IN PARTNERSHIP WITH:
Institut national des sciences appliquées de Lyon

Activity Report 2017

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:

A1. - Architectures, systems and networks
A1.1. - Architectures
A1.2. - Networks
A1.3. - Distributed Systems
A1.4. - Ubiquitous Systems
A3. - Data and knowledge
A4. - Security and privacy
A4.1. - Threat analysis
A4.3. - Cryptography
A4.8. - Privacy-enhancing technologies

Other Research Topics and Application Domains:

B9. - Society and Knowledge
B9.8. - Privacy
B9.9. - Risk management
B9.10. - Ethics

1. Personnel

Research Scientists

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

Faculty Members

Mathieu Cunche [INSA Lyon, Associate Professor]
Antoine Boutet [INSA Lyon, from Sep 2017, Associate Professor]

Post-Doctoral Fellows

Mohammad Alaggan [Inria, until Sep 2017]
Sourya Joyee de [Inria, until Feb 2017]
Gabor Gulyas [Inria, until May 2017]
Ali Kassem [Inria, until May 2017]

PhD Students

Levent Demir [INCAS IT-SEC company, until Sep 2017]
Jessye Dos Santos [CEA, until Au 2017]
Célestin Matte [INSA Lyon]
Victor Morel [Inria]
Mathieu Thiery [Inria, from Apr 2017]
Guillaume Celosia [INSA Lyon, from Nov 2017]

Technical staff

Gabor Gulyas [Inria, from Jun 2017]
Belkacem Teibi [Inria]

Interns

Sumish Ajmani [Inria, from May 2017 until Jul 2017]
Coline Boniface [Inria, from Jul 2017 until Aug 2017]
Jean Yves Franceschi [Ecole Normale Supérieure Lyon, from Feb 2017 until Jun 2017]
Iris Lohja [Inria, until Aug 2017]
Amine Mansour [Inria, from Apr 2017 until Sep 2017]
Jennifer Ridgers [Inria, from Jul 2017 until Aug 2017]

Administrative Assistant

Helen Pouchot-Rouge-Blanc [Inria]

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. 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. 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. An Privacy Risk Analysis of the TES system

The decree of 28 October 2016 authorising the creation of a centralised file of "secure electronic documents" (TES) has raised a certain number of questions and concerns. The main aim put forward by the French government is the fight against identity fraud. However, the text of the decree also authorises certain accesses to the database by officers of the national police, national Gendarmerie and intelligence. Many voices have been raised to highlight the risks that such a centralised file could represent with regard to individual freedom, and particularly the invasion of citizens' privacy. The strengthening of the means to fight fraud (and, more generally, criminality) and the requirement to protect privacy are not necessarily in contradiction. However, in order to be able to reach a decision on the advantages and disadvantages of a management system for electronic documents, it seemed necessary to: (1) Clearly define the desired functionalities and the advantages that can be expected from them, in particular with respect to the current situation and other solutions. (2) Describe the technical solution chosen in a sufficiently precise way to enable its analysis. (3) Rigorously analyse the risks of an invasion of privacy with regard to the expected benefits.

As a contribution to this debate, we have analyzed several architectures and alternative solutions which are described in an Inria Analysis Note [15]. This note received a lot of attention, and was partially covered by several high-audience media.

4.2. A Novel Authentication Scheme based on Implicit Memory

Selecting and remembering secure passwords puts a high cognitive burden on the user, which has adverse effects on usability and security. Authentication schemes based on implicit memory can relieve the user of the burden of actively remembering a secure password. In [8], we propose a new authentication scheme (MooneyAuth) that relies on implicitly remembering the content of previously seen Mooney images. These images are thresholded two-tone images derived from images containing single objects. Our scheme has two phases: In the enrollment phase, a user is presented with Mooney images, their corresponding original images, and labels. This creates an implicit link between the Mooney image and the object in the user's memory that serves as the authentication secret. In the authentication phase, the user has to label a set of Mooney images, a task that gets performed with substantially fewer mistakes if the images have been seen in the enrollment phase. We applied an information-theoretical approach to compute the eligibility of the user, based on which images were labeled correctly. This new dynamic scoring is substantially better than previously proposed static scoring by considering the surprisal of the observed events. We built a prototype and performed three experiments with 230 and 70 participants over the course of 264 and 21 days, respectively. We show that MooneyAuth outperforms current implicit memory-based schemes, and demonstrates a promising new approach for fallback authentication procedures on the Web. This work was published at ISOC NDSS'17, one of top conferences in security and privacy.

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.

- Participant: Vincent Roca
- Contact: Vincent Roca

5.2. Mobilitcs

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, Franck Baudot, Geoffrey Delcroix, Gwendal Le Grand, Stéphane Petitcolas and Vincent Roca
- Contact: Claude Castelluccia

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: Claude Castelluccia and Pierre Rouveyrol
- Contact: Claude Castelluccia

5.5. OPENFEC

KEYWORD: Error Correction Code
FUNCTIONAL DESCRIPTION: OpenFEC is a C-language implementation of several Application-Level Forward Erasure Correction (AL-FEC) codecs, namely: Reed-Solomon (RFC 5510), LDPC-Staircase (RFC 5170) codes, and RLC (https://datatracker.ietf.org/doc/draft-ietf-tsvwg-rlc-fec-scheme/). Two versions are available: an open-source, unsupported version (http://openfec.org), and an advanced version commercialized by the Expway SME.

RELEASE FUNCTIONAL DESCRIPTION: Added support of RLC codes (Random Linear Codes), based on a sliding encoding window.

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

6. New Results

6.1. A refinement approach for the reuse of privacy risk analysis results

Participants: Daniel Le Métayer, Sourya joyee de.

With the adoption of the EU General Data Protection Regulation (GDPR), conducting a data protection impact assessment will become mandatory for certain categories of personal data processing. A large body of literature has been devoted to data protection impact assessment and privacy impact assessment. However, most of these papers focus on legal and organizational aspects and do not provide many details on the technical aspects of the impact assessment, which may be challenging and time consuming in practice. The general objective of [10] was to fill this gap and to propose a methodology which can be applied to conduct a privacy risk analysis in a systematic way, to use its results in the architecture selection process (following the privacy by design approach and to re-use its generic part for different products or deployment contexts. The proposed analysis proceeds in three broad phases: (1) a generic privacy risk analysis phase which depends only on the specifications of the system and yields generic harm trees; (2) an architecture-based privacy risk analysis which takes into account the definitions of the possible architectures of the system and refines the generic harm trees into architecture-specific harm trees. (3) a context-based privacy risk analysis which 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 into context-specific harm trees. Context-specific harm trees can be used to take decisions about the most suitable architectures.

6.2. Interdisciplinarity in practice: Challenges and benefits for privacy research

Participant: Daniel Le Métayer.

The objective of this work was to draw the lessons learned from a project that involved security systems engineers, computer scientists, lawyers and social scientists. Since one of the goals of the project was to propose actual solutions following the privacy by design approach, its aim was to go beyond multidisciplinarity and build on the variety of expertise available in the consortium to follow a true interdisciplinary approach. We have described the challenges before analyzing the solutions adopted by the project to meet them and the outcomes and benefits of the approach. We have concluded the study with some lessons to be drawn from this experience and recommendations for future interdisciplinary projects.

6.3. Capacity: an abstract model of control over personal data

Participant: Daniel Le Métayer.

While the control of individuals over their personal data is increasingly seen as an essential component of their privacy, the word "control" is usually used in a very vague way, both by lawyers and by computer scientists. This lack of precision may lead to misunderstandings and makes it difficult to check compliance. To address this issue, we have proposed in [17] a formal framework based on capacities to specify the notion of control over personal data and to reason about control properties. We have illustrated our framework with social network systems and shown that it makes it possible to characterize the types of control over personal data that they provide to their users and to compare them in a rigorous way. This work will be presented at CODASPY 2018.

6.4. Privacy Risk Analysis to Enable Informed Privacy Settings

Participants: Daniel Le Métayer, Sourya joyee de.

We have proposed in [16] a method to enable better informed choices of privacy preferences or privacy settings by individuals. The method relies on a privacy risk analysis framework parameterized with privacy settings. The user can express his choices, visualize their impact on the privacy risks through a user-friendly interface, and decide to revise them as necessary to reduce risks to an acceptable level.

6.5. Secure electronic documents: is the centralisation of biometric data really inevitable? Inria Analysis Note

Participants: Claude Castelluccia, Daniel Le Métayer.

The decree of 28 October 2016 authorising the creation of a centralised file of "secure electronic documents" (TES) has raised a certain number of questions and concerns. The main aim put forward by the French government is the fight against identity fraud. However, the text of the decree also authorises certain accesses to the database by officers of the national police, national Gendarmerie and intelligence. Many voices have been raised to highlight the risks that such a centralised file could represent with regard to individual freedom, and particularly the invasion of citizens' privacy. The strengthening of the means to fight fraud (and, more generally, criminality) and the requirement to protect privacy are not necessarily in contradiction. However, in order to be able to reach a decision on the advantages and disadvantages of a management system for electronic documents, it seemed necessary to:

- Clearly define the desired functionalities and the advantages that can be expected from them, in particular with respect to the current situation and other solutions.
- Describe the technical solution chosen in a sufficiently precise way to enable its analysis.
- Rigorously analyse the risks of an invasion of privacy with regard to the expected benefits.

As a contribution to this debate, we have analyzed several architectures and alternative solutions which are described in an Inria Analysis Note [15].

6.6. Biometric Systems Private by Design: Reasoning about privacy properties of biometric system architectures

Participant: Daniel Le Métayer.

The goal of this was to show the applicability of the privacy by design approach to biometric systems and the benefit of using formal methods to this end. Starting from a general framework to define privacy architectures and to formally reason about their properties, we have described its adaptation to biometrics. The choice of particular techniques and the role of the components (central server, secure module, biometric terminal, smart card, etc.) in the architecture have a strong impact on the privacy guarantees provided by a biometric system. In the literature, some architectures have already been analysed in some way. However, the existing proposals were made on a case by case basis, which makes it difficult to compare them and to provide a rationale for the choice of specific options. In this work, we have described, on different architectures providing different levels of protection, how a general framework for the definition of privacy architectures can be used to specify the design options of a biometric systems and to reason about them in a formal way.

6.7. Wi-Fi and privacy

Participants: Mathieu Cunche, Célestin Matte.

As communications-enabled devices are becoming more and more ubiquitous, it becomes easier to track the movements of individuals through the radio signals broadcasted by their devices. While there is a strong interest for physical analytics platforms to leverage this information for many purposes, this tracking also threatens the privacy of individuals. To solve this issue, we propose a privacy-preserving solution for collecting aggregate mobility patterns while at the same time satisfying the strong guarantee of ε-differential privacy. More precisely, we introduce a sanitization mechanism for efficient, privacy-preserving and non-interactive approximate distinct counting for physical analytics based on perturbed Bloom filters. We also extend and generalize previous approaches for estimating distinct count of events and joint events (i.e., intersection, and more generally tout of -n cardinalities). Finally, we experimentally evaluate our approach and compare it to previous ones on a real dataset.

Wi-Fi signals emitted by mobile smartphones can be exploited to passively track users' mobility. Turning off the Wi-Fi interface of the device is often presented as a mean to evade those tracking systems. As a matter of fact this method is sometime suggested by the actors of the Wi-Fi tracking industry as a way to opt-out from those systems. The Android system features an option to enable or disable Wi-Fi on the device. However, disabling Wi-Fi through this option is not sufficient to prevent all Wi-Fi activity of the device. Based on measurements on a range of Android devices, we show in [18] that another option, called "Always allow scanning", when activated, makes a device send Wi-Fi frames which can be used to track this device, even if the Wi-Fi switch is off. This option is not clearly described in all Android versions, and sometimes even not deactivatable. Besides, the Google Maps application prompts the user to activate this option.

6.8. Towards Privacy-preserving Wi-Fi Analytics

Participants: Mathieu Cunche, Mohammad Alaggan.

A new technique enabling non-interactive (t, n)-incidence count estimation for indicator vectors ensuring Differential Privacy has been introduced. Given one or two differentially private indicator vectors, estimating the distinct count of elements in each and their intersection cardinality (equivalently, their inner product) have been studied in the literature, along with other extensions for estimating the cardinality set intersection in case the elements are hashed prior to insertion. The core contribution behind all these studies was to address the problem of estimating the Hamming weight (the number of bits set to one) of a bit vector from its differentially private version, and in the case of inner product and set intersection, estimating the number of positions which are jointly set to one in both bit vectors. We develop in [13] the most general case of estimating the number of positions which are set to one in exactly t out of n bit vectors (this quantity is denoted the (t, n)-incidence count), given access only to the differentially private version of those bit vectors. This means that if each bit vector belongs to a different owner, each can locally sanitize their bit vector prior to sharing it, hence the non-interactive nature of our algorithm. The newly introduced algorithm simultaneously estimates the (t, n)-incidence counts for all $t \in \{0, ..., n\}$. Upper and lower bounds to the estimation error have been derived. The lower bound is achieved by generalizing the limit of two-party differential privacy into n-party differential privacy, which is a contribution of independent interest. We prove that a lower bound on the additive error that must be incurred by any n-wise inner product of n mutually differentially-private bit vectors. Those results are very general and are not limited to differentially private bit vectors. They should apply to a large class of sanitization mechanism of bit vectors which depend on flipping the bits with a constant probability. Some potential applications for this technique include physical mobility analytics, call-detail-record analysis, and similarity metrics computation.

6.9. Towards Implicit Visual Memory-Based Authentication

Participant: Claude Castelluccia.

Selecting and remembering secure passwords puts a high cognitive burden on the user, which has adverse effects on usability and security. Authentication schemes based on implicit memory can relieve the user of the burden of actively remembering a secure password. In [8], we propose a new authentication scheme (MooneyAuth) that relies on implicitly remembering the content of previously seen Mooney images. These images are thresholded two-tone images derived from images containing single objects. Our scheme has two phases: In the enrollment phase, a user is presented with Mooney images, their corresponding original images, and labels. This creates an implicit link between the Mooney image and the object in the user's memory that serves as the authentication secret. In the authentication phase, the user has to label a set of Mooney images, a task that gets performed with substantially fewer mistakes if the images have been seen in the enrollment phase. We applied an information-theoretical approach to compute the eligibility of the user, based on which images were labeled correctly. This new dynamic scoring is substantially better than previously proposed static scoring by considering the surprisal of the observed events. We built a prototype and performed three experiments with 230 and 70 participants over the course of 264 and 21 days, respectively. We show that MooneyAuth outperforms current implicit memory-based schemes, and demonstrates a promising new approach for fallback authentication procedures on the Web.

6.10. MyAdChoices: Bringing transparency and control to online advertising

Participant: Claude Castelluccia.

The intrusiveness and the increasing invasiveness of online advertising have, in the last few years, raised serious concerns regarding user privacy and Web usability. As a reaction to these concerns, we have witnessed the emergence of a myriad of ad-blocking and antitracking tools, whose aim is to return control to users over advertising. The problem with these technologies, however, is that they are extremely limited and radical in their approach: users can only choose either to block or allow all ads. With around 200 million people regularly using these tools, the economic model of the Web—in which users get content free in return for allowing advertisers to show them ads—is at serious peril. In [3], we propose a smart Web technology that aims at bringing transparency to online advertising, so that users can make an informed and equitable decision regarding ad blocking. The proposed technology is implemented as a Web-browser extension and enables users to exert fine-grained control over advertising, thus providing them with certain guarantees in terms of privacy and browsing experience, while preserving the Internet economic model. Experimental results in a real environment demonstrate the suitability and feasibility of our approach, and provide preliminary findings on behavioral targeting from real user browsing profiles.

6.11. Differentially Private Mixture of Generative Neural Networks

Participant: Claude Castelluccia.

Generative models are used in a wide range of applications building on large amounts of contextually rich information. Due to possible privacy violations of the individuals whose data is used to train these models, however, publishing or sharing generative models is not always viable. In [4], we develop a novel technique for privately releasing generative models and entire high-dimensional datasets produced by these models. We model the generator distribution of the training data with a mixture of k generative neural networks. These are trained together and collectively learn the generator distribution of a dataset. Data is divided into k clusters, using a novel differentially private kernel k-means, then each cluster is given to separate generative neural networks, such as Restricted Boltzmann Machines or Variational Autoencoders, which are trained only on their own cluster using differentially private gradient descent. We evaluate our approach using the MNIST dataset, as well as call detail records and transit datasets, showing that it produces realistic synthetic samples, which can also be used to accurately compute arbitrary number of counting queries.

6.12. Revisiting Private Web Search using Intel SGX

Participant: Antoine Boutet.

The leakage of user search queries by search engines, which is at the heart of their economic model, makes private Web search an essential functionality to offer to those users that care about their privacy. Nowadays, there exists no satisfactory approach to enable users to access search engines in a privacy-preserving way. Existing solutions are either too costly due to the heavy use of cryptographic mechanisms (e.g., private information retrieval protocols), subject to attacks (e.g., Tor, TrackMeNot, GooPIR) or rely on weak adversarial models (e.g., PEAS). This work [6] introduces X-Search, a novel private Web search mechanism building on the disruptive software guard extensions (SGX) proposed by Intel. We compare X-Search to its closest competitors, Tor and PEAS using a dataset of real web search queries. Our evaluation shows that: (1) X-Search offers stronger privacy guarantees than its competitors as it operates under a stronger adversarial model; (2) it better resists state-of-the-art re-identification attacks; (3) from the performance perspective, X-Search outperforms its competitors both in terms of latency and throughput by orders of magnitude.

6.13. PULP: Achieving Privacy and Utility Trade-off in User Mobility Data

Participant: Antoine Boutet.

Leveraging location information in location-based services leads to improving service utility through geo-contextualization. However, this raises privacy concerns as new knowledge can be inferred from location records, such as user's home and work places, or personal habits. Although Location Privacy Protection Mechanisms (LPPMs) provide a means to tackle this problem, they often require manual configuration posing significant challenges to service providers and users. Moreover, their impact on data privacy and utility is seldom assessed. In [9], we present PULP, a model-driven system which automatically provides user-specific privacy protection and contributes to service utility via choosing adequate LPPM and configuring it. At the heart of PULP is nonlinear models that can capture the complex dependency of data privacy and utility for each individual user under given LPPM considered, i.e., Geo-Indistinguishability and Promesse. According to users' preferences on privacy and utility, PULP efficiently recommends suitable LPPM and corresponding configuration. We evaluate the accuracy of PULP's models and its effectiveness to achieve the privacy-utility trade-off per user, using four real-world mobility traces of 770 users in total. Our extensive experimentation shows that PULP ensures the contribution to location service while adhering to privacy constraints for a great percentage of users, and is orders of magnitude faster than non-model based alternatives.

6.14. The Pitfalls of Hashing for Privacy

Participants: Cédric Lauradoux, Mathieu Cunche, Levent Demir.

Boosted by recent legislations, data anonymization is fast becoming a norm. However, as of yet no generic solution has been found to safely release data. As a consequence, data custodians often resort to ad-hoc means to anonymize datasets. Both past and current practices indicate that hashing is often believed to be an effective way to anonymize data. Unfortunately, in practice it is only rarely effective. In [2], we expose the limits of cryptographic hash functions as an anonymization technique. Anonymity set is the best privacy model that can be achieved by hash functions. However, this model has several shortcomings. We provide three case studies to illustrate how hashing only yields a weakly anonymized data. The case studies include MAC and email address anonymization as well as the analysis of Google Safe Browsing.

6.15. Duck Attack on Accountable Distributed Systems

Participant: Cédric Lauradoux.

Accountability plays a key role in dependable distributed systems. It allows to detect, isolate and churn malicious/selfish nodes that deviate from a prescribed protocol. To achieve these properties, several accountable systems use at their core cryptographic primitives that produce non-repudiable evidence of inconsistent or incorrect behavior. In [11], we show how selfish and colluding nodes can exploit the use of cryptographic digests in accountability protocols to mount what we call a duck attack. In a duck attack, selfish and colluding nodes exploit the use of cryptographic digests to alter the transmission of messages while masquerading as honest entities. The end result is that their selfish behavior remains undetected. This undermines the security

guarantees of the accountability protocols. We first discover the duck attack while analyzing PAG – a custom cryptographic protocol to build accountable systems presented at ICDCS 2016. We later discover that accountable distributed systems based on a secure log (essentially a hash-based data structure) are also vulnerable to the duck attack and apply it on AcTinG – a protocol presented at SRDS 2014. To defeat our attack, we modify the underlying secure log to have high-order dependency on the messages stored in it.

6.16. Less Latency and Better Protection with AL-FEC Sliding Window Codes: a Robust Multimedia CBR Broadcast Case Study

Participants: Vincent Roca, Belkacem Teibi.

Application-Level Forward Erasure Correction (AL-FEC) codes have become a key component of communication systems in order to recover from packet losses. This work analyzes the benefits of the AL-FEC codes based on a sliding encoding window (A.K.A. convolutional codes) for the reliable broadcast of real-time flows to a potentially large number of receivers over a constant bit rate channel. It first details the initialization of both sliding window codes and traditional block codes in order to keep the maximum AL-FEC decoding latency below a target latency budget. Then it presents detailed performance analyzes using official 3GPP mobility traces, representative of our use case which involves mobile receivers. This work highlights the major benefits of RLC codes, representative of sliding window codes, that outperform any block code, from Raptor codes (that are part of 3GPP MBMS standard) up to ideal MDS codes, both in terms of reduced added latency and improved robustness. It also demonstrates that our RLC codec features decoding speeds that are an order of magnitude higher than that of Raptor codes.

6.17. Coding for efficient Network Communications Research Group (NWCRG)

Participants: Vincent Roca, Belkacem Teibi.

In the context of the "Coding for efficient Network Communications IRTF Research Group (NWCRG) » (https://datatracker.ietf.org/rg/nwcrg/), several activities have been carried out. First of all, a recommended terminology for Network Coding concepts and constructs has been elaborated. It provides a comprehensive set of terms in order to avoid ambiguities in future Network Coding IRTF and IETF documents.

Then, in order to facilitate the use of Sliding Window Codes, such as RLC (see the above FEC Scheme) and RLNC codes (i.e., the well known codes for network coding applications, with potential re-encoding within the network), a work started that introduces a generic Application Programming Interface (API) for window-based FEC codes. This API is meant to be usable by any sliding window FEC code, independently of the FEC Scheme or network coding protocol that may rely on it. This API defines the core procedures and functions meant to control the codec (i.e., implementation of the FEC code), but leaves out all upper layer aspects (e.g., signalling) that are the responsibility of the application making use of the codec. A goal of this document is to pave the way for a future open-source implementation of such codes.

Finally, we started to work on the motivation and requirements for the use of Network Level Packet Erasure Coding to improve the performance of the QUIC protocol that is proposed a new transport protocol. The goal at this level is not specify a specific code but to list the salient features that a code should have in order to deal with know loss patterns on QUIC paths.

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

Title: ADAGE (Anonymous Mobile Traffic Data Generation).

Type: FUI.

Duration: July 2016 - September 2018.

Coordinator: Orange.

Others partners: Inria, CNRS LAAS.

Abstract: The project ADAGE aims at developping solutions for the anonymization of mobility traces produced by mobile operators.

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.

8.1.2.2. SIDES 3.0

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

Type: ANR.

Duration: August 2017 - August 2020.

Coordinator: Uness (France).

Others partners: Inria, UGA, ENS, Theia, Viseo.

Abstract: Since 2013, faculties of medicine have used a shared national platform that enables them to carry out all of their validating exams on tablets with automatic correction. This web platform entitled SIDES allowed the preparation of the medical students to the Computerized National Classing Events (ECN) which were successfully launched in June 2016 (8000 candidates simultaneously throughout France). SIDES 3.0 proposes to upgrade the existing platform. Privatics goals in this project is to ensure that privacy is respected and correctly assessed .

8.1.2.3. DAPCODS/IOTics

Title: DAPCODS/IOTics.

Type: ANR 2016.

Duration: May 2017 - Dec. 2020.

Coordinator: Inria PRIVATICS.

Others partners: Inria DIANA, EURECOM, Univ. Paris Sud, CNIL.

Abstract:

Thanks to the exponential growth of Internet, citizens have become more and more exposed to personal information leakage in their digital lives. This trend began with web tracking when surfing the Internet with our computers. The advent of smartphones, our personal assistants always connected and equipped with many sensors, further reinforced this tendency. And today the craze for "quantified self" wearable devices, for smart home appliances or for other connected devices enable the collection of potentially highly sensitive personal information in domains that were so far out of reach. However, little is known about the actual practices in terms of security, confidentiality, or data exchanges. The enduser is therefore prisoner of a highly asymmetric system. This has important consequences in terms of regulation, sovereignty, and leads to the hegemony of the GAFAs (Google, Amazon, Facebook and Apple). Security, transparency and user control are three key properties that should be followed by all the stakeholders of the smartphone and connected devices ecosystem. Recent scandals show that the reality is sometimes at the opposite.

The DAPCODS project gathers four renowned research teams, experts in security, privacy and digital economy. They are seconded by CNIL, the French data protection agency. The project aims at contributing along several axes:

- by analyzing the inner working of a significant set of connected devices in terms of personal information leaks. This will be made possible by analyzing their data flows (and associated smartphone application if applicable) from outside (smartphone and/or Wifi network) or inside, through ondevice static and dynamic analyses. New analysis methods and tools will be needed, some of them leveraging on previous works when applicable;
- by studying the device manufacturers' privacy policies along several criteria (e.g., accessibility, precision, focus, privacy risks). In a second step, their claims will be compared to the actual device behavior, as observed during the test campaigns. This will enable an accurate and unique ranking of connected devices;
- by understanding the underlying ecosystem, from the economical viewpoint. Data collected will make it possible to define the blurred boundaries of personal information market, a key aspect to set up an efficient regulation;
- and finally, by proposing a public website that will rank those connected devices and will inform citizens. We will then test the impact of this information on the potential change of behavior of stakeholders.

By giving transparent information of hidden behaviors, by highlighting good and bad practices, this project will contribute to reduce the information asymmetry of the system, to give back some control to the endusers, and hopefully to encourage certain stakeholders to change practices.

8.1.3. Inria Innovation Laboratory

Title: LEELCO (Low End-to-End Latency COmmunications).

Duration: 3 years (2015 - 2018).

Coordinator: Inria PRIVATICS.

Others partners: Expway.

Abstract:

This Inria Innovation Lab aims at strengthening Expway (http://www.expway.com/) commercial offer with technologies suited to real-time data transmissions, typically audio/video flows. In this context, the end-to-end latency must be reduced to a minimum in order to enable a high

quality interaction between users, while keeping the ability to recover from packet losses that are unavoidable with wireless communications in harsh environments. In this collaboration we focus on new types of Forward Erasure Correction (FEC) codes based on a sliding encoding windows, and on the associated communication protocols, in particular an extension to FECFRAME (RFC6363) to such FEC codes. The outcomes of this work are proposed to both IETF and 3GPP standardisation organisations, in particular in the context of 3GPP mission critical communication services activity. The idea of this 3GPP activity is to leverage on the 3GPP Evolved Multimedia Broadcast Multicast Services (eMBMS) and on the existing Long Term Evolution (LTE) infrastructure for critical communications and such services as group voice transmissions, live high-definition video streams and large data transmissions. In this context, the advanced FEC codes studied in LEELCO offer a significant improvement both from the reduced latency and increased loss recovery viewpoints compared to the Raptor codes included in the existing standard (https://hal.inria.fr/hal-01571609v1/en/).

8.1.4. Inria CNIL project

Privatics is in charged of the Cnil-Inria collaboration. This collaboration was at the origin of the Mobilitics project and it is now at the source of many discussions and collaborations on data anoymisation, risk analysis, consent or IoT Privacy. Privatics and Cnil are both actively involved on the IoTics project, that is the follow-up of the Mobilitics projects. The goal of the Mobilitics project was to study information leakage in mobile phones. The goal of IoTics is to extend this work to IoT and connected devices.

Privatics is also in charged of the organization of the Cnil-Inria prize that is awarded every year to an outstanding publication in the field of data privacy.

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).

8.3.3. Data Institute

- Title: Data Institute UGA
- Duration: 2017 - .
- Coordinator: TIMC-IMAG.

- Others partners: AGEIS, BIG, CESICE, GIN, GIPSA-lab, IAB, IGE, IPAG, LAPP, LARHRA, LIDILEM, LIG, LISTIC, LITT&ArTS, LJK, LUHCIE, LECA, OSUG, PACTE, TIMC-IMAG, Inria
- Abstract: Privatics is leading the WP5 (Data Governance, Data Protection and Privacy). This action (WP5) aims to analyze, in a multi-disciplinary perspective, why and how specific forms of data governance emerge as well as the consequences on the interaction between the state, the market and society. The focus will be on the challenges raised by the collection and use of data for privacy, on the data subjects' rights and on the obligations of data controllers and processors. A Privacy Impact/Risk assessments methodology and software will be proposed. A case study will focus on medical and health data and make recommendations on how they should be collected and processed

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific Events Organisation

9.1.1.1. Member of the Organizing Committees

C. Castelluccia: Co-chair of the DTL Grant program (http://datatransparencylab.org/grants-program/), Co-chair of the Workshop on "Intelligence Oversight", (Nov., Montbonnot).

D. Le Metayer: APVP 2017 (Jun., Autrans), panel on "Algorithms: too intelligent to be intelligeable ?" at CPDP 2017 (Jan., Brussels).

M. Cunche: APVP 2017 (Jun., Autrans).

9.1.2. Scientific Events Selection

9.1.2.1. Member of the Conference Program Committees

C. Castelluccia: DTL Grant program, ACM Symposium on Applied Computing (Privacy by Design in Practice track).

D. Le Métayer: CSF 2017, IWPE 2017, APF 2017, CPDP 2017, Conference "Converging trends between law and digital technologies".

V. Roca: VTC 2017, SPACOMM 2017, SpaCCS 2017.

M. Cunche: Mobiquitous 2017, ICISSP 2017.

9.1.3. Invited Talks

D. Le Métayer on *Intelligence and the scientific community*, organized by the French Intelligence Academy in partnership with the Academy of Technologies, (Paris, Jun. 2017).

D. Le Métayer on *Personal data protection*, organized by ANVIE (Association nationale de valorisation interdisciplinaire de la recherche en sciences humaines et sociales auprès des entreprises), (Paris, May 2017).

D. Le Métayer on *The ethics of algorithms*, organized by FFA (Fédération Française des Assurance), (Paris, Jul. 2017).

D. Le Métayer on *Algorithmes prédictifs: Quels enjeux éthiques et juridiques?*, organized by CREOGN (Centre de recherche de l'École des officiers de la gendarmerie nationale), (Paris, Oct. 2017).

D. Le Métayer on *Capacity: an abstract model of control over personal data* invited talk at Chalmers University, (Göteborg, Nov. 2017).

Claude Castelluccia on *Promoting Peace on the Internet*, organized by Unesco (Paris, Apr. 2017).

Claude Castelluccia Oxford Internet Institute, (Oxford, Jul. 2017).

9.1.4. Leadership within the Scientific Community

C. Castelluccia: member of the scientific committee of the CNIL-Inria Privacy Award, co-creator and board member of the Amnesys (Alpine Multidisciplinary NEtwork on CYber-security Studies) group (http://amnecys.inria.fr), co-leader of the WP5 of the Data Institute of UGA (https://data-institute.univ-grenoble-alpes.fr).

D. Le Métayer: member of the scientific committee of the CNIL-Inria Privacy Award, member of the editorial committee of the Transalgo Inria platform.

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

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 : 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 : 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 : Jessye Dos Santos, *Sensor Networks and Privacy*, Claude Castelluccia and Cedric Lauradoux.

PhD defended : Levent Demir, *Trusted module for data outsourcing in the Cloud*, Vincent Roca.

PhD defended : Celestin Matte, *Wi-Fi tracking: Fingerprinting Attacks and Counter-Measures*, Mathieu Cunche.

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

PhD in progress : Mathieu Thiery, *IoT privacy* , September 2016, Vincent Roca.

PhD in progress : Guillaume Celosia, *Wireless Privacy in the Internet of Things* , November 2017, Mathieu Cunche and Daniel.

Intern (M2): Jean-Yves Franceschi, *Accountability of Decision Algorithms*, Daniel Le Métayer Le Métayer.

Intern (M2): Amine Mansour, *Algorithmes d'aide à la décision : des questions éthiques aux défis techniques*, Daniel Le Métayer.

Intern (M2): Jean-Yves Franceschi, *Accountability of Decision Algorithms*, Daniel Le Métayer.

Intern (M2): Coline Boniface, *Laws and Cyberweapons*, Cédric Lauradoux and Claude Castelluccia.

Intern (M2): Jennifer Ridgers, *Surveillance and Social Networks*, Claude Castelluccia and Cédric Lauradoux.

Intern (M1): Iris Lohja, *Mail-Analytics*, Cédric Lauradoux.

9.2.3. Juries

HdR: Melek ONEN, *Security and Privacy for Emerging Technologies*, Eurecom, 12/01/2017, Claude Castelluccia.

PhD: Jessye Dos Santos, *Sensor Networks and Privacy*, 18/10/2016, Claude Castelluccia and Cédric Lauradoux.

PhD: Levent Demir, *Trusted module for data outsourcing in the Cloud*, Université Grenoble Alpes, Grenoble, 07/12/2017, Vincent Roca.

PhD: Celestin Matte, *Wi-Fi tracking: Fingerprinting Attacks and Counter-Measures*, Université Claude Bernard Lyon 1, 8/9/2016, Mathieu Cunche.

PhD: Pierre Laperdrix, *Browser Fingerprinting: Diversity to Augment Authentication and Build Client-side Countermesures*, Rennes University, 03/10/2017, Claude Castelluccia.

PhD: Alban Petit, *Introducing Privacy in Current Web Search Engines*, Insa Lyon, 15/03/2017, Claude Castelluccia..

PhD: Raphaël Gellert, *Understanding the risk-based approach to data protection: An analysis of the links between law, regulation, and risk*, Vrije Universiteit Brussel (VUB), Belgium, 15/06/2017, Daniel Le Métayer.

PhD: Walid Benghabrit, *A formal model for accountability*, IMT Atlantique Bretagne-Pays de la Loire, 27/10/2017, Daniel Le Métayer.

PhD: Raul Pardo, 22 November 2017, Privacy policies for social network – A formal approach, Chalmers University, Göteborg, Sweeden, 22/11/2017, Daniel Le Métayer.

9.3. Popularization

9.3.1. Hearings

D. Le Métayer at the French National Assembly about the implementation of the General Data Protection Regulation (Jan. 2017).

D. Le Métayer at the Conseil national du numérique (CNNum) about the regulation of algorithms (Jul. 2017).

M. Cunche at le Comité Consultatif National d'Ethique (CCNE)[1] (Mar. 2017).

[1] http://www.ccne-ethique.fr/fr

9.3.2. Interviews

M. Cunche by Valentine Faure in Glamour, Donner ses données, juin-juillet 2017.

M. Cunche by Martin Untersinger in lemonde.fr, Apple donne à nouveau des gages en matière de vie privée, 27/09/2017, http://www.lemonde.fr/pixels/article/2017/09/27/apple-donne-a-nouveau-des-gages-en-matiere-de-vie-privee_5192469_4408996.html

M. Cunche by Arnaud Devillard in Sciences et Avenir, Même coupé, le Wi-Fi sous Android peut suivre le téléphone, Oct. 2017, https://www.sciencesetavenir.fr/high-tech/meme-coupe-le-wi-fi-sous-android-peut-suivre-le-telephone_116061

M. Cunche by Camille Gruhier in Que-choisir, Smartphones Android Même une fois le Wi-Fi désactivé, vous êtes pisté, Oct. 2017 https://www.quechoisir.org/actualite-smartphones-android-meme-une-fois-le-wi-fi-desactive-vous-etes-piste-n46076/

M. Cunche by Emilie Brouze in Rue89 - L'Obs, Tu es resté 22 minutes chez l'opticien jeudi. Le centre commercial le sait, le 12 juillet 2017, http://tempsreel.nouvelobs.com/rue89/rue89-nos-vies-connectees/20170711.OBS1939/vous-etes-reste-22-minutes-chez-l-opticien-jeudi-et-le-centre-commercial-le-sait.html

M. Cunche by ZDnet.fr, http://www.zdnet.fr/actualites/android-desactiver-le-wi-fi-n-empeche-pas-d-etre-espionne-39856640.htm

M. Cunche by 01Net, http://www.01net.com/actualites/sur-android-le-wi-fi-peut-vous-tracer-meme-s-il-est-desactive-1245292.html

M. Cunche by l'informaticien, https://www.linformaticien.com/actualites/id/44894/desactiver-le-wifi-pour-eviter-le-flicage-une-protection-illusoire.aspx

M. Cunche by Nextinpact, https://m.nextinpact.com/news/105038-suivi-clients-dans-magasins-question-wi-fi-nest-pas-seule-a-se-poser.htm

C. Lauradoux by Sophie Eremian in Inriality, Quand l'énergie devient intelligente, Oct. 2017, https://www.inriality.fr/environnement/quand-lenergie-devient-intelligente/.

9.3.3. Press articles

D. Le Métayer in Slate, *Designing, explaining and controling algorithms*, in Presidential election, 100 proposals from the research community (Mar. 2017).

D. Le Métayer in Le Monde, *Gouverner les algorithmes pour éviter qu'ils nous gouvernent*, (Nov. 2017).

C. Castelluccia and D. Le Métayer in Inria Analysis note, *Secure electronic documents: is the centralisation of biometric data really inevitable?*, (Feb. 2017).

9.3.4. Conferences

M. Cunche and C. Matte, *le traçage cyberphysique via Wi-Fi*, Exposition Terra Data at Cité des Sciences et de l'Industrie, Apr. 2017.

M. Cunche and C. Matte, *le traçage cyberphysique via Wi-Fi*, Fête de la science at Cité des Sciences et de l'Industrie, Oct. 2017 (broadcasted by Science et Vie TV and animated by l'Esprit Sorcier).

C. Lauradoux, *Email et vie privée: pourquoi utiliser GPG ?*, Cours Master 2, Nov. 2017.

C. Lauradoux, *Mathématiques et la protection de la vie privée*, Olympiades académiques de Mathématiques, May 2017.

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

C. Lauradoux, *Cryptanalyse*, stage MathC2+, 06/2017.

10. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] C. MATTE. *Wi-Fi Tracking: Fingerprinting Attacks and Counter-Measures*, Université de Lyon, December 2017, https://hal.archives-ouvertes.fr/tel-01659783

Articles in International Peer-Reviewed Journals

[2] L. DEMIR, A. KUMAR, M. CUNCHE, C. LAURADOUX. *The Pitfalls of Hashing for Privacy*, in "Communications Surveys and Tutorials, IEEE Communications Society", 2018, https://hal.inria.fr/hal-01589210

[3] J. PARRA-ARNAU, J. P. ACHARA, C. CASTELLUCCIA. *MyAdChoices: Bringing transparency and control to online advertising*, in "ACM Transaction on the Web", April 2017, vol. 11, n^{o} 1, https://hal.inria.fr/hal-01636611

International Conferences with Proceedings

[4] G. ACS, L. MELIS, E. DI CRISTOFARO, C. CASTELLUCCIA. *Differentially Private Mixture of Generative Neural Networks*, in "ICDM 2017 - IEEE International Conference on Data Mining", New-orleans, United States, November 2017, https://hal.inria.fr/hal-01636571

[5] M. ALAGGAN, M. CUNCHE, M. MINIER. *Non-interactive (t, n)-Incidence Counting from Differentially Private Indicator Vectors*, in "3rd International Workshop on Security and Privacy Analytics (IWSPA 2017)", Scottsdale, United States, March 2017, https://hal.inria.fr/hal-01485412

[6] S. BEN MOKHTAR, A. BOUTET, P. FELBER, M. PASIN, R. PIRES, V. SCHIAVONI. *X-Search: Revisiting Private Web Search using Intel SGX*, in "Middleware", Las Vegas, United States, December 2017, 12 p. [*DOI :* 10.1145/3135974.3135987], https://hal.inria.fr/hal-01588883

[7] M. CANET, A. KUMAR, C. LAURADOUX, M.-A. RAKOTOMANGA, R. SAFAVI-NAINI. *Decompression Quines and Anti-Viruses*, in "CODASPY 2017 - 7th ACM Conference on Data and Application Security and Privacy", Scottsdale, United States, March 2017 [*DOI :* 10.1145/3029806.3029818], https://hal.inria.fr/hal-01589192

[8] C. CASTELLUCCIA, M. DUERMUTH, M. GOLLA, F. DENIZ. *Towards Implicit Visual Memory-Based Authentication*, in "Network and Distributed System Security Symposium (NDSS)", San Diego, United States, ISOC, February 2017, https://hal.inria.fr/hal-01109765

[9] S. CERF, V. PRIMAULT, A. BOUTET, S. BEN MOKHTAR, R. BIRKE, S. BOUCHENAK, L. Y. CHEN, N. MARCHAND, B. ROBU. *PULP: Achieving Privacy and Utility Trade-off in User Mobility Data*, in "SRDS 2017 - 36th IEEE International Symposium on Reliable Distributed Systems", Hong Kong, Hong Kong SAR China, September 2017, https://hal.archives-ouvertes.fr/hal-01578635

[10] S. J. DE, D. LE MÉTAYER. *A Refinement Approach for the Reuse of Privacy Risk Analysis Results*, in "Annual Privacy Forum", Vienne, Austria, June 2017, vol. 10518, pp. 52 - 83, https://hal.inria.fr/hal-01671345

[11] A. KUMAR, C. LAURADOUX, P. LAFOURCADE. *Duck Attack on Accountable Distributed Systems*, in "MobiQuitous 2017 - 14th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services", Melbourne, Australia, November 2017, pp. 1-8, https://hal.inria.fr/hal-01589196

[12] V. ROCA, B. TEIBI, C. BURDINAT, T. TRAN, C. THIENOT. *Less Latency and Better Protection with AL-FEC Sliding Window Codes: a Robust Multimedia CBR Broadcast Case Study*, in "WiMob 2017 - 13th IEEE International Conference on Wireless and Mobile Computing, Networking and Communications", Rome, Italy, General Chair: Abderrahim Benslimane - University of Avignon, France, October 2017, 9 p. , https://hal.inria.fr/hal-01571609

Conferences without Proceedings

[13] M. ALAGGAN, M. CUNCHE, S. GAMBS. *Towards Privacy-preserving Wi-Fi Analytics*, in "Atelier sur la Protection de la Vie Privée (APVP)", Autran, France, June 2017, https://hal.inria.fr/hal-01587745

[14] S. BEN MOKHTAR, A. BOUTET, L. BOUZOUINA, P. BONNEL, O. BRETTE, L. BRUNIE, M. CUNCHE, S. D 'ALU, V. PRIMAULT, P. RAVENEAU, H. RIVANO, R. STANICA. *PRIVA'MOV: Analysing Human Mobility Through Multi-Sensor Datasets*, in "NetMob 2017", Milan, Italy, April 2017, https://hal.inria.fr/hal-01578557

Research Reports

[15] C. CASTELLUCCIA, D. LE MÉTAYER. *NOTE D'ANALYSE Titres électroniques sécurisés : la centralisation des données biométriques est-elle vraiment inévitable ? Analyse comparative de quelques architectures*, Inria Grenoble - Rhône-Alpes, February 2017, https://hal.inria.fr/hal-01467902

[16] D. LE MÉTAYER, S. J. DE. *Privacy Risk Analysis to Enable Informed Privacy Settings*, Inria - Research Centre Grenoble – Rhône-Alpes, December 2017, n^{o} RR-9125, pp. 1-24, https://hal.inria.fr/hal-01660045

[17] D. LE MÉTAYER, P. RAUZY. *Capacity: an Abstract Model of Control over Personal Data*, Inria Grenoble Rhône-Alpes ; Université Paris 8, November 2017, n^{o} RR-9124, pp. 1-21 [*DOI :* 10.1145/3176258.3176314], https://hal.inria.fr/hal-01638190

[18] C. MATTE, M. CUNCHE, V. TOUBIANA. *Does disabling Wi-Fi prevent my Android phone from sending Wi-Fi frames?*, Inria - Research Centre Grenoble – Rhône-Alpes ; INSA Lyon, August 2017, n^{o} RR-9089, https://hal.inria.fr/hal-01575519

Scientific Popularization

[19] C. MATTE. *Transfert de style : et si Van Gogh peignait Tux ?*, in "Linux Magazine France", March 2017, n^{o} 202, https://hal.inria.fr/hal-01518996

Other Publications

[20] B. ADAMSON, C. ADJIH, J. BILBAO, V. FIROIU, F. FITZEK, G. SAMAH A. M., E. LOCHIN, A. MASUCCI, M.-J. MONTPETIT, M. V. PEDERSEN, G. PERALTA, V. ROCA, S. PARESH, S. SIVAKUMAR. *Network Coding Taxonomy*, July 2017, Internet Research Task Force - Working document of the Network Coding Research Group (NWCRG), draft-irtf-nwcrg-network-coding-taxonomy-05 (work in progress), https://datatracker.ietf.org/doc/draft-irtf-nwcrg-network-coding-taxonomy/, https://hal.inria.fr/hal-00998506

[21] V. ROCA, A. BEGEN. *Forward Error Correction (FEC) Framework Extension to Sliding Window Codes*, July 2017, Working document of the TSVWG (Transport Area Working Group) group of IETF (Internet Engineering Task Force), draft-ietf-tsvwg-fecframe-ext-00 (work in progress), https://datatracker.ietf.org/doc/draft-ietf-tsvwg-fecframe-ext/, https://hal.inria.fr/hal-01345125

[22] V. ROCA, J. DETCHART, C. ADJIH, M. V. PEDERSEN, I. SWETT. *Generic Application Programming Interface (API) for Window-Based Codes*, October 2017, Internet Research Task Force - Working document of the Network Coding Research Group (NWCRG), draft-roca-nwcrg-generic-fec-api-00 (work in progress), https://datatracker.ietf.org/doc/draft-roca-nwcrg-generic-fec-api/, https://hal.inria.fr/hal-01630138

[23] V. ROCA, B. TEIBI, C. BURDINAT, T. TRAN-THAI, C. THIENOT. *Block or Convolutional AL-FEC Codes? A Performance Comparison for Robust Low-Latency Communications*, February 2017, working paper or preprint, https://hal.inria.fr/hal-01395937

[24] V. ROCA, B. TEIBI. *Sliding Window Random Linear Code (RLC) Forward Erasure Correction (FEC) Schemes for FECFRAME*, October 2017, pp. 1-25, Working document of the TSVWG (Transport Area Working Group) group of IETF (Internet Engineering Task Force), draft-ietf-tsvwg-rlc-fec-scheme-01 (work in progress), https://datatracker.ietf.org/doc/draft-ietf-tsvwg-rlc-fec-scheme/, https://hal.inria.fr/hal-01630089

[25] I. SWETT, M.-J. MONTPETIT, V. ROCA. *Network Layer Coding for QUIC: Requirements*, October 2017, Internet Research Task Force - Working document of the Network Coding Research Group (NWCRG), https://hal.inria.fr/hal-01630152

[26] C. THIENOT, C. BURDINAT, T. TRAN, V. ROCA, B. TEIBI. *Pseudo-CR Convolutional FEC for MCVideo*, November 2017, 3GPP TSG-SA WG4 Meeting #96, Albuquerque, New Mexico, 13th – 17th November 2017, https://hal.inria.fr/hal-01632469