IN PARTNERSHIP WITH:
Institut national des sciences appliquées de Lyon

Activity Report 2014

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

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

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

1. Members

Research Scientists

Claude Castelluccia [Team leader, Senior Researcher, HdR]
Mohamed Ali Kaafar [Inria, Researcher]
Cédric Lauradoux [Inria, Researcher]
Daniel Le Métayer [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]
James-Douglass Lefruit [Inria, until Oct 2014]
Pierre Rouveyrol [Inria, from Oct 2014 until May 2015]

PhD Students

Jagdish Achara [Inria]
Thibaud Antignac [Inria]
Abdelberi Chaabane [Inria, ANR, until Feb 2014]
Levent Demir [CIFRE, from Jul 2014]
Jessye Dos Santos [CEA]
Amrit Kumar [Univ. Grenoble I]
Célestin Matte [INSA Lyon, ARC7, from Oct 2014]
Ferdaouss Mattoussi [Inria, until Jan 2014]
Lukasz Olejnik [Inria, until Jan 2015]
Minh-Dung Tran [Univ. Grenoble I, until Sep 2014]

Post-Doctoral Fellows

Denis Butin [Inria, until Jul 2014, granted by FP7 PARIS project]
Christophe Lazaro [Inria, until Sep 2014, granted by FP7 PARIS project]
Javier Parra Arnau [Inria, from Oct 2014]
Vinh Thong Ta [Inria, from Feb 2014]

Administrative Assistant

Helen Pouchot [Inria]

Others

Kevin Chaumont [Inria, Intern (IUT), from Apr 2014 until Jun 2014]
Marouane Fazouane [Inria, Intern (M2), until Sep 2014]
Emmanuel Perrier [Inria, Intern (M2), from Mar 2014 until Jul 2014]

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.

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

3.2. Domain 2: Big Data and Privacy

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

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

Privacy-Preserving Data Collection: In the untrusted model, individuals do not trust their data publisher. For example, websites commonly use third party web analytics services, such as Google Analytics to obtain aggregate traffic statistics such as most visited pages, visitors' countries, etc. Similarly, other applications, such as smart metering or targeted advertising applications, are also tracking users in order to derive aggregated information about a particular class of users. Unfortunately, to obtain this aggregate information, services need to track users, resulting in a violation of user privacy. One of our goals is to develop Privacy-Preserving Data Collection solutions. We propose to study whether it is possible to provide efficient collection/aggregation solutions without tracking users, i.e. without getting or learning individual contributions.

4. New Software and Platforms

4.1. Mobilitics

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

In the presence of a wide range of different smartphones available in terms of operating systems and hardware architecture, Mobilitics project focuses actually its study on the two 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.

A Mobilitics prototype for iOS has been developed since early 2012. A Mobilitics prototype for Android has been developped since mid-2013, running on Galaxy Nexus smartphones. In parallel an analysis tool has been developped, capable of analyzing the databases containing the raw data of both Mobile Operating Systems.

A first live experiment has been conducted by CNIL with the Mobilitics sofwtare for IOS with the help of volunteers equipped with iphones in September 2012-January 2013. As a result, some visualization tools have been developed for the data collected in order to showcase private data leakage by the apps which the participants of the experiment have used. A press conference has been held by CNIL and Inria in Paris in April 2013 and several Mobilitics results have been published in French newspapers (see Section 8.3).

A second live experiment has been conducted by CNIL with the Mobilitics software for Android, with the help of volunteers equipped with Galaxy Nexus smartphones, in June-September 2014. A press conference has been held by CNIL and Inria in December 2014, and several results have been published in French newspapers (see Section 8.3).

4.2. Omen+

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.

The actual efficiency of that implementation in the cracking of passwords will be tested in the coming days. The processing of the personal information will be implemented before the end of January. The hardest part of that side of Omen+ will be the collection and classification of the information for a particular target.

4.3. OpenFEC

OpenFEC (http://openfec.org) is an open-source C-language implementation of several Application-Level Forward Erasure Correction (AL-FEC) codecs, namely: 2D-parity, Reed-Solomon (RFC 5510, http://tools.ietf.org/html/rfc5510) and LDPC-Staircase (RFC 5170, http://tools.ietf.org/html/rfc5170) 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.

A commercial, highly optimized version of OpenFEC is available, along with an implementation of the FLUTE (RFC 6726, http://tools.ietf.org/html/rfc6726) large scale content delivery protocol, and both softwares are currently commercialized by the Expway (http://expway.com) French SME. These softwares have been deployed in many places throughout the world (for instance there were more than 1.5 millions of terminals in Japan implementing the ISDB-Tmm standard, powered by our FLUTE/LDPC-Staircase softwares, in Q3-2013).

Thanks to the success of the industrial transfer of the OpenFEC and FLUTE softwares to Expway, Vincent Roca has been awarded the third FIEEC (Federation des Industries Electriques, Electroniques et Communications) applied research prize in October 2014.

5. New Results

5.1. Highlights of the Year

Vincent Roca was awarded the 3rd Applied Research price of the Fédération des Industries Electriques, Electroniques et Communications (FIEEC), for his transfer activities to the Expway French SME, Lyon, October 8th, 2014.

The team got two major contributions:

- *A Case Study: Privacy Preserving Release of Spatio-temporal Density in Paris* was published by Gergely Acs and Castelluccia at KDD 2014.
- *Censorship in the Wild: Analyzing Internet Filtering in Syria* was published by Chaabane Abdelberi, Mathieu Cunche,and Mohamed Ali Kaafar at IMC 2014.

5.2. Filtering and blocking the Internet

Participants: Mohamed Ali Kaafar, Abdelberi Chaabane, Mathieu Cunche, Cédric Lauradoux, Amrit Kumar.

- **Censorship**

  Based on 600GB leaked logs from appliances used to filter Internet traffic in Syria, we performed an analysis of the Syrian censorship apparatus. This study have been published in ACM Internet Measurement Conference [7].

  We found that the Internet traffic in Syria was filtered in several ways using IP addresses, domain names and keywords. Content sharing, instant messaging and proxy technologies were heavily censored. Some social media such as badoo.com were fully censored, but others such as Facebook are only censored for specific political and religious pages. We also found evidences of successful usage of censorship-circumvention techniques such as Tor and VPN. We also found that P2P file-sharing and Google cache were used to escape censorship blockage.

  While our work might help organizations on both sides of the censorship line, we believe the presented results can help understand the underlying technologies, policies and can inform the design of tools designed to evade the censorship.
- **Attacking filters** Many major Internet companies use probabilistic techniques to filter the users requests or to prevent malicious attacks. In our work [35], [34], we show how they can be polluted/saturated using pre-image attacks and how it increases the false-positive probability. Then, we show how to forge false-positives to mount attacks. In the adversarial settings, we have the liberty to assume that the inputs to the filter are non uniformly distributed. This observation leads to our second contribution: we compute the worst case false-positive probability and obtain new equations for Bloom filter parameters. To support our contributions, we provide four attacks on software applications based on Bloom filter: Bloom-enabled SCRAPY web spider, BITLY DABLOOMS spam filter, SQUID web cache and GOOGLE Safe Browsing. Our attacks retain some form of DoS. They are all based on the forgery of Uniform Resource Locators (URLs) matching certain pre-image or second pre-image property. The impact of our attack ranges from denial-of-service to massively distributed denial-of-service with reflection.

5.3. Selling Off Privacy at Auction

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

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

In [13], we characterize and quantify the potential user web history leakage from ad exchanges to bidders in RTB as a result of exchanging user data. We also discuss and quantify the extent to which companies can potentially collude to increase their tracked user profiles using CM. In addition, we leverage a design characteristic of RTB to observe the winning price of each RTB auction. By analyzing these prices, we show how advertisers evaluate the value of user privacy. This work (titled Selling Off Privacy at Auction) will be presented in NDSS 2014, San Diego, USA in February, 2014.

5.4. Data anonymization

Participants: Claude Castelluccia, Gergely Acs.

With billions of handsets in use worldwide, the quantity of mobility data is gigantic. When aggregated they can help understand complex processes, such as the spread viruses, and built better transportation systems, prevent traffic congestion. While the benefits provided by these datasets are indisputable, they unfortunately pose a considerable threat to location privacy. At KDD 2014 [9], we present a new anonymization scheme to release the spatio-temporal density of Paris, in France, i.e., the number of individuals in 989 different areas of the city released every hour over a whole week. The density is computed from a call-data-record (CDR) dataset, provided by the French Telecom operator Orange, containing the CDR of roughly 2 million users over one week. Our scheme is differential private, and hence, provides provable privacy guarantee to each individual in the dataset. Our main goal with this case study is to show that, even with large dimensional sensitive data, differential privacy can provide practical utility with meaningful privacy guarantee, if the anonymization scheme is carefully designed. This work is part of the national project XData (http://xdata.fr) that aims at combining large (anonymized) datasets provided by different service providers (telecom, electricity, water management, postal service, etc.).

5.5. Wi-Fi and privacy

Participants: Jagdish Achara, Mathieu Cunche, Vincent Roca.

In Android, installing an application implies accepting the permissions it requests, and these permissions are then enforced at runtime. In our WISEC 2014 paper [29], we focus on the privacy implications of the `ACCESS_WIFI_STATE` permission. For this purpose, we analyzed permissions of the 2700 most popular applications on Google Play and found that the `ACCESS_WIFI_STATE` permission is used by 41% of them. We then performed a static analysis of 998 applications requesting this permission and based on the results, chose 88 applications for dynamic analysis. Our analyses reveal that this permission is already used by some companies to collect user Personally Identifiable Information (PII). We also conducted an online survey to study users' perception of the privacy risks associated with this permission. This survey shows that users largely underestimate the privacy implications of this permission. As this permission is very common, most users are therefore potentially at risk.

5.6. Sensor security and privacy

Participant: Marine Minier.

Wireless sensor networks (WSNs) are composed of a large number of low-cost, low-power, and multi-functional sensor nodes that communicate at short distance through wireless links. They are usually deployed in an open and uncontrolled environment where attackers may be present. Due to the use of low-cost materials, hardware components are not tamper-resistant and an adversary could access to a sensor's internal state. With Ochirkhand Erdene-Ochir and Pierre Brunisholz, we continue to work on the notion of resiliency in WSNs [17], [31].

5.7. Buidling blocks

Participant: Marine Minier.

In the context of the BLOC project funded by the ANR, we continue to work on Extended Generalized Feistel Network and on new ligthweight block cipher design (see [30]). We hope to obtain results in this area at the beginning of 2015. With Christine Solnon and Julia Reboul, we work on the formalism of related-key and chosen-key attacks against symmetric key primitives using constraint programming (CP). This preliminary work was presented at the CP 2014 workshop ModRef 2014 in [42].

5.8. Formal and legal issues of privacy

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

- **Privacy Architectures: Reasoning About Data Minimization and Integrity** Privacy by design will become a legal obligation in the European Community if the Data Protection Regulation eventually gets adopted. However, taking into account privacy requirements in the design of a system is a challenging task. We present an approach based on the specification of privacy architectures at FM 2014 [12] and focus on a key aspect of privacy, data minimisation, and its tension with integrity requirements. We illustrate our formal framework through a smart metering case study.
- **Log Analysis for Data Protection Accountability**

  Accountability is increasingly recognized as a cornerstone of data protection, notably in European regulation, but the term is frequently used in a vague sense. For accountability to bring tangible benefits, the expected properties of personal data handling logs and the assumptions regarding the logging process must be defined with accuracy. At STM 2014 [10], we provide a formal framework for accountability and show the correctness of the log analysis with respect to abstract traces used to specify privacy policies. We also show that compliance with respect to data protection policies can be checked based on logs free of personal data, and describe the integration of our formal framework in a global accountability process.

6. Bilateral Contracts and Grants with Industry

6.1. Bilateral Contracts with Industry

6.1.1. XDATA

Title: XDATA.

Type: FUI.

Duration: April 2013 - April 2015.

Coordinator: Data Publica

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

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

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

6.1.2. 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.

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. Privamov’

Title: Privamov'

Type: Labex IMU.

Duration: September 2013 - 2015.

Coordinator: LIRIS.

Others partners: EVS-ITUS, Inria Urbanets.

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

7.1.2. SCCyPhy

Title: SCCyPhy

Type: Labex Persyval.

Duration: September 2013 - 2015.

Coordinator: Institut Fourier.

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

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

7.2. National Initiatives

7.2.1. FUI

7.2.1.1. XDATA

Title: XDATA.

Type: FUI.

Duration: April 2013 - April 2015.

Coordinator: Data Publica

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

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

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

7.2.2. ANR

7.2.2.1. 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.

7.2.2.2. 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.

7.2.2.3. pFlower

Title: Parallel Flow Recognition with Multi-Core Processor.

Type: ANR.

Duration: March 2011 - September 2014.

Coordinator: LISTIC Université de Savoie.

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

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

7.2.3. Other

7.2.3.1. MOBILITICS

Title: MOBILITICS

Type: joint project.

Duration: January 2012 - Ongoing.

Coordinator: CNIL.

Others partners: CNIL.

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

7.2.3.2. 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.

7.3. European Initiatives

7.3.1. FP7 Projects

7.3.1.1. PRIPARE

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

Type: COOPERATION (ICT).

Instrument: Support Action (SA).

Duration: October 2013 - September 2015.

Coordinator: Trialog (France).

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

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

7.3.1.2. PARIS

Title: Privacy preserving infrastructure for surveillance.

Type: COOPERATION (ICT).

Instrument: Specific Targeted Research Project (STREP).

Duration: January 2013 - December 2015.

Coordinator: Trialog (France).

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

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

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

7.3.2. Collaborations in European Programs, except FP7

7.3.2.1. FI-WARE

Title: Future Internet Ware.

Type: COOPERATION (ICT).

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

Instrument: Integrated Project (IP).

Duration: May 2011 - April 2014.

Coordinator: Telefonica. (Spain)

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

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

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

7.4. International Initiatives

7.4.1. Inria Associate Teams

7.4.1.1. CLOUDY

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

International Partner (Institution - Laboratory - Researcher):

University of California Berkeley (ÉTATS-UNIS)

Duration: 2012 - 2014

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

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

7.5. International Research Visitors

7.5.1. Visits of International Scientists

7.5.1.1. Explorer programme

Cunche Mathieu

Date: Oct 2014 - Nov 2014

Institution: NICTA (Australia)

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific events organisation

8.1.1.1. Member of the organizing and program committee

Claude Castelluccia : PETs'14, WISEC 2014, AFP 2014.

Mathieu Cunche : WISEC 2014 (publicity chair).

Cédric Lauradoux : Journées C2.

Daniel Lemetayer: CPDP 2014, AFP 2014.

Marine Minier : SAR-SSI 2014

Vincent Roca : SAR-SSI 2014.

8.1.2. Scientific events selection

8.1.2.1. Chair of conference program committee

Claude Castelluccia : WISEC 2014.

Marine Minier : CIS 2014.

8.1.2.2. Member of the conference program committee

Mathieu Cunche : WCNC 2014, APVP 2014, ICISSP 2015.

Cédric Lauradoux : Wisec 2014, SDTA 2014, CCSW 2014, Wisec 2015, Journées C2.

Vincent Roca : SPACOMM 2014, SNDS 2014

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

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

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

Undergraduate course : Marine Minier, Probabilities, 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.

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

Master : Cédric Lauradoux, Introduction to Cryptology, 30h, 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, 2h, M2, INSA-Lyon, France.

8.2.2. Supervision

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

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

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

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): Célestin Matte, Identification and Analysis of Privacy issues in the Wi-Fi technology (01/2014 - 07/2014)

Intern (M2): Pierre Brunisholz, OFDM decoding on a Virtex (02/2014- 09/2014)

Intern (M2): Emmanuel Poirier, Privacy preserving Wi-Fi tracking (02/2014-08/2014)

Intern (M1): Julia Reboul, Solving a Symmetric Key Cryptographic Problem with Constraint Programming (03/2014 - 08/2014)

Intern (M1): Pierre Rouverol, Study of Radio-Frequency tracking Technologies" (03/2014 - 08/2014)

8.2.3. Juries

HdR : Vincent Roca, Codes AL-FEC et protocoles de diffusion robuste de contenus : composants pour des services performants et passant à l'échelle, Toulouse, 19/06/2014, Claude Castelluccia.

HdR : Sebastien Gambs, Respect de la vie privée dans la société de l'information, Rennes, 23/06/2014, Daniel Le Métayer.

PhD : Minh-Dung Tran, Privacy challenges in Online Targeted Advertising, Université de Grenoble, 13/11/2014, Claude Castelluccia.

PhD : Gwenaelle DEJULYS, Analysis of entropy accumulators for cryptographic RNGs, Université de Grenoble, 18/12/2014, Cédric Lauradoux.

PhD : Lukasz Olejnik, Internet Tracking and Profiling, Université de Grenoble, 30/12/2015, Claude Castelluccia.

PhD : Abdelberi Chaabane, Threats against privacy on Internet: evaluation and solutions, Université de Grenoble, 22/05/2014, Claude Castelluccia.

PhD : Ferdaouss Mattoussi, Design and optimization of AL-FEC codes: the GLDPC-Staircase codes, Université de Grenoble, 13/02/2014, Vincent Roca and Claude Castelluccia.

PhD : Guillaume Smith, Enabling Private Real-Time Applications by Exploiting the Links Between Erasure Coding and Secret Sharing Mechanisms, Université de Toulouse, 04/12/2014, Vincent Roca.

PhD : Amira Bradai, Secured trust and reputation system : analysis of malicious behaviors and optimization, Université Pierre et Marie Curie, Paris 6, 29/09/2014, Vincent Roca.

PhD : Raphaël Jamet, Protocols and Models for the Security of Wireless Ad-Hoc Networks , Université de Grenoble, 03/11/2014, Marine Minier.

8.3. Popularization

Interview of Mathieu Cunche on Radio Canada in the chronicle of Janic Tremblay, 3rd February 2014.

Interview of Mathieu Cunche on Radio France Inter in "Journal de 18h", February 28th 2014.

Seminar of Mathieu Cunche " Je sais tout sur vous grâce au Wi-Fi! " Séminaire sur la Confiance Numérique at Clermont Ferrand, March 6th, 2014.

Interview of Mathieu Cunche on Radio France Info in "Tout comprendre" chronicle, March 18th, 2014.

Interview of Mathieu Cunche in Ouest-France news-paper, May 10th, 2014.

Participation of Mathieu Cunche to the TV show "Le Monde en Face" on France 5, June 17th, 2014.

Participation of Mathieu Cunche to the round table " Numériquement vôtre " at Futur en Seine, June 14h, 2014.

Seminar of Mathieu Cunche " Internet: Vie privée, Surveillance et Censure " at St-Génis Les Ollières, December 20th, 2014.

Seminar of Cédric Lauradoux " Identifiants et guesswork " Séminaire sur la Confiance Numérique at Clermont Ferrand, January 9th, 2014.

Seminar of Cédric Lauradoux " Identifiants et guesswork " Séminaire sur la Confiance Numérique at Clermont Ferrand, January 9th, 2014.

Seminar of Cédric Lauradoux " Déni de Service Algorithmique ", Journées Sécurité des Systèmes d'informations at Rouen, November 13th, 2014.

Seminar of Cédric Lauradoux " L'Internet des Objets et l'Internet des identifiants ", Colloque Sćurité de l'Internet des Objets (chaire de cyberdéfense et cybersécurité Saint-Cyr – Sogeti – Thalès) at Rouen, September 19th, 2014

Interview of Vincent Roca and Mathieu Cunche, “ Comment brouiller sa trace dans les réseaux ? ” Sciences et Avenir, issue 809, July 2014.

Interview of Vincent Roca, “ Spécial Grenoble : portrait de trois chercheurs ”, Le Point édition régionale, issue 2195, October 9th, 2014.

Editorial of Claude Castelluccia and Vincent Roca, “ Mobilitics Saison 2: les smartphones et leurs apps sous le microscope de la CNIL et d’Inria ”, La lettre Innovation et Prospective de la CNIL, issue 8, December 2014.

Seminar of Vincent Roca, “ Vie privée et Smartphone : le projet Mobilitics Inria/CNIL ”, DAFP-RAF Inria meeting, Paris, October 16th, 2014.

Seminar of Vincent Roca, “ Vie privée et Smartphone : le projet Mobilitics Inria/CNIL ”, organized by the Guilde des Utilisateurs d’Informatique Libre du Dauphiné (GUILDE), Grenoble, November 4th, 2014.

Short TV subject with Vincent Roca, “ Applications mobiles : de vrais espions ? ”, ARTE X:enius magazine, September 1st, 2014. http://www.arte.tv/guide/fr/051090-010/x-enius?vid=051090-010_PLUS7-F

Press conference, organized by CNIL in association with Inria, “ Vie privée et smartphones : les nouveaux résultats du projet Mobilitics Inria-CNIL ”, December 15th, 2014.

Seminar of Daniel Le Métayer, at the Cybersecurity Forum (ETH Zurich), 2014.

Participation of Daniel Le Métayer to a panel on privacy by design at the Annual Privacy Forum (APF 2014, Athens).

Participation of Daniel Le Métayer to Panel on at Computers Privacy and Data Protection (CPDP 2014 – Brussels).

Nomination of Daniel Le Métayer at the Commission of the French Parliament “Commission de réflexion et de propositions ad hoc sur le droit et les libertés à l’âge du numérique. ”

Organization of a seminar on privacy for the COERLE (Inria) by Claude Castelluccia and Daniel Le Métayer, November 2014.

9. Bibliography

Publications of the year

Doctoral Dissertations and Habilitation Theses

[1] F. MATTOUSSI. *Design and optimization of AL-FEC codes: the GLDPC-Staircase codes*, Université de Grenoble, February 2014, https://tel.archives-ouvertes.fr/tel-00969573

[2] V. ROCA. *AL-FEC codes and robust content distribution protocols: components for high performance and scalable services*, Université de Grenoble, April 2014, version 2.0, 20 février 2014, Habilitation à diriger des recherches, https://tel.archives-ouvertes.fr/tel-00925955

Articles in International Peer-Reviewed Journals

[3] D. LE MÉTAYER, L. CHRISTOPHE. *Le consentement au traitement des données personnelles : une perspective comparative sur l’autonomie du sujet*, in "La Revue Juridique Themis", 2014, vol. 48, n^{o} 3, 32 p. , https://hal.inria.fr/hal-01089902

[4] M. Minier, F. Dedouit, D. Maret, M. Vergnault, F.-Z. Mokrane, H. Rousseau, N. Telmon, D. Rougé, P. Adalian. *Fetal age estimation using MSCT scans of the mandible*, in "International Journal of Legal Medicine", 2014, vol. 128, n^{o} 3, pp. 493-499 [*DOI :* 10.1007/s00414-013-0933-5], https://hal.archives-ouvertes.fr/hal-01085005

[5] M. Minier, D. Maret, F. Dedouit, M. Vergnault, F.-Z. Mokrane, H. Rousseau, P. Adalian, D. Rougé, N. Telmon. *Fetal age estimation using MSCT scans of deciduous tooth germs*, in "International Journal of Legal Medicine", 2014, vol. 128, n^{o} 1, pp. 177-182 [*DOI :* 10.1007/s00414-013-0890-z], https://hal.archives-ouvertes.fr/hal-01085019

Articles in National Peer-Reviewed Journals

[6] G. Gössler, D. Le Métayer, E. Mazza, M.-L. Potet, L. Astefanoaei. *Apport des méthodes formelles pour l'exploitation de logs informatiques dans un contexte contractuel*, in "Technique et Science Informatiques (TSI)", 2014, pp. 63-84 [*DOI :* 10.3166/tsi.33.63-84], https://hal.inria.fr/hal-01078220

International Conferences with Proceedings

[7] C. Abdelberi, T. Chen, M. Cunche, E. Decristofaro, A. Friedman, M. A. Kaafar. *Censorship in the Wild: Analyzing Internet Filtering in Syria*, in "Internet Measurement Conference (IMC)", Vancouver, BC, Canada, Canada, November 2014, https://hal.inria.fr/hal-01052581

[8] P. Achara, M. Cunche, V. Roca, A. Francillon. *Short Paper: WifiLeaks: Underestimated Privacy Implications of the ACCESS_WIFI_STATE Android Permission*, in "7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec))", Oxford, United Kingdom, July 2014 [*DOI :* 10.1145/2627393.2627399], https://hal.inria.fr/hal-00997716

[9] G. Acs, C. Castelluccia. *A Case Study: Privacy Preserving Release of Spatio-temporal Density in Paris*, in "KDD '14 Proceedings of the 20th ACM SIGKDD international conference on Knowledge discovery and data mining", New York, United States, ACM, August 2014, https://hal.inria.fr/hal-01060070

[10] T. Antignac, D. Le Métayer. *Privacy Architectures: Reasoning About Data Minimisation and Integrity*, in "STM - 10th International Workshop on Security and Trust Management", Wroclaw, France, C. Damsgaard Jensen, S. Mauw (editors), Springer, September 2014, vol. 8743, https://hal.inria.fr/hal-01054758

[11] T. Antignac, D. Le Métayer. *Privacy by Design: From Technologies to Architectures (Position Paper)*, in "APF - Annual Privacy Forum 2014", Athens, Greece, B. Preneel, D. Ikonomou (editors), Springer, May 2014, vol. 8450, pp. 1-17 [*DOI :* 10.1007/978-3-319-06749-0_1], https://hal.inria.fr/hal-01070140

[12] D. Butin, D. Le Métayer. *Log Analysis for Data Protection Accountability*, in "FM2014 - 19th International Symposium on Formal Methods", Singapore, Singapore, Springer, May 2014, vol. 8442, pp. 163-178 [*DOI :* 10.1007/978-3-319-06410-9_12], https://hal.inria.fr/hal-00984308

[13] C. Castelluccia, C. Castelluccia, L. Olejnik, T. Minh-Dung. *Selling Off Privacy at Auction*, in "Network and Distributed System Security Symposium (NDSS)", San Diego, California, United States, NDSS, ISOC, November 2014, https://hal.inria.fr/hal-01087557

[14] A. Chaabane, Y. Ding, R. Dey, M. Ali Kaafar, K. Ross. *A Closer Look at Third-Party OSN Applications: Are They Leaking Your Personal Information?*, in "Passive and Active Measurement conference (2014)", Los Angeles, United States, Springer, March 2014, https://hal.inria.fr/hal-00939175

[15] M. CUNCHE, M. A. KAAFAR, R. BORELI. *Asynchronous Covert Communication Using BitTorrent Trackers*, in "International Symposium on Cyberspace Safety and Security (CSS)", Paris, France, August 2014, https://hal.inria.fr/hal-01053147

[16] L. DEMIR, M. CUNCHE, C. LAURADOUX. *Analysing the privacy policies of Wi-Fi trackers*, in "Workshop on Physical Analytics", Bretton Woods, United States, ACM, June 2014 [*DOI :* 10.1145/2611264.2611266], https://hal.inria.fr/hal-00983363

[17] O. ERDENE-OCHIR, M. ABDALLAH, K. QARAQE, M. MINIER, F. VALOIS. *Routing Resilience Evaluation for Smart Metering: Definition, Metric and Techniques*, in "PIMRC - IEEE 25th International Symposium on Personal, Indoor and Mobile Radio Communications", Washington DC, United States, September 2014, https://hal.inria.fr/hal-01015801

[18] S. GAMBS, M.-O. KILLIJIAN, C. LAURADOUX, C. ONETE, M. ROY, M. TRAORÉ. *VSSDB: A Verifiable Secret-Sharing and Distance-Bounding protocol*, in "International Conference on Cryptography and Information security (BalkanCryptSec'14)", Istanbul, Turkey, October 2014, https://hal.inria.fr/hal-01090056

[19] L. JACQUIN, V. ROCA, J.-L. ROCH. *Too Big or Too Small? The PTB-PTS ICMP-based Attack against IPsec Gateways*, in "IEEE Global Communications Conference (GLOBECOM'14)", Austin, United States, T. RAPPAPORT (editor), IEEE, December 2014, https://hal.inria.fr/hal-01052994

[20] D. LE MÉTAYER, H. KOPP, R. VAN DER HEIJDEN, F. KARGL, M. FAZOUANE. *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

[21] Z. LI, G. XIE, J. LIN, Y. JIN, M. A. KAAFAR, K. SALAMATIAN. *On the geographic patterns of a large-scale mobile video-on-demand system*, in "33rd IEEE INFOCOM conference", Toronto, Canada, April 2014, pp. 397-405 [*DOI :* 10.1109/INFOCOM.2014.6847962], https://hal.archives-ouvertes.fr/hal-01066515

[22] Z. MA, D. BUTIN, F. JAIME, F. COUDERT, A. KUNG, C. GAYREL, A. MAÑA, C. JOUVRAY, N. TRUSSART, N. GRANDJEAN, V. MANUEL HIDALGO, M. BOSSUET, F. CASADO, M. C. HIDALGO. *Towards a Multidisciplinary Framework to Include Privacy in the Design of Video Surveillance Systems*, in "Second Annual Privacy Forum (APF 2014)", Athènes, Greece, Springer, May 2014, vol. 8450, pp. 101-116 [*DOI :* 10.1007/978-3-319-06749-0_7], https://hal.inria.fr/hal-00994303

[23] K. MATSUZONO, V. ROCA, H. ASAEDA. *Structured Random Linear Codes (SRLC): Bridging the Gap between Block and Convolutional Codes*, in "IEEE Global Communications Conference (GLOBECOM'14)", Austin, United States, T. RAPPAPORT (editor), IEEE, December 2014, https://hal.inria.fr/hal-01059554

[24] N. NOTARIO, D. LE MÉTAYER, A. CRESPO, A. KUNG, I. KROENER, C. TRONCOSO, J. DEL ALAMO, Y.-S. MARTÍN. *PRIPARE: A New Vision on Engineering Privacy and Security by Design*, in "Cyber Security & Privacy Forum", Athènes, Greece, May 2014, https://hal.inria.fr/hal-01089889

[25] L. OLEJNIK, K. AGNIESZKA, C. CASTELLUCCIA. *I'm 2.8% Neanderthal - The Beginning of Genetic Exhibitionism?*, in "Workshop on Genome Privacy", Amsterdam, Netherlands, Netherlands, July 2014, https://hal.inria.fr/hal-01087696

[26] V.-T. TA, T. ANTIGNAC. *Privacy by Design: On the Conformance Between Protocols and Architectures*, in "FPS - 7th International Symposium on Foundations & Practice of Security", Montreal, Canada, P. W.

L. Fong, F. Cuppens, J. Garcia-Alfaro, N. Zincir Heywood (editors), Springer, November 2014, https://hal.inria.fr/hal-01103546

Conferences without Proceedings

[27] C. Matte, M. Cunche. *Beam me up, Scotty: identifying the individual behind a MAC address using Wi-Fi geolocation spoofing*, in "1er Colloque sur la Confiance Numérique en Auvergne", Clermont-Ferrand, France, December 2014, https://hal.inria.fr/hal-01093524

Scientific Books (or Scientific Book chapters)

[28] D. Butin, M. Chicote, D. Le Métayer. *Strong Accountability: Beyond Vague Promises*, in "Reloading Data Protection: Multidisciplinary Insights and Contemporary Challenges", S. Gutwirth, R. Leenes, P. De Hert (editors), Springer, 2014, pp. 343-369 [*DOI :* 10.1007/978-94-007-7540-4_16], https://hal.inria.fr/hal-00917350

Research Reports

[29] P. Achara, M. Cunche, V. Roca, A. Francillon. *WifiLeaks: Underestimated Privacy Implications of the ACCESS_WIFI_STATE Android Permission*, May 2014, n° RR-8539, 21 p. , A short version has been accepted for publication in: 7th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WISEC'14) Oxford, United Kingdom, July 23rd - 25th 2014, https://hal.inria.fr/hal-00994926

[30] C. Boura, M. Minier, M. Naya-Plasencia, V. Suder. *Improved Impossible Differential Attacks against Round-Reduced LBlock*, IACR, April 2014, http://eprint.iacr.org/2014/279, https://hal.archives-ouvertes.fr/hal-01068887

[31] P. Brunisholz, M. Minier, F. Valois. *The Gain of Network Coding in Wireless Sensor Networking*, Inria ; INP Grenoble, December 2014, n° RR-8650, https://hal.inria.fr/hal-01092287

[32] M. Cunche, M. A. Kaafar, R. Boreli. *Asynchronous Covert Communication Using BitTorrent Trackers*, June 2014, n° RR-8554, https://hal.inria.fr/hal-01011739

[33] L. Demir, M. Cunche, C. Lauradoux. *Analysing the privacy policies of Wi-Fi trackers*, March 2014, n° RR-8506, https://hal.inria.fr/hal-00968585

[34] T. Gerbet, A. Kumar, C. Lauradoux. *The Power of Evil Choices in Bloom Filters*, Inria Grenoble, November 2014, n° RR-8627, https://hal.inria.fr/hal-01082158

[35] T. Gerbet, A. Kumar, C. Lauradoux. *(Un)Safe Browsing*, September 2014, n° RR-8594, https://hal.inria.fr/hal-01064822

[36] A. Kumar, P. Lafourcade, C. Lauradoux. *Performances of Cryptographic Accumulators*, May 2014, https://hal.archives-ouvertes.fr/hal-00999432

Scientific Popularization

[37] V. Roca. *Privacy and Smartphones: the Mobilitics Inria/CNIL project*, November 2014, Séminaire Guilde, https://hal.inria.fr/hal-01087967

Patents and standards

[38] A. Kountouris, O. Erdene-Ochir, M. Minier, F. Valois. *Protocole de routage à sauts multiples*, May 2014, n^{o} 12773078.6 - 1857, https://hal.inria.fr/hal-01003848

Other Publications

[39] J. Detchart, V. Roca, J. Lacan, E. Lochin. *Tetrys, an On-the-Fly Network Coding protocol*, October 2014, Working document of the NWCRG (Network Coding Research Group) group of IRTF (Internet Research Task Force), https://hal.inria.fr/hal-01089745

[40] V. Firoiu, B. Adamson, V. Roca, C. Adjih, J. Bilbao, F. Fitzek, A. Masucci, M.-J. Montpetit. *Network Coding Taxonomy*, November 2014, Internet Research Task Force - Working document of the Network Coding Research Group (NWCRG), https://hal.inria.fr/hal-00998506

[41] D. Le Métayer, G. Danezis, M. Hansen, J.-H. Hoepman, R. Tirtea, S. Schiffner, J. Domingo-Ferrer. *Privacy and Data Protection by Design - from policy to engineering*, December 2014, ENISA Report, https://hal.inria.fr/hal-01097119

[42] M. Minier, C. Solnon, J. Reboul. *Solving a Symmetric Key Cryptographic Problemwith Constraint Programming*, July 2014, 13 p. , ModRef 2014, Workshop of the CP 2014 Conference, September 2014, Lyon, France, https://hal.inria.fr/hal-01092574

[43] V. Roca, K. Matsuzono. *Structured RLC codes: an update*, March 2014, IETF89 - NWCRG meeting, https://hal.inria.fr/hal-00955772

[44] V. Roca. , A. Vazquez-Castro (editor) *RLC and AL-FEC @ IETF: when codes meet transport protocols and practical aspects*, February 2014, Algebraic approaches to storage and network coding - COST IC1104, https://hal.inria.fr/hal-00948895