IN PARTNERSHIP WITH:
Institut national des sciences appliquées de Lyon

Activity Report 2015

Project-Team PRIVATICS

Privacy Models, Architectures and Tools for the Information Society

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
9.10. - Ethics
9.8. - Privacy
9.9. - Risk management

1. Members

Research Scientists

Claude Castelluccia [Team leader, Inria, Senior Researcher, HdR]
Cedric 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 [INSA Lyon, Associate Professor, HdR]

Engineers

Gergely Acs [Inria, granted by ANR PFLOWER project]
Pierre Rouveyrol [Inria, until May 2015]
Belkacem Teibi [Inria, from Oct 2015]

PhD Students

Jagdish Achara [Inria]
Thibaud Antignac [Inria, until Feb 2015, granted by FP7 PRIPARE project]
Levent Demir [INCAS-ITSEC, granted by CIFRE]
Jessye Dos Santos [CEA]
Amrit Kumar [Univ. Grenoble I]
Celestin Matte [INSA Lyon]
Lukasz Olejnik [Inria, until Jan 2015]

Post-Doctoral Fellows

Sourya Joyee de [Inria, from Jul 2015]
Gabor Gulyas [Inria, from Jun 2015]
Sofiane Lagraa [INSA Lyon, from Oct 2015]
Javier Parra Arnau [Inria, until Nov 2015]
Pablo Rauzy [Inria, from Oct 2015]

Visiting Scientist

Luca Melis [Inria, PhD, from Sep 2015 until Dec 2015]

Administrative Assistant

Helen Pouchot-Rouge-Blanc [Inria]

Others

Leo Le Taro [Univ. Lyon I, Stagiaire M2, from Feb 2015 until Jul 2015]
Khaoula Dhifallah [Inria, Stagiaire M2, from Feb 2015 until Jul 2015]
Jose Paul Dominguez [Inria, Stagiaire M1, from Feb 2015]
Saikou Fall [Inria, Stagiaire M2, from May 2015 until Sep 2015]
Lenka Kunikova [Inria, Stagiaire M1, from Feb 2015 until Jun 2015]
Michael Omer [Inria, Stagiaire M1, from Feb 2015 until Jun 2015]
Quentin Ricard [Inria, Stagiaire M1, from Feb 2015 until Aug 2015]
Aude Tessier [Inria, Stagiaire M2, from Jul 2015 until Sep 2015]
Mathieu Thiery [Inria, Stagiaire M1, from Mar 2015 until Sep 2015]
Jonathan Tournier [Inria, Stagiaire M1, from Feb 2015 until Jun 2015]
Mathilde Vernet [Inria, Stagiaire L3, from May 2015 until Jul 2015]

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

Our work on "Probabilistic k^m-anonymity" was published in the IEEE International Conference on Big Data (BigData) 2015.

Our results on Password security, "Faster Password Guessing Using an Ordered Markov Enumerator" and "Interleaving Cryptanalytic Time-memory Trade-offs on Non-Uniform Distributions", were published at ESSOS'15 and ESORICS'15.

The team published 2 papers about his research in the newspaper "Lemonde", 1 article in "Science & Avenir" and in "La Recherche".

The team organized the 31 November 2015 the conference "Privacy across cultures, Convergences and divergences in a global world" in the context of the Rencontres Jacques Cartier.

4.1.1. Awards

The paper "Reasoning about privacy properties of biometric system architectures in the presence of information leakage" [15] received the best paper award at ISC 2015.

BEST PAPER AWARD:

[15]
D. LE MÉTAYER, H. CHABANNE, L. ROCH, J. BRINGER. *Reasoning about privacy properties of biometric system architectures in the presence of information leakage*, in "Information Security Conference (ISC 2015)", Trondheim, Norway, Springer , November 2015, https://hal.inria.fr/hal-01247064

5. New Software and Platforms

5.1. 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/fr/mobilitics/

5.2. 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

5.3. 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/

5.4. FECFRAME

FUNCTIONAL DESCRIPTION

FECFRAME implements IETF FECFRAME (RFC 6363). It allows to transmit multimedia streams to one or severals receivers at the same time while being robust to packet losses occurring on the network (par ex. 3G/4G or Wifi). This software is compatible with OpenFec which provides error-correcting codes.

- Participants: Vincent Roca
- Contact: Vincent Roca

5.5. WALTER

Walter experiment: "Is My Web Content Altered?". A web based tool detecting the unwanted injection of scripts and other contents in unencrypted webpages.

FUNCTIONAL DESCRIPTION

Disputable network agents, namely free Wi-Fi hotspots providers such as those found in airports or coffee shops, have been found to monetize their networks by injecting advertisements and trackers into their customers' traffic. Such adverts are served by network agents instead of website publishers. This is a relatively new approach, and we are trying to determine its usage worldwide. This website is designed to assess whether your internet connection is affected by such practices. We also detect local page alterations that come from browser extensions and programs that may run on your machine.

- Participants: Mathieu Cunche, Leo Letaro.
- Contact: Mathieu Cunche

6. New Results

6.1. Surveillance

Participants: Claude Castelluccia, Javier Parra Arnau.

In recent times, we are witnessing an increasing concern by governments and intelligence agencies to deploy mass-surveillance systems that help them fight terrorism. In [40], we conduct a formal analysis of the overall cost of such surveillance systems. Our analysis starts with a fairly-known result in statistics, namely, the false-positive paradox. We propose a quantitative measure of the total cost of a monitoring program, and study a detection system that is designed to minimize it, subject to a constraint in the number of terrorists the agency wishes to capture. In the absence of real, accurate behavioral models, we perform our analysis on the basis of several simple but insightful examples. With these examples, we illustrate the different parameters involved in the design of the detection system, and provide some indicative and representative figures of the cost of the monitoring program.

6.2. 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 softwares and lose all personal data to security companies. As a example of this dilemma, we analyze the solution proposed by Google for Safe Browsing in [29] and shows that their privacy policies do not match the reality: Google can perform tracking.

6.3. Users characterization

Participants: Jagdish Achara, Gergely Acs, Claude Castelluccia.

Prior works have shown that the list of apps installed by a user reveal a lot about user interests and behavior. These works rely on the semantics of the installed apps and show that various user traits could be learnt automatically using off-the-shelf machine-learning techniques. In this work, we focus on the re-identifiability issue and thoroughly study the unicity of smartphone apps on a dataset containing 54,893 Android users collected over a period of 7 months. Our study finds that any 4 apps installed by a user are enough (more than 95% times) for the re-identification of the user in our dataset. As the complete list of installed apps is unique for 99% of the users in our dataset, it can be easily used to track/profile the users by a service such as Twitter that has access to the whole list of installed apps of users. As our analyzed dataset is small as compared to the total population of Android users, we also study how unicity would vary with larger datasets. This work emphasizes the need of better privacy guards against collection, use and release of the list of installed apps.

6.4. Data anonymization

Participants: Claude Castelluccia, Gergely Acs.

Set-valued dataset contains different types of items/values per individual, for example, visited locations, purchased goods, watched movies, or search queries. As it is relatively easy to re-identify individuals in such datasets, their release poses significant privacy threats. Hence, organizations aiming to share such datasets must adhere to personal data regulations. In order to get rid of these regulations and also to benefit from sharing, these datasets should be anonymized before their release. In this paper, we revisit the problem of anonymizing set-valued data. We argue that anonymization techniques targeting traditional k^m-anonymity model, which limits the adversarial background knowledge to at most m items per individual, are impractical for large real-world datasets. Hence, we propose in [25] a probabilistic relaxation of k^m-anonymity and present an anonymization technique to achieve it. This relaxation also improves the utility of the anonymized data. We also demonstrate the effectiveness of our scalable anonymization technique on a real-world location dataset consisting of more than 4 million subscribers of a large European telecom operator. We believe that our technique can be very appealing for practitioners willing to share such large datasets.

6.5. Wi-Fi and privacy

Participants: Jagdish Achara, Mathieu Cunche, Vincent Roca, Celestin Matte.

- **Geolocation spoofing attack** Our work at WiSec 2015 [17] shows how it is possible to manipulate the geolocation information of a single device and how to exploit this information as a side channel to identify the owner of the device on geottaged platforms such as social networks.
- **Extraction of sementical information from Wi-Fi network identifiers** Methods based on text similarity metrics can be used to infer user's interests based on the list of their preferred networks. We present in [23] a method identifying the physical entity (shop, restaurant, company ...) associated to Wi-Fi networks identifiers (SSID).

6.6. Formal and legal issues of privacy

Participants: Thibaud Antignac, Daniel Le Metayer.

- **Privacy by design** Privacy by design will become a legal obligation in the European Community when the Data Protection Regulation eventually gets adopted. However, taking into account privacy requirements in the design of a system is a challenging task. We have proposed an approach based on the specification of privacy architectures and illustrated our formal framework through several case studies. In collaboration with Morpho, we have applied it in the context of biometrics systems. The choice of particular techniques and the role of the components (central server, secure module, terminal, smart card, etc.) in the architecture have a strong impact on the privacy guarantees provided by a biometric system. However, 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. We have shown that a general framework for the definition of privacy architectures can be used to specify these options and to reason about them in a formal way. In 2015 the results on biometrics were presented at the conferences FM2015 [16] and ISC 2015 [15] (best paper award) and the general approach itself has led to Thibaud Antignac's PhD defense.
- **Verification of privacy properties**

  Electric vehicles are an up-and-coming technology that provides significant environmental benefits. A major challenge of these vehicles is their somewhat limited range, requiring the deployment of many charging stations. To effectively deliver electricity to vehicles and guarantee payment, a protocol was developed as part of the ISO 15118 standardization effort. A privacy-preserving variant of this protocol, POPCORN, has been proposed in recent work, claiming to provide significant privacy for the user, while maintaining functionality. We have proposed an approach for the verification of privacy properties of the protocol. We have provided a formal model of the expected privacy properties in the applied Pi-Calculus and used ProVerif to check them. We have identified weaknesses in the protocol in [11] and suggest improvements to address them.
- **Control over personal data**

More than ever the notion of control plays a pivotal and pervasive role in the discourses of privacy and data protection. Privacy scholarship and regulators propose to increase individual control over personal information as the ultimate prescriptive solution to tackle the issues raised by emergent data processing technologies. Conceived as the claim of individuals to determine for themselves when, how, and to what extent information about them is communicated to others, the notion of control is not new. It is often considered as the unique means of empowerment of the data subject. The mechanisms of this empowerment remain however surprisingly vague and understudied. What does it really mean to be in control of one's data in the context of contemporary socio-technical environments and practices? What are the characteristics, purposes and potential limits of such control and how can we guarantee data subjects effective control over their own data? We have carried out an interdisciplinary review of the concept of control to explore such questions in the fields of law and computer science and suggested conditions for the effective application of this concept (see [5]).

- **Accountability** The use of body-worn cameras by police forces around the world is spreading quickly. The resulting mobile and ubiquitous surveillance is often marketed as an instrument for accountability and an effective way of reducing violence. It also involves remarkable potential for intrusion into the privacy of both individuals and police agents. We have studied in [4] the deployment of police body-worn cameras in five countries, investigated their suitability as an accountability tool given the associated privacy threats, and analyzed the societal impact of their deployment as well as the risk of function creep.

6.7. Buidling blocks

Participant: Marine Minier.

- **Symmetric cryptography** During this year, a fruitful work in collaboration with Céline Blondeau from University of AAlto has appeared in FSE 2015 [8] concerning the equivalence between the key recovery parts of the three attacks (Zero-Correlation, impossible and integral) using the matrix method.

  With Thierry Berger, Julien Francq and also Gaël Thomas, we have proposed 2 new lightweight block ciphers : Lilliput and CubeCipher.

  Concerning symmetric cryptography, we obtain some results in both sides: on the one hand, we provide 2 new families of lightweight block ciphers: CubeCipher familiy and Lilliput; on the other hand, we work on the matrix method to simplify the representation of some attacks such as zero-correlation attack, impossible and integral attacks.

  We also published the extended version of our Secrypt 2013 paper in the journal Security and Communication Networks [2] concerning the performances on a dedicated platform.

- **Passwords Cracking** Passwords are widely used for user authentication, and will likely remain in use in the foreseeable future, despite several weaknesses. One important weakness is that human-generated passwords are far from being random, which makes them susceptible to guessing attacks. Understanding the adversaries' capabilities for guessing attacks is a fundamental necessity for estimating their impact and advising countermeasures. We develop OMEN [9], a new Markov model-based password cracker that extends ideas proposed by Narayanan and Shmatikov (CCS 2005). The main novelty of our tool is that it generates password candidates according to their occurrence probabilities, i.e., it outputs most likely passwords first. As shown by our extensive experiments, OMEN significantly improves guessing speed over existing proposals. In particular, we compare the performance of OMEN with the Markov mode of John the Ripper, which implements the password indexing function by Narayanan and Shmatikov. OMEN guesses more than 40% of passwords correctly with the first 90 million guesses, while JtR-Markov (for T = 1 billion) needs at least eight times as many guesses to reach the same goal, and OMEN guesses more than 80% of passwords correctly at 10 billion guesses, more than all probabilistic password crackers we compared against.

- **Time-memory trade-off** Cryptanalytic time-memory trade-offs (TMTO) are well-known tools available in any security expert toolbox. They have been used to break ciphers such as A5/1, but their efficiency to crack passwords made them even more popular in the security community. While symmetric keys are generated randomly according to a uniform distribution, passwords chosen by users are in practice far from being random, as confirmed by recent leakage of databases. Unfortunately, the technique used to build TMTOs is not appropriate to deal with non-uniform distributions. In [6], we introduce an efficient construction that consists in partitioning the search set into subsets of close densities, and a strategy to explore the TMTOs associated to the subsets based on an interleaved traversal. This approach results in a significant improvement compared to currently used TMTOs. We experimented our approach on a classical problem, namely cracking 7-character NTLM Hash passwords using an alphabet with 34 special characters, which resulted in a 16 × speedup over rainbow tables, which are considered as the most efficient variant of time-memory trade-offs.

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. XDATA

Title: XDATA.

Type: FUI.

Duration: April 2013 - April 2015.

Coordinator: Data Publica

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

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

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

8.1.1.2. 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.

8.1.2.2. BLOC

Title: Analysis of block ciphers dedicated to constrained environments.

Type: ANR.

Duration: October 2013 - September 2015.

Coordinator: INSA-Lyon (France).

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

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

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

8.1.2.3. 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.

8.1.2.4. CAPPRIS

Title: CAPPRIS

Type: Inria Project Lab

Duration: January 2011 - 2014.

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.

8.2. European Initiatives

8.2.1. FP7 & H2020 Projects

8.2.1.1. PRIPARE

Title: PReparing Industry to Privacy-by-design by supporting its Application in REsearch

Programm: FP7

Duration: October 2013 - September 2015

Coordinator: France-Trialog

Inria contact: Daniel Le Métayer

The mission of PRIPARE is twofold: facilitate the application of a privacy and security-by-design methodology that will contribute to the advent of unhindered usage of Internet against disruptions, censorship and surveillance, support its practice by the ICT research community to prepare for industry practice; foster risk management culture through educational material targeted to a diversity of stakeholders. To this end PRIPARE will specify a privacy and security-by-design software and systems engineering methodology, using the combined expertise of the research community and taking into account multiple viewpoints (advocacy, legal, engineering, business), prepare best practices material (guidelines, patterns, success stories) for the development and implementation of products and services of ICT-based systems and use-cases in the area of cloud computing, mobile services and the management of cyber incidents, support FP7 and Horizon 2020 research projects through training workshops and practical support in applying PRIPARE best practices in their environment. It also provides educational material on approaches for risk management of privacy and create awareness on the need for risk management culture among users. Material consistent with PRIPARE methodology will be structured in a modular way in order to fit to different targets (policy makers, users, ICT students and professional). Identify gaps and provide recommendations on privacy and security-by-design practices, support of unhindered usage of Internet and on the creation of a risk management culture. A research agenda will be proposed. PRIPARE consists of a consortium of 11 partners with strong links with the privacy community (data protection authorities/policy makers, privacy advocacy organisations, technology, engineering). In order to prepare for the longer term adoption by the industry, a representative advisory board will be set up. The support action duration is 24 months.

8.2.2. Collaborations in European Programs, except FP7 & H2020

8.2.2.1. 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.

8.3. Regional Initiatives

8.3.1. Privamov'

Title: Privamov'

Type: Labex IMU.

Duration: September 2013 - 2015.

Coordinator: LIRIS.

Others partners: EVS-ITUS, Inria Urbanets.

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

8.3.2. SCCyPhy

Title: SCCyPhy

Type: Labex Persyval.

Duration: September 2013 - 2015.

Coordinator: Institut Fourier.

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

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

8.3.3. 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).

9. Dissemination

9.1. Promoting Scientific Activities

9.1.1. Scientific events organisation

9.1.1.1. Member of the organizing committee

Cédric Lauradoux : GREHACK 2015.

Daniel Le Metayer : La vie privee à travers les cultures: divergences et convergences dans un monde globalisé, Rencontres Jacques Cartier, Lyon, 31 November 2015.

9.1.2. Scientific events selection

9.1.2.1. Chair of conference program committee

Cédric Lauradoux : GREHACK 2015.

9.1.2.2. Member of the conference program committee

Mathieu Cunche : Trustcom 2015, ICISSP 2015, HotPlanet 2015.

Cédric Lauradoux : Wisec 2015.

Daniel Le Métayer : IWPE 2015, WETICE 2015.

Claude Castelluccia : WISEC 2015, PETs'15.

Marine Minier : WCC 2015.

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 : Cédric Lauradoux, Advanced Topics in Security, 20h, L3, ENSIMAG, France.

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

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

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

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

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

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

9.2.2. Supervision

PhD defended : Gael Thomas, Algebraic Automata in Symetric Cryptography, Marine Minier.

PhD defended : Lukasz Olejnik, Internet Tracking and Profiling, Claude Castelluccia.

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

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

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

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

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

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): Khaoula Dhifallah, Resiliency properties of protocols for WSNs (02/2015 - 07/2015)

Intern (M2): Saikou Fall, Packet Too Big or Too Small ? The PTB-PTS ICMP-based attack against IPsec gateways and tunneling mechanisms (05/2015 - 09/2015)

Intern (M2): Aude Tessier, Etude comparee technico-juridique des lois dites de renseignement (02/2014- 09/2014)

Intern (M2): Leo Letaro, Détection des altération de pages Web (02/2015-07/2015)

Intern (M1): Mathieu Thiery, NeuroAuth-Authenticating People from their Implicit Memory (03/2015 - 09/2015)

Intern (M1): Lenka Kunikova, An efficient implementation of a generic two-party secure computation protocol in the UC framework (02/2015 - 06/2014)

Intern (M1): Jose Paul Dominguez, Tarantula: individual targeting for passphrase attacks (02/2015 - 06/2014)

Intern (M1): Michael Omer, Security and QR-codes (02/2015 - 06/2014)

Intern (M1): Quentin Ricard, Algorithmic complexity attacks against sorting algorithms (02/2015 - 08/2014)

Intern (M1): Jonathan Tournier, Evaluating Forensics Tools (02/2015 - 06/2014)

9.2.3. Juries

PhD : Lukasz Olejnik, Internet Tracking and Profiling, Université de Grenoble, Grenoble, 30/01/2015, Claude Castelluccia.

HDR : Benoît Parrein, Le code à effacement Mojette: applications dans les réseaux et dans le Cloud, Université de Nantes, Nantes, 22/06/2015, Vincent Roca.

PhD : Regina Melo Marin, Enhancing Privacy Protection in Social Network Systems Through Decentralization and Policy Conflict Management, Université de Rennes, Rennes, 07/09/2015, Daniel Le Métayer.

PhD : Paul Mazenc-Lajoie, Réputation et respect de la vie privée dans les réseaux dynamiques auto-organisés, Université de Rennes, Rennes, 25/09/2015, Daniel Le Métayer.

PhD : Koen Decroix,Model-Based Analysis of Privacy in Electronic Services, Université de Leuven, Leuven, 21/10/2015, Daniel Le Métayer.

PhD : Thibaud Antignac, Méthodes formelles pour le respect de la vie privée par construction, INSA Lyon, Lyon, 25/02/2015, Daniel Le Métayer.

PhD : Joëlle Roué, Analyse de sécurité des chiffrements par bloc, 14/10/2015, Université Pierre et Marie Curie, Paris, Marine Minier.

9.3. Popularization

Article of C.Castelluccia and D.Le Métayer in le Monde, Oui, la loi sur le renseignement prépare bien une surveillance de masse, 09/06/2015.

Article of C.Castelluccia and D.Le Métayer in Pour La Science, Renseignement : le traitement massif de données est aussi dangereux qu'inefficace, 11/06/2015.

Interview of C.Castelluccia and D.Le Métayer in le Monde, Des dizaines de milliers de personnes vont être suspectées à tort, 06/05/2015.

Article of C.Castelluccia and D.Le Métayer in La Recherche, Les failles de la loi sur le renseignement, 11/2015.

Interview of V. Roca on France Culture in Les Nouvelles Vagues, Privacy leaks in smartphones, 10/2015

Article of V. Roca in Interstice, Quand nos smartphones sont espionnés, https://interstices.info/jcms/p_83464/quand-nos-smartphones-sont-espionnes, 09/2015.

Representation of Privatics by V. Roca at Journée numérique au Sénat, 11/02/2015.

Representation of Privatics by M. Cunche at Journée numérique au Sénat, 11/02/2015.

Seminar of C. Lauradoux at the security seminar LORIA, Google Safe Browsing: Security and Privacy, 18/11/2015.

Seminar of C. Lauradoux at GRACE seminar (Inria Saclay), Membership Tests in Security, 18/11/2015.

Seminar CCA of C. Lauradoux, Exploitations concrètes des mauvaises utilisations des fonctions de hachage, 12/06/2015.

Workshop of C. Lauradoux at GREHACK 2015, Sécurité des drones.

Seminar of Marine Miner at LIMOS seminar, CUBE Cipher: Une Famille de Chiffrement par Blocs Quasi-Involutifs et Facile à Masquer, 01/10/2015.

Seminar of Marine Miner at XLIM seminar, CUBE Cipher: Une Famille de Chiffrement par Blocs Quasi-Involutifs et Facile à Masquer, 10/02/2015.

Seminar of Marine Miner at Rennes, Some solutions for security of WSNs, 11/2015.

10. Bibliography

Publications of the year

Articles in International Peer-Reviewed Journals

[1] P. Brunisholz, O. Erdene-Ochir, M. Abdallah, K. QARAQE, M. Minier, F. Valois. *Network Coding versus Replication Based Resilient Techniques to Mitigate Insider Attacks for Smart Metering*, in "International Journal of Distributed Sensor Networks", 2015, vol. 2015, n^o^ Article ID 737269, 11 p. [*DOI :* 10.1155/2015/737269], https://hal.archives-ouvertes.fr/hal-01199787

[2] M. Cazorla, S. Gourgeon, K. Marquet, M. Minier. *Survey and benchmark of lightweight block ciphers for MSP430 16-bit microcontroller*, in "Security and communication networks", 2015, 16 p. [*DOI :* 10.1002/sec.1281], https://hal.archives-ouvertes.fr/hal-01199786

[3] G. Gössler, D. Le Métayer. *A general framework for blaming in component-based systems*, in "Science of Computer Programming", 2015, vol. 113, Part 3 [*DOI :* 10.1016/j.scico.2015.06.010], https://hal.inria.fr/hal-01211484

[4] D. Le Métayer, D. Butin, F. Coudert. *Body-worn cameras for police accountability: Opportunities and risks*, in "Computer Law and Security Review", December 2015, vol. 31, n^o^ 6, 13 p. , https://hal.inria.fr/hal-01247051

[5] D. Le Métayer, L. Christophe. *Control over personal data: true remedy or fairy tale ?*, in "Scripted. A Journal of Law, Technology and Society", June 2015, vol. 12, n^o^ 1, https://hal.inria.fr/hal-01247056

International Conferences with Proceedings

[6] G. Avoine, X. Carpent, C. Lauradoux. *Interleaving Cryptanalytic Time-memory Trade-offs on Non-Uniform Distributions*, in "European Symposium on Research in Computer Security - ESORICS 2015", Vienna, Austria, LNCS, September 2015, vol. 9326 et 9327, https://hal.inria.fr/hal-01199151

[7] T. P. Berger, J. Francq, M. Minier. *CUBE Cipher: A Family of Quasi-Involutive Block Ciphers Easy to Mask*, in "Codes, Cryptology, and Information Security - First International Conference, C2SI 2015, May 2 6-28, Proceedings - In Honor of Thierry Berger", Rabat, Morocco, S. E. Hajji, A. Nitaj, C. Carlet, E. M. Souidi (editors), Lecture Notes in Computer Science, Springer, 2015, vol. 9084, pp. 89–105, https://hal.archives-ouvertes.fr/hal-01199224

[8] C. BLONDEAU, M. MINIER. *Analysis of Impossible, Integral and Zero-Correlation Attacks on Type-II Generalized Feistel Networks Using the Matrix Method*, in "Fast Software Encryption - 22nd International Workshop, FSE 2015, March 8-11, Revised Selected Papers", Istanbul, Turkey, G. LEANDER (editor), Lecture Notes in Computer Science, Springer, 2015, vol. 9054, pp. 92–113 [*DOI :* 10.1007/978-3-662-48116-5_5], https://hal.archives-ouvertes.fr/hal-01199223

[9] M. DUERMUTH, F. ANGELSTORF, C. CASTELLUCCIA, D. PERITO, A. CHAABANE. *OMEN: Faster Password Guessing Using an Ordered Markov Enumerator*, in "International Symposium on Engineering Secure Software and Systems", milan, Italy, March 2015, https://hal.archives-ouvertes.fr/hal-01112124

[10] O. ERDENE-OCHIR, M. ABDALLAH, K. QARAQE, M. MINIER, F. VALOIS. *A theoretical framework of resilience: Biased random walk routing against insider attacks*, in "WCNC 2015 - IEEE Wireless Communications and Networking Conference", New Orleans, United States, IEEE, March 2015, pp. 1602–1607, https://hal.archives-ouvertes.fr/hal-01199222

[11] M. FAZOUANE, H. KOPP, R. VAN DER HEIJDEN, D. LE MÉTAYER, F. KARGL. *Formal verification of privacy properties in electrical vehicle charging*, in "International Symposium on Engineering Secure Software and Systems (ESSOS15)", Milan, Italy, March 2015, https://hal.inria.fr/hal-01089925

[12] T. GERBET, A. KUMAR, C. LAURADOUX. *The Power of Evil Choices in Bloom Filters*, in "Annual IEEE/IFIP International Conference on Dependable Systems and Networks - DSN 2015", Rio De Janeiro, Brazil, June 2015, https://hal.inria.fr/hal-01199150

[13] A. KUMAR, C. LAURADOUX. *A Survey of Alerting Websites: Risks and Solutions*, in "IFIP SEC", Hamburg, Germany, Chapter ICT Systems Security and Privacy Protection of the series IFIP Advances in Information and Communication Technology, May 2015, vol. 455, pp. 126-141 [*DOI :* 10.1007/978-3-319-18467-8_9], https://hal.archives-ouvertes.fr/hal-01199703

[14] D. LE MÉTAYER, D. BUTIN, V.-T. TA. *Formal Accountability for Biometric Surveillance: A Case Study*, in "Annual Privacy Forum (APF 2015)", Luxembourg, Luxembourg, Springer , October 2015, https://hal.inria.fr/hal-01247119

[15] *Best Paper*
D. LE MÉTAYER, H. CHABANNE, L. ROCH, J. BRINGER. *Reasoning about privacy properties of biometric system architectures in the presence of information leakage*, in "Information Security Conference (ISC 2015)", Trondheim, Norway, Springer , November 2015, https://hal.inria.fr/hal-01247064.

[16] D. LE MÉTAYER, L. ROCH, J. BRINGER, H. CHABANNE. *Privacy by design in practice: reasoning about privacy properties of biometric system architectures*, in "20th int. Symposium on Formal Methods (FM 2015)", Oslo, Norway, Springer , June 2015, n^{o} 9109, https://hal.inria.fr/hal-01247110

[17] C. MATTE, J. P. ACHARA, M. CUNCHE. *Short: Device-to-Identity Linking Attack Using Targeted Wi-Fi Geolocation Spoofing*, in "ACM WiSec 2015", New York, United States, June 2015 [*DOI :* 10.1145/2766498.2766521], https://hal.inria.fr/hal-01176842

[18] F. MATTOUSSI, V. ROCA, B. SAYADI. *Impacts of the Packet Scheduling on the Performance of Erasure Codes: Methodology and Application to GLDPC-Staircase Codes*, in "IEEE European Conference on Net-

works and Communications (EUCNC'15)", Paris, France, IEEE (editor), Nicolas Demassieux and Mário Campolargo, EUCNC 2015 Chairs, June 2015, https://hal.inria.fr/hal-01144380

[19] N. Notario, A. Crespo, Y.-S. Martín, J. del Alamo, D. Le Métayer, T. Antignac, A. Kung, I. Kroener, W. David. *PRIPARE: Integrating Privacy Best Practices into a Privacy Engineering Methodology*, in "International Workshop on Privacy Engineering (IWPE 2015)", San Jose, CA, United States, IEEE, May 2015, 8 p. [*DOI :* 10.1109/SPW.2015.22], https://hal.inria.fr/hal-01244588

[20] V. Primault, S. Ben Mokhtar, C. Lauradoux, L. Brunie. *Time Distortion Anonymization for the Publication of Mobility Data with High Utility*, in "14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications", Helsinki, Finland, August 2015, https://hal.archives-ouvertes.fr/hal-01170060

[21] P. Raveneau, R. Stanica, M. Fiore, S. Uppoor, M. Cunche, H. Rivano, Z. Smoreda. *Urban-scale Cellular Offloading through Wi-Fi Access Points: a Measurement-based Case Study*, in "RTSI 2015 - 1st International Forum on Research and Technologies for Society and Industry", Turin, Italy, September 2015, https://hal.archives-ouvertes.fr/hal-01201719

[22] P. Rouveyrol, P. Raveneau, M. Cunche. *Large Scale Wi-Fi tracking using a Botnet of Wireless Routers*, in "SAT 2015 - Workshop on Surveillance & Technology", Philadelphia, United States, June 2015, https://hal.inria.fr/hal-01151446

[23] S. Seneviratne, F. Jiang, M. Cunche, A. Seneviratne. *SSIDs in the Wild: Extracting Semantic Information from WiFi SSIDs*, in "The 40th IEEE Conference on Local Computer Networks (LCN)", Clearwater Beach, Florida, United States, October 2015, https://hal.inria.fr/hal-01181254

Conferences without Proceedings

[24] J. P. Achara, G. Acs, C. Castelluccia. *On the Unicity of Smartphone Applications*, in "ACM CCS Workshop on Privacy in Electronic Society (WPES)", Denver, Colorado, USA, France, October 2015, Published at ACM CCS Workshop on Privacy in Electronic Society (WPES) 2015, https://hal.inria.fr/hal-01181040

[25] A. Gergely, J. P. Achara, C. Castelluccia. *Probabilistic k^m-anonymity*, in "IEEE Internation Conference on Big Data (BigData) 2015", Santa Clara, United States, October 2015, https://hal.inria.fr/hal-01205533

[26] V. Roca, L. Jacquin, S. Fall, J.-L. Roch. *New Results for the PTB-PTS Attack on Tunneling Gateways*, in "GreHack 2015", Grenoble, France, Cédric Lauradoux, Florent Autréau, November 2015, https://hal.inria.fr/hal-01245629

Scientific Books (or Scientific Book chapters)

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

Research Reports

[28] T. Antignac, D. Le Métayer. *Trust Driven Strategies for Privacy by Design (Long Version)*, Inria, February 2015, n^{o} RR-8676, 21 p. , https://hal.inria.fr/hal-01112856

[29] T. GERBET, A. KUMAR, C. LAURADOUX. *A Privacy Analysis of Google and Yandex Safe Browsing*, Inria, February 2015, n^o RR-8686, https://hal.inria.fr/hal-01120186

[30] C. LAZARO, D. LE MÉTAYER. *The control over personal data: True remedy or fairy tale ?*, Inria - Research Centre Grenoble – Rhône-Alpes ; Inria, April 2015, n^o RR-8681, 25 p. , https://hal.inria.fr/hal-01141461

Scientific Popularization

[31] C. CASTELLUCCIA, D. LE MÉTAYER. *Les failles de la loi sur le renseignement*, in "La Recherche", November 2015, n^o 505, https://hal.inria.fr/hal-01247131

[32] C. CASTELLUCCIA, D. LE MÉTAYER. *Renseignement : le traitement massif de données est aussi dangereux qu'inefficace*, in "Pour la science", July 2015, https://hal.inria.fr/hal-01247129

[33] D. LE MÉTAYER. *Analyser et prévenir les risques d'atteinte à la vie privée*, in "Assemblée Nationale - Rapport d'information de la Commission de réflexion et de propositions sur le droit et les libertés à l'âge du numérique", C. PAUL, C. FÉRAL-SCHUHL (editors), October 2015, https://hal.inria.fr/hal-01247124

[34] D. LE MÉTAYER, C. CASTELLUCCIA, G. ACS. *Anonymous versus personal data: from a binary view to a rigorous risk-based approach*, December 2015, Contribution to the European Parliament High-level conference co-organised by the LIBE Committee and the STOA Panel, Protecting online privacy by enhancing IT security and strengthening EU IT capabilities, https://hal.inria.fr/hal-01247125

Other Publications

[35] C. BLONDEAU, M. MINIER. *Analysis of Impossible, Integral and Zero-Correlation Attacks on Type-II Generalized Feistel Networks using the Matrix Method*, 2015, 141 p. , http://eprint.iacr.org/2015/141 , https://hal.archives-ouvertes.fr/hal-01199221

[36] C. CASTELLUCCIA, M. DUERMUTH, M. GOLLA, F. IMAMOGLU. *Towards Implicit Visual Memory-Based Authentication*, January 2015, working paper or preprint, https://hal.inria.fr/hal-01109765

[37] J. DETCHART, E. LOCHIN, J. LACAN, V. ROCA. *Tetrys, an On-the-Fly Network Coding protocol*, July 2015, Working document of the NWCRG (Network Coding Research Group) group of IRTF (Internet Research Task Force), https://hal.inria.fr/hal-01089745

[38] L. LE TARO. *New Methods for Targeted Advertising and User Tracking on the Internet*, Universite Claude Bernard Lyon 1 ; INSA de Lyon, June 2015, 29 p. , https://hal.inria.fr/hal-01167493

[39] M.-J. MONTPETIT, V. ROCA, J. DETCHART. *Dynamic Network Coding*, March 2015, Working document of the NWCRG (Network Coding Research Group) group of IRTF (Internet Research Task Force), https://hal.inria.fr/hal-01132183

[40] J. PARRA-ARNAU, C. CASTELLUCCIA. *Dataveillance and the False-Positive Paradox*, May 2015, working paper or preprint, https://hal.archives-ouvertes.fr/hal-01157921

[41] 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

[42] V. ROCA. *FECFRAMEv2: Adding Sliding Encoding Window Capabilities to the FEC Framework: Problem Position*, June 2015, 18 p. , Working document of the NWCRG (Network Coding Research Group) group of IRTF (Internet Research Task Force), https://hal.inria.fr/hal-01141470