to as Hotspot 2.0, where we show that Linux and Windows send Access Network Query Protocol (ANQP) requests using their real MAC address.

- **Extraction of semantical information from Wi-Fi network identifiers** MAC address randomization in Wi-Fi-enabled devices has recently been adopted to prevent passive tracking of mobile devices. However, Wi-Fi frames still contain fields that can be used to fingerprint devices and potentially allow tracking. Panoptiphone is a tool inspired by the web browser fingerprinting tool Panopticlick, which aims to show the identifying information that can be found in the frames broadcast by a Wi-Fi-enabled device. Information is passively collected from devices that have their Wi-Fi interface enabled, even if they are not connected to an access point. Panoptiphone uses this information to create a fingerprint of the device and empirically evaluate its uniqueness among a database of fingerprints. The user is then shown how much identifying information its device is leaking through Wi-Fi and how unique it is.

6.7. Formal and legal issues of privacy

Participant: Daniel Le Metayer.

- **Privacy by design** Based on our previous work on the use of formal methods to reason about privacy properties of system architectures, we have proposed a logic to reason about properties of architectures including group authentication functionalities. By group authentication, we mean that a user can authenticate on behalf of a group of users, thereby keeping a form of anonymity within this set. Then we show that this extended framework can be used to reason about privacy properties of a biometric system in which users are authenticated through the use of group signatures.
- **Privacy Risk Analysis** Privacy Impact Assessments (PIA) are recognized as a key step to enhance privacy protection in new IT products and services. They will be required for certain types of products in Europe when the future General Data Protection Regulation becomes effective. From a technical perspective, the core of a PIA is a privacy risk analysis (PRA), which has so far received relatively less attention than organizational and legal aspects of PIAs. We have proposed a rigorous and systematic methodology for conducting a PRA and illustrated it with a quantified-self use-case.

  The smart grid initiative promises better home energy management. However, there is a growing concern that utility providers collect, through smart meters, highly granular energy consumption data that can reveal a lot about the consumer's personal life. This exposes consumers to a large number of privacy harms, of various degrees of severity and likelihood: surveillance by the government and law-enforcement bodies, various forms of discrimination etc. A privacy impact assessment is vital for early identification of potential privacy breaches caused by an IT product or service and for choosing the most appropriate protection measures. So, a data protection impact assessment (DPIA) template for smart grids has been developed by the Expert Group 2 (EG2) of the European Commission's Smart Grid Task Force (SGTF). To carry out a true privacy risk analysis and go beyond a traditional security analysis, it is essential to distinguish the notions of feared events and their impacts, called "privacy harms" here, and to establish a link between them. The Working Party 29 highlights the importance of this link in its feedback on EG2's DPIA. We have provided in [11] a clear relationship among harms, feared events, privacy weaknesses and risk sources and described their use in the analysis of smart grid systems.

  Although both privacy by design and privacy risk analysis have received the attention of researchers and privacy practitioners during the last decade, to the best of our knowledge, no method has been documented yet to establish a clear connection between these two closely related notions. We have proposed a methodology to help designers select suitable architectures based on an incremental privacy risk analysis. The analysis proceeds in three broad phases: 1) a generic privacy risk analysis phase depending only on the specifications of the system and yielding generic harm trees; 2) an architecture-based privacy risk analysis that takes into account the definitions of the possible architectures of the system and yields architecture-specific harm trees by refining the generic harm trees and 3) a context-based privacy risk analysis that takes into account the context of deployment of the system (e.g., a casino, an office cafeteria, a school) and further refines the architecture-specific harm trees to yield context-specific harm trees which can be used to take decisions about the most suitable architectures. To illustrate our approach, we have considered the design of a biometric access control system. Such systems are now used commonly in many contexts such as border security controls, work premises, casinos, airports, chemical plants, hospitals, schools, etc. However, the collection, storage and processing of biometric data raise complex privacy issues. To deal with these privacy problems in biometric access control, a wide array of dedicated techniques (such as secure sketches or fuzzy vaults) as well as adaptations of general privacy preserving techniques (such as encryption, homomorphic encryption, secure multi-party computation) have been proposed. However, each technique solves specific privacy problems and is suitable in specific contexts. Therefore, it is useful to provide guidance to system designers and help them select a solution and justify it with respect to privacy risks. We have used as an illustration of context a deployment in casinos. The verification of the identities of casino customers is required by certain laws (to prevent access by minors or individuals on blacklists) which can justify the implementation of a biometric access control system to speed up the verification process.

6.8. Building blocks

Participants: Marine Minier, Vincent Roca.

- **Symmetric cryptography**

  In [7], we introduce Constraint Programming (CP) models to solve a cryptanalytic problem: the chosen key differential attack against the standard block cipher AES. The problem is solved in two steps: In Step 1, bytes are abstracted by binary values; In Step 2, byte values are searched. We introduce two CP models for Step 1: Model 1 is derived from AES rules in a straightforward way; Model 2 contains new constraints that remove invalid solutions filtered out in Step 2. We also introduce a CP model for Step 2. We evaluate scale-up properties of two classical CP solvers (Gecode and Choco) and a hybrid SAT/CP solver (Chuffed). We show that Model 2 is much more efficient than Model 1, and that Chuffed is faster than Choco which is faster than Gecode on the hardest instances of this problem. Furthermore, we prove that a solution claimed to be optimal in two recent cryptanalysis papers is not optimal by providing a better solution.

  Using dedicated hardware is common practice in order to accelerate cryptographic operations: complex operations are managed by a dedicated co-processor and RAM/crypto-engine data transfers are fully managed by DMA operations. The CPU is therefore free for other tasks, which is vital in embedded environments with limited CPU power. In this work we discuss and benchmark XTS-AES, using either software or mixed approaches, using Linux and dm-crypt, and a low-power At-mel(tm) board. This board featurs an AES crypto-engine that supports ECB-AES but not the XTS-AES mode. We show that the `dm-crypt` module used in Linux for full disk encryption has limitations that can be relaxed when considering larger block sizes. In particular we demonstrate in [14] that performance gains almost by a factor two are possible, which opens new opportunities for future use-cases.

6.9. Other results

Participants: Mathieu Cunche, Vincent Roca.

- **Error-correcting codes**

  Recent work have shown that Reed-Muller (RM) codes achieve the erasure channel capacity. However, this performance is obtained with maximum-likelihood decoding which can be costly for practical applications. In [12], we propose an encoding/decoding scheme for Reed-Muller codes on the packet erasure channel based on Plotkin construction. We present several improvements over the generic decoding. They allow, for a light cost, to compete with maximum-likelihood decoding performance, especially on high-rate codes, while significantly outperforming it in terms of speed.

In [3], we provide fundamentals in the design and analysis of Generalized Low Density Parity Check (GLDPC)-Staircase codes over the erasure channel. These codes are constructed by extending an LDPC-Staircase code (base code) using Reed Solomon (RS) codes (outer codes) in order to benefit from more powerful decoders. The GLDPC-Staircase coding scheme adds, in addition to the LDPC-Staircase repair symbols, extra-repair symbols that can be produced on demand and in large quantities, which provides small rate capabilities. Therefore, these codes are extremely flexible as they can be tuned to behave either like predefined rate LDPC-Staircase codes at one extreme, or like a single RS code at another extreme, or like small rate codes. Concerning the code design, we show that RS codes with " quasi " Hankel matrix-based construction fulfill the desired structure properties, and that a hybrid (IT/RS/ML) decoding is feasible that achieves Maximum Likelihood (ML) correction capabilities at a lower complexity. Concerning performance analysis, we detail an asymptotic analysis method based on Density evolution (DE), EXtrinsic Information Transfer (EXIT) and the area theorem. Based on several asymptotic and finite length results, after selecting the optimal internal parameters, we demonstrate that GLDPC-Staircase codes feature excellent erasure recovery capabilities, close to that of ideal codes, both with large and very small objects. From this point of view they outperform LDPC-Staircase and Raptor codes, and achieve correction capabilities close to those of RaptorQ codes. Therefore all these results make GLDPC-Staircase codes a universal Application-Layer FEC (AL-FEC) solution for many situations that require erasure protection such as media streaming or file multicast transmission.

7. Bilateral Contracts and Grants with Industry

7.1. Bilateral Contracts with Industry

7.1.1. IPSec with pre-shared key for MISTIC security

Title: IPSec with pre-shared key for MISTIC security.

Type: CIFRE.

Duration: Juillet 2014 - Juillet 2017.

Coordinator: Inria

Others partners: Privatics, Moais and Incas-ITSec.

8. Partnerships and Cooperations

8.1. National Initiatives

8.1.1. FUI

8.1.1.1. HuMa

Title: HuMa.

Type: FUI.

Duration: Juin 2015 - Mai 2018.

Coordinator: INTRINSEC.

Others partners: Inria, SYDO, Wallix, INSA Lyon, CASSIDIAN Cybersecurity, Oberthur, INTRINSEC.

Abstract:

The goal of huMa is to improve the tools used to distinguish legitimate network flows from attacks in complex systems including IoT.

8.1.2. ANR

8.1.2.1. 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.

8.1.3. Inria Project Labs

8.1.3.1. CAPPRIS

Title: CAPPRIS

Type: Inria Project Lab

Duration: January 2011 - 2016.

Coordinator: PRIVATICS

Others partners: Inria (CIDRE, Comete, Secsi,Smis), Eurecom, LAAS and CRIDS

Abstract: Cappris (Collaborative Action on the Protection of Privacy Rights in the Information Society) is an Inria Project Lab initiated in 2013. The general goal of Cappris is to foster the collaboration between research groups involved in privacy in France and the interaction between the computer science, law and social sciences communities in this area.

8.1.4. Inria CNIL project

8.1.4.1. 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.

8.2. European Initiatives

8.2.1. Collaborations in European Programs, ANR Chistera

8.2.1.1. COPES

Title: COnsumer-centric Privacy in smart Energy gridS

Programm: CHISTERA

Duration: December 2015 - december 2018

Coordinator: KTH Royal Institute of Technology

Inria contact: Cédric Lauradoux

Smart meters have the capability to measure and record consumption data at a high time resolution and communicate such data to the energy provider. This provides the opportunity to better monitor and control the power grid and to enable demand response at the residential level. This not only improves the reliability of grid operations but also constitutes a key enabler to integrate variable renewable generation, such as wind or solar. However, the communication of high resolution consumption data also poses privacy risks as such data allows the utility, or a third party, to derive detailed information about consumer behavior. Hence, the main research objective of COPES is to develop new technologies to protect consumer privacy, while not sacrificing the ”smartness”, i.e., advanced control and monitoring functionalities. The core idea is to overlay the original consumption pattern with additional physical consumption or generation, thereby hiding the consumer privacy sensitive consumption. The means to achieve this include the usage of storage, small scale distributed generation and/or elastic energy consumptions. Hence, COPES proposes and develops a radically new approach to alter the physical energy flow, instead of purely relying on encryption of meter readings, which provides protection against third party intruders but does not prevent the use of this data by the energy provider.

8.2.1.2. UPRISE-IoT

Title: User-centric PRIvacy & Security in IoT

Programm: CHISTERA

Duration: December 2016 - december 2019

Coordinator: SUPSI (Suisse)

Inria contact: Claude Castelluccia

The call states that “Traditional protection techniques are insufficient to guarantee users’ security and privacy within the future unlimited interconnection”: UPRISE-IoT will firstly identify the threats and model the behaviours in IoT world, and further will build new privacy mechanisms centred around the user. Further, as identified by the call “all aspects of security and privacy of the user data must be under the control of their original owner by means of as simple and efficient technical solutions as possible”, UPRISE-IoT will rise the awareness of data privacy to the users. Finally, it will deeply develop transparency mechanisms to “guarantee both technically and regulatory the neutrality of the future internet.” as requested by the call. The U-HIDE solution developed inn UPRISE-IoT will “empower them to understand and make their own decisions regarding their data, which is essential in gaining informed consent and in ensuring the take-up of IoT technologies”, using a methodology that includes “co-design with users to address the key, fundamental, but inter-related and interdisciplinary aspects of privacy, security and trust.”

8.3. Regional Initiatives

8.3.1. ACDC

Title: ACDC

Type: AGIR 2016 Pole MSTIC.

Duration: September 2016 - 2017.

Coordinator: Inria.

Others partners: UGA.

Abstract: The objective of this project is to evaluate the security and privacy impacts of drone. The project targets 2 milestones: the evaluation of the possiblity to tamper with the drone control/command systems and the capacity of drone to collect private information (for instance text recognition).

8.3.2. AMNECYS

- Title: AMNECYS
- Duration: 2015 - .
- Coordinator: CESICE, UPMF.
- Others partners: Inria/Privatics and LIG/Moais, Gipsa-lab, LJK, Institut Fourier, TIMA, Vérimag, LISTIC (Pole MSTIC) .
- Abstract: Privatics participates to the creation of an Alpine Multidisciplinary NEtwork on CYbersecurity Studies (AMNECYS). The academic teams and laboratories participating in this project have already developed great expertise on encryption technologies, vulnerabilities analysis, software engineering, protection of privacy and personal data, international & European aspects of cybersecurity. The first project proposal (ALPEPIC ALPs-Embedded security: Protecting Iot & Critical infrastructure) focuses on the protection of the Internet of Things (IoT) and Critical Infrastructure (CI).

8.4. International Research Visitors

8.4.1. Visits of International Scientists

Lucas Melis

Gergely Acs

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

Daniel Le Metayer: CPDP 2016 (panel chairman), Privacy protection, new technical and legal instruments (Colloque Inria CAPPRIS).

Cédric Lauradoux: Nombre et cryptographie, maison pour la science Alpes Dauphiné

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

Cédric Lauradoux: RESSI 2016 and ATC 2016.

Daniel Le Metayer: Infer 2016, STM 2016, Annual Privacy Forum 2016, IWPE 2016, CPDP 2016 and WETICE-FISA.

Marine Minier: MyCrypt 2016 and RESSI 2016.

Vincent Roca: GreHack 2016, SPACOMM 2016 and VTC2016-Spring.

Mathieu Cunche: APVP 2016, HotPlanet 2016, ICISSP 2017 and IEEE TrustCom 2016.

Claude Casteluccia: Wisec 2016, DTL 2016, AFP 2016, UEOP'16 and DAT'2016.

9.1.3. Invited Talks

Daniel Le Metayer: IFIP SEC 2016 and France Stratégie, Algorithms: transparency and responsibility panel.

Claude Casteluccia: LIG Keynote.

9.1.4. Leadership within the Scientific Community

Vincent Roca: co-chair of the research group NWCRG (Network Coding Research Group) of IRTF (Internet Research Task Force)

Daniel Le Metayer: member of the scientific committee of the CNIL-Inria Privacy Award

9.2. Teaching - Supervision - Juries

9.2.1. Teaching

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

Undergraduate course : Vincent Roca, *On Network Communications*, 44h, L1, IUT-2 (UPMF University) Grenoble, France.

Undergraduate course : Marine Minier, *Probabilities*, 80h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, *Signal Processing*, 20h, L3, INSA-Lyon, France.

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

Undergraduate course : Marine Minier, *Introduction to Cryptography*, 10h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, *Information Theory*, 10h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, *Computer Architecture*, 20h, L3, INSA-Lyon, France.

Undergraduate course : Marine Minier, *Computer Security*, 20h, L3,IUT-Lyon, France.

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

Master : Mathieu Cunche, *Wireless Security*, 6h, M2, INSA-Lyon, France.

Undergraduate course : Mathieu Cunche, *On Wireless Network Security*, 10h, L1, IUT-2 (UPMF - Grenoble University) , France.

Undergraduate course : Mathieu Cunche, *Advanced Topics in Security*, 20h, L3, ENSIMAG, France.

Undergraduate course : Mathieu Cunche, *Security & Privacy*, 21h, L3, INSA-Lyon, France.

Undergraduate course : Daniel Le Métayer, *Security & Privacy*, 17h, L3, INSA-Lyon, France.

Undergraduate course : Daniel Le Métayer, *Privacy*, 12h, L3, INSA-Lyon, France.

Master : Cédric Lauradoux, *Introduction to Cryptology*, 30h, M1, University of Grenoble Alpes, France.

Master : Cédric Lauradoux, *Internet Security*, M2, University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Advanced Topics in Security*, 20h, M2, Ensimag/University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Advanced Topics in Security*, 15h, M2, Ensimag/INPG, France.

Master : Claude Castelluccia, *Security & Privacy*, 18h, Master MOSIG, University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Privacy*, 4h, M2, College de droit University of Grenoble Alpes, France.

Master : Marine Minier, *Security for wireless networks*, 20h, M2, INSA-Lyon, France.

Master : Mathieu Cunche, *Wireless Security*, 6h, M2, INSA-Lyon, France.

Master : Daniel Le Métayer, *Privacy*, 6h, M2 MASH, Université Paris Dauphine, France.

9.2.2. Supervision

PhD defended : Jagdish Achara, *Unveiling and Controlling Online Tracking*, Claude Castelluccia and Vincent Roca.

PhD defended : Amrit Kumar, *Security and Privacy of Hash-Based Software Applications* , Cedric Lauradoux.

PhD in progress : Victor Morel, *IoT privacy* , September 2016, Daniel Le Métayer.

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

PhD in progress : Célestin Matte, *Système d'observation des flux humains via Wi-Fi respectueux de la vie privée*, October 2014, Marine Minier et Mathieu Cunche.

Intern (M2): Alessandro Tedesco, *The rise of Internet of things made possible the large-scale collection of personal data and metadata*, Claude Castelluccia

Intern (M2): Jose-Paul Domingez, *The geopolitics of Internet protocols*, Claude Castelluccia

Intern (M2): Zoltan Kovac, *MyRealOnlineChoices*, Claude Castelluccia

Intern (M1): Margaux Canet Sola, *decompression bombs*, Cédric Lauradoux

Intern (M1): Julie Catania, Fuzzing the `zlib`, Cédric Lauradoux

Intern (M1): Aurelien Monnet Paquet, *Anti-virus DOS attacks*, Amrit Kumar

Intern (M1): Mary-Andrea Rakotomanga, *Compression quines*, Cédric Lauradoux

9.2.3. Juries

PhD: Yagdish Achara, *Unveiling and Controlling Online Tracking*, 18/10/2016, Claude Castelluccia and Vincent Roca.

PhD: Amrit Kumar, *Security and Privacy of Hash-Based Software Applications*, Université de Grenoble, Nantes, 18/10/2016, Cédric Lauradoux.

PhD : Tarek Sayah, *Exposition seélective et probleème de fuite d'inférence dans le Linked Data*, Université Claude Bernard Lyon 1, 8/9/2016, Vincent Roca.

PhD : Karina Sokolova Perez, *Bridging the Gap between Privacy by Design and Mobile Systems by Patterns*, UTT Troyes, 27/04/2016, Daniel Le Métayer.

PhD: Tania Richmond, *Implantation sécurisée de protocoles cryptographiques basés sur les codes correcteurs d'erreurs*, Université de Saint-Etienne, 24/10/2016, Marine Minier.

PhD: Nora El Amrani, *Codes MDS additifs pour la cryptographie*, Université de Limoges, 24/02/2016, Marine Minier.

9.3. Popularization

9.3.1. Interview

Privatics team has participated to an episode of X:enius entitled: "Données personnelles : à quel point sommes-nous prévisibles ?". It features an interview of Claude Castelluccia, Daniel Le Métayer and Mathieu Cunche. The episode was broadcasted the 12th december 2016 on Arte.

9.3.2. Articles

D. Le Métayer in *France Stratégie, Algorithmes, libertés et responsabilités*, 10/03/2016.

C. Castelluccia in Le Monde, *Que reproche-t-on au TES, le « mégafichier » des 60 millions de Français*, 08/11/2016.

M. Cunche and C. Matte in GNU/Linux Magazine HS 84, *Traçage Wi-Fi : applications et contre-mesures*, 05/2016.

M. Cunche in Arte Futuremag, *Données personnelles, nos smartphones nous espionnent-ils?*, 05/2016.

9.3.3. Conferences

C. Castelluccia, *An Introduction to DataVeillance (Data + Surveillance)*, LIG UGA Keynote, 07/04/2016

V. Roca, *Vie privé et smartphones font ils bon ménage?*, Cours Universite´ Ouverte, Lyon 1, cycle Impact de l'informatique sur la socie´te´ et sur nos vies, 11/2016.

C. Lauradoux, *Email et vie privée: pourquoi utiliser GPG ?*, Cours Master 2, 01/12/2016

C. Lauradoux, *Cryptographie et grands nombres*, Olympiades académiques de Mathématiques, 04/07/2016

C. Lauradoux, *Cryptographie visuelle*, Collège/Lycée Jean Prévost, 01/06/2016

C. Lauradoux, *Cryptanalyse*, stage MathC2+, 06/2016

C. Lauradoux, *Protéger la confidentialité de ces messages*, Collège Paul Fort Is sur Tille, 04/10/2016

C. Lauradoux, *Internet et vie privée*, Collège Poncet Cluses, 15/12/2016

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] J. P. ACHARA. *Unveiling and Controlling Online Tracking*, Université Grenoble-Alpes, October 2016, https://hal.inria.fr/tel-01386405

[2] A. KUMAR. *Security and Privacy of Hash-Based Software Applications*, Université Grenoble Alpes, October 2016, https://hal.inria.fr/tel-01385488

Articles in International Peer-Reviewed Journals

[3] F. MATTOUSSI, V. ROCA, B. SAYADI. *GLDPC-Staircase AL-FEC codes: A Fundamental study and New results*, in "EURASIP Journal on Wireless Communications and Networking", July 2016, https://hal.inria.fr/hal-01346126

International Conferences with Proceedings

[4] G. ACS, C. CASTELLUCCIA, D. LE MÉTAYER. *Testing the robustness of anonymization techniques: acceptable versus unacceptable inferences*, in "The Brussels Privacy Symposium", brussels, Belgium, November 2016, https://hal.inria.fr/hal-01399858

[5] J. BRINGER, H. CHABANNE, D. LE MÉTAYER, L. ROCH. *Reasoning about privacy properties of architectures supporting group authentication and application to biometric systems*, in "30th Annual IFIP WG 11.3 Conference on Data and Applications Information Security and Privacy (DBSec 2016)", Trento, Italy, S. RANISE, V. SWARUP (editors), Data and Applications Security and Privacy XXX, Springer, July 2016, vol. 9766, pp. 313-327 [*DOI :* 10.1007/978-3-319-41483-6_22], https://hal.inria.fr/hal-01403885

[6] J. DOS SANTOS, C. HENNEBERT, C. LAURADOUX, J. FONBONNE. *Ephemeral: Lightweight Pseudonyms for 6LowPAN Mac Addresses*, in "27th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications - PIMRC 2016", Valence, Spain, IEEE, September 2016, https://hal.inria.fr/hal-01399831

[7] D. GERAULT, M. MINIER, C. SOLNON. *Constraint Programming Models for Chosen Key Differential Cryptanalysis*, in "22nd International Conference on Principles and Practice of Constraint Programming (CP 2016)", Toulouse, France, 22nd International Conference on Principles and Practice of Constraint Programming (CP), Springer, September 2016, https://hal.archives-ouvertes.fr/hal-01331222

[8] T. Gerbet, A. Kumar, C. Lauradoux. *A Privacy Analysis of Google and Yandex Safe Browsing*, in "46th IEEE/IFIP International Conference on Dependable Systems and Networks - DSN 2016", Toulouse, France, IEEE, June 2016 [*DOI :* 10.1109/DSN.2016.39], https://hal.inria.fr/hal-01399829

[9] G. G. Gulyás, B. Simon, S. Imre. *An Efficient and Robust Social Network De-anonymization Attack*, in "Workshop on Privacy in the Electronic Society", Vienna, Austria, October 2016 [*DOI :* 10.1145/2994620.2994632], https://hal.inria.fr/hal-01380768

[10] D. Le Métayer, S. J. De. *PRIAM: a Privacy Risk Analysis Methodology*, in "Data Privacy Management and Security Assurance", Heraklion, Greece, G. Livraga, V. Torra, A. Aldini, F. Martinelli, N. Suri (editors), Springer, September 2016, https://hal.inria.fr/hal-01420983

[11] D. Le Métayer, S. J. De. *Privacy Harm Analysis: a Case Study on Smart Grids*, in "International Workshop on Privacy Engineering (IWPE 2016)", San Jose, United States, May 2016, https://hal.inria.fr/hal-01403889

[12] A. Soro, J. Lacan, V. Roca, V. Savin, M. Cunche. *Enhanced Recursive Reed-Muller Erasure Decoding*, in "IEEE International Symposium on Information Theory (ISIT)", Barcelona, Spain, IEEE (editor), IEEE International Symposium on Information Theory (ISIT), July 2016, https://hal.inria.fr/hal-01320563

Conferences without Proceedings

[13] M. Alaggan, M. Cunche, M. Minier. *Privacy-Preserving t-Incidence for WiFi-based Mobility Analytics*, in "7e Atelier sur la Protection de la Vie Privée (APVP'16)", Toulouse, France, July 2016, https://hal.inria.fr/hal-01376798

[14] L. Demir, M. Thiery, V. Roca, J.-L. Roch, J.-M. Tenkes. *Improving dm-crypt performance for XTS-AES mode through extended requests: first results*, in "GreHack 2016. The 4th International Symposium on Research in Grey-Hat Hacking - aka GreHack", Grenoble, France, November 2016, https://hal.inria.fr/hal-01399967

[15] G. G. Gulyás, G. Acs, C. Castelluccia. *Near-Optimal Fingerprinting with Constraints*, in "PET Symposium '16", Darmstadt, Germany, July 2016 [*DOI :* 10.1515/popets-2016-0051], https://hal.inria.fr/hal-01321659

[16] C. Matte, M. Cunche. *DEMO: Panoptiphone: How Unique is Your Wi-Fi Device?*, in "ACM WiSec 2016", Darmstadt, Germany, July 2016 [*DOI :* 10.1145/2939918.2942417], https://hal.inria.fr/hal-01330479

[17] M. Vanhoef, C. Matte, M. Cunche, L. Cardoso, F. Piessens. *Why MAC Address Randomization is not Enough: An Analysis of Wi-Fi Network Discovery Mechanisms*, in "ACM AsiaCCS", Xi'an, China, May 2016 [*DOI :* 10.1145/2897845.2897883], https://hal.inria.fr/hal-01282900

Scientific Books (or Scientific Book chapters)

[18] D. Le Métayer, S. J. De. , E. Bertino, R. Sandhu (editors) *Privacy Risk Analysis*, Synthesis Lectures on Information Security, Privacy, and Trust, Morgan & Claypool Publishers, September 2016, vol. 8, n^{o} 3, 133 p. [*DOI :* 10.2200/S00724ED1V01Y201607SPT017], https://hal.inria.fr/hal-01420968

[19] D. Le Métayer. *Whom to trust? Using technology to enforce privacy*, in "Enforcing Privacy", D. Wright, P. D. Hert (editors), Springer , February 2016, https://hal.inria.fr/hal-01247114

Research Reports

[20] S. J. DE, D. LE MÉTAYER. *A Risk-based Approach to Privacy by Design (Extended Version)*, Inria - Research Centre Grenoble – Rhône-Alpes, December 2016, n° 9001, 54 p. , https://hal.inria.fr/hal-01420954

[21] S. J. DE, D. LE MÉTAYER. *PRIAM: A Privacy Risk Analysis Methodology*, Inria - Research Centre Grenoble – Rhône-Alpes, April 2016, n° RR-8876, https://hal.inria.fr/hal-01302541

Scientific Popularization

[22] C. MATTE, M. CUNCHE. *Traçage Wi-Fi : applications et contre-mesures*, in "GNU Linux Magasine France", May 2016, vol. HS 84, https://hal.inria.fr/hal-01419943

Other Publications

[23] J. P. ACHARA, J. PARRA-ARNAU, C. CASTELLUCCIA. *MyTrackingChoices: Pacifying the Ad-Block War by Enforcing User Privacy Preferences*, April 2016, Accepted at The Workshop on the Economics of Information Security (WEIS), 2016, https://hal.inria.fr/hal-01302613

[24] J. P. ACHARA, V. ROCA, C. CASTELLUCCIA, A. FRANCILLON. *MobileAppScrutinator: A Simple yet Efficient Dynamic Analysis Approach for Detecting Privacy Leaks across Mobile OSs*, May 2016, working paper or preprint, https://hal.inria.fr/hal-01322286

[25] J. PARRA-ARNAU, J. P. ACHARA, C. CASTELLUCCIA. *MyAdChoices: Bringing Transparency and Control to Online Advertising*, February 2016, working paper or preprint, https://hal.inria.fr/hal-01270186

[26] V. ROCA, A. BEGEN. *Forward Error Correction (FEC) Framework version 2*, October 2016, Working document of the TSVWG (Transport Area Working Group) group of IETF (Internet Engineering Task Force), https://hal.inria.fr/hal-01345125

[27] V. ROCA, S. FALL. *Too Big or Too Small? The PTB-PTS ICMP-based Attack against IPsec Gateways*, January 2016, 16 p. , Work in Progress document of the IPSECME (IP Security Maintenance and Extensions) of the IETF (Internet Engineering Task Force), https://hal.inria.fr/hal-01178390

[28] V. ROCA. *FECFRAMEv2: Adding Sliding Encoding Window Capabilities to the FEC Framework: Problem Position*, May 2016, 18 p. , Working document of the NWCRG (Network Coding Research Group) group of IRTF (Internet Research Task Force), https://hal.inria.fr/hal-01141470

[29] V. ROCA, B. TEIBI, C. BURDINAT, T. TRAN, C. THIENOT. *Block or Convolutional AL-FEC Codes? A Performance Comparison for Robust Low-Latency Communications*, November 2016, working paper or preprint, https://hal.inria.fr/hal-01395937