IN PARTNERSHIP WITH:
Institut national des sciences appliquées de Lyon

Activity Report 2019

Project-Team PRIVATICS

Privacy Models, Architectures and Tools for the Information Society

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

RESEARCH CENTERS
Grenoble - Rhône-Alpes
Sophia Antipolis - Méditerranée

THEME
Security and Confidentiality

Table of contents

Project-Team PRIVATICS

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

Keywords:

Computer Science and Digital Science:

A1. - Architectures, systems and networks
A3. - Data and knowledge
A4. - Security and privacy
A9. - Artificial intelligence

Other Research Topics and Application Domains:

B2. - Health
B6. - IT and telecom
B8. - Smart Cities and Territories
B9. - Society and Knowledge

1. Team, Visitors, External Collaborators

Research Scientists

Claude Castelluccia [Team leader, Inria, Senior Researcher, Grenoble - Rhône-Alpes, HDR]
Vincent Roca [Team leader, Inria, Researcher, Grenoble - Rhône-Alpes, HDR]
Nataliia Bielova [Inria, Researcher, since October 2019, Sophia Antipolis - Méditerranée]
Cédric Lauradoux [Inria, Researcher, Grenoble - Rhône-Alpes]
Daniel Le Métayer [Inria, Senior Researcher, Grenoble - Rhône-Alpes, HDR]

Faculty Members

Antoine Boutet [INSA Lyon, Associate Professor, Grenoble - Rhône-Alpes]
Mathieu Cunche [INSA Lyon, Associate Professor, Grenoble - Rhône-Alpes]

Post-Doctoral Fellows

Raul Pardo Jimenez [Inria, Post-Doctoral Fellow, until Jul 2019, Grenoble - Rhône-Alpes]
Celestin Matté [Inria, Post-Doctoral Fellow, Sophia Antipolis - Méditerranée]

PhD Students

Supriya Sreekant Adhatarao [Inria, PhD Student, Grenoble - Rhône-Alpes]
Coline Boniface [Univ Grenoble Alpes, PhD Student, Grenoble - Rhône-Alpes]
Guillaume Celosia [INSA Lyon, PhD Student, Grenoble - Rhône-Alpes]
Imane Fouad [Inria, Phd Student, Sophia Antipolis - Méditerranée]
Clement Henin [Ministère de l'Ecologie, de l'Energie, du Développement durable et de la Mer, PhD Student, Grenoble - Rhône-Alpes]
Theo Jourdan [INSERM, PhD Student, Grenoble - Rhône-Alpes]
Raouf Kerkouche [Univ Grenoble Alpes, PhD Student, Grenoble - Rhône-Alpes]
Victor Morel [Inria, PhD Student, Grenoble - Rhône-Alpes]
Mathieu Thiery [Inria, PhD Student, Grenoble - Rhône-Alpes]
Michael Toth [Inria, Phd Student, Sophia Antipolis - Méditerranée]

Technical staff

Adrien Baud [Inria, Engineer, from Oct 2019, Grenoble - Rhône-Alpes]

Interns and Apprentices

Jan Aalmoes [Inria, from Jun 2019 until Aug 2019, Grenoble - Rhône-Alpes]

Hilaire Bouaddi [Inria, from Jun 2019 until Aug 2019, Grenoble - Rhône-Alpes]
George-Antoine Christakis [Ministère de l'Education Nationale, Mar 2019, Grenoble - Rhône-Alpes]
Felix Fonteneau [INSA Lyon, from Jun 2019 until Aug 2019, Grenoble - Rhône-Alpes]
Andres Olivares Arredondo [Inria, until Mar 2019, Grenoble - Rhône-Alpes]
Piyush Patil [Univ Grenoble Alpes, from Feb 2019 until Jul 2019, Grenoble - Rhône-Alpes]
Vincent Prax [Inria, from Feb 2019 until Jul 2019, Grenoble - Rhône-Alpes]

Administrative Assistant

Helen Pouchot-Rouge-Blanc [Inria, Administrative Assistant, Grenoble - Rhône-Alpes]

Visiting Scientists

Jeremie Decouchant [Université du Luxembourg, Oct 2019, Grenoble - Rhône-Alpes]
Gergely Acs [Budapest University of Technology and Economics, Jul 2019, Grenoble - Rhône-Alpes]

2. Overall Objectives

2.1. Context

Since its creation in 2014, the PRIVATICS project-team focusses on privacy protection in the digital world. It includes, on one side, activities that aim at understanding the domain and its evolution, both from theoretical and practical aspects, and, on the other side, activities that aim at designing privacy-enhancing tools and systems. The approach taken in PRIVATICS is fundamentally inter-disciplinary and covers theoretical, legal, economical, sociological and ethical aspects by the means of enriched collaborations with the members of these disciplines.

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

PRIVATICS members have written several position documents for policy makers: a report on facial recognition, algorithmic decision-making, pseudonymisation and a white book on cybersecurity.

5. New Software and Platforms

5.1. FECFRAME

FEC Framework following RFC 6363 specifications (https://datatracker.ietf.org/doc/rfc6363/)

KEYWORDS: Error Correction Code - Content delivery protocol - Robust transmission

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

- Participant: Vincent Roca
- Contact: Vincent Roca

5.2. Wombat

Wi-Fi tracking system for testing and demonstrational purpose

KEYWORDS: Wi-Fi - Privacy - Multimodal tracking of human activity - Wireless network

FUNCTIONAL DESCRIPTION: Wombat is a fully functional Wi-Fi tracking platform supporting three main features: collection, storage/processing, query/output. These three features are implemented through a distributed infrastructure composed of:

Sensor nodes: small devices with wireless monitoring capabilities. They collect information sent on wireless channels and forward it to the server. Central server: the central entity of the system. It receives data sent by sensor nodes and then stores it in an internal data structure. It is also in charge of answering queries related to the stored data.

To ensure communication between the sensor nodes and the server, the Wombat system relies on a wired network (Ethernet). In addition, Wombat can be enriched with a user interface and an opt-out node:

User interface: a device in charge of displaying detailed information about one or several tracked devices (see figure below). The device to display can be specified manually by its MAC address or through proximity detection. Opt-out node: an element in charge of implementing an opt-out mechanism for users refusing to be tracked by the system.

The system is made to work on a dedicated network (the server includes a DHCP server). Nodes can be switched off at any time (they function in read-only mode to be crash-proof).

- Partner: Insa de Lyon
- Contact: Mathieu Cunche
- URL: https://github.com/Perdu/wombat

5.3. Cookie glasses

KEYWORDS: GDPR - Cookie - Consent

SCIENTIFIC DESCRIPTION: In the paper Do Cookie Banners Respect my Choice? Measuring Legal Compliance of Banners from IAB Europe's Transparency and Consent Framework, we show that Consent Management Providers (CMPs) of IAB Europe's Transparency & Consent Framework (TCF) do not always respect user's choice. This extension allows users to verify that their consent is stored appropriately by themselves.

This extension for Firefox and Chrome queries CMPs of IAB Europe's TCF in the same position as a third-party advertiser, making it possible to see consent set by CMPs in real time. In other words, you can see whether consent registered by cookie banners is actually the consent you gave. Will only work with cookie banners of IAB Europe's TCF.

We also added a functionality to manually decode a so-called "consent string" of the framework.

- Participants: Célestin Matte and Nataliia Bielova
- Contact: Alain Prette

5.4. BELL

Browser fingerprinting via Extensions and Login-Leaks

KEYWORDS: Browser Extensions - Security and Privacy in Web Services - Social Networks Security and Privacy

FUNCTIONAL DESCRIPTION: Recent studies show that users can be tracked based on their web browser properties. This software is designed to conduct an experiment on such kinds of user tracking. In this experiment, we demonstrate that a Web user can also be tracked by

- her browser extensions (such as AdBlock, Pinterest, or Ghostery), and

- the websites she has logged in (such as Facebook, Gmail, or Twitter).

In the experiment, we collect user's browser fingerprint, together with the browser extensions installed and a list of websites she has logged in. We only collect anonymous data during the experiment (more details in our Privacy Policy [1]), we will securely store the data on an Inria server, use it only for research purposes and not share it with anyone outside of Inria.

- Contact: Gabor Gulyas
- URL: https://extensions.inrialpes.fr/

5.5. SWIF-codec

An open-source sliding window FEC codec

KEYWORD: Error Correction Code

FUNCTIONAL DESCRIPTION: This development is done in the context of the "Coding for Efficient Network Communications" IRTF Research Group (NWCRG, [https://datatracker.ietf.org/rg/nwcrg]) and IETF hackathon.

[1] https://extensions.inrialpes.fr/privacy.php

This work has strong relationships with the Generic API I-D [https://datatracker.ietf.org/doc/draft-roca-nwcrg-generic-fec-api/] and RFC 8681 on RLC codes [https://www.rfc-editor.org/rfc/rfc8681] as examples of sliding window codes.

- Authors: Vincent Roca, Cédric Adjih, Oumaima Attia and François Michel
- Contact: Vincent Roca
- URL: https://github.com/irtf-nwcrg/swif-codec

6. New Results

6.1. Differential Inference Testing

Participant: Claude Castelluccia.

In order to protect individuals' privacy, data have to be "well-sanitized" before sharing them, i.e. one has to remove any personal information before sharing data. However, it is not always clear when data shall be deemed well-sanitized. In [10], we argue that the evaluation of sanitized data should be based on whether the data allows the inference of sensitive information that is specific to an individual, instead of being centered around the concept of re-identification. We propose a framework to evaluate the effectiveness of different sanitization techniques on a given dataset by measuring how much an individual's record from the sanitized dataset influences the inference of his/her own sensitive attribute. Our intent is not to accurately predict any sensitive attribute but rather to measure the impact of a single record on the inference of sensitive information. We demonstrate our approach by sanitizing two real datasets in different privacy models and evaluate/compare each sanitized dataset in our framework.

6.2. Analyse des impacts de la reconnaissance faciale - Quelques éléments de méthode (in French)

Participants: Claude Castelluccia, Daniel Le Métayer.

Significant technical progress has been made in recent years in the field of image processing, in particular in facial recognition. The deployments and experiments of this type of systems are more and more numerous. However, opinions differ on their use, especially in public space. Noting the lack of consensus on a technology that can have a significant impact on society, many organizations have alerted public opinion and asked for a public debate on the subject. We believe that such a debate is indeed necessary. However, for it to be truly productive, it is necessary to be able to confront the arguments in a rigorous manner while avoiding, as far as possible, the preconceptions, and by distinguishing established facts from assumptions or opinions. The purpose of this document [14] is precisely to help put the terms of the debate on solid foundations. It is therefore not a question here of taking a position on facial recognition in general nor of providing an exhaustive review of its applications but of proposing elements of method, illustrated by a few examples. We first present a quick overview of the applications of facial recognition before detailing the reasons that make it a particularly sensitive subject, emphasizing in particular the risks linked to a possible generalization of its use. We then present an incremental, comparative and rigorous approach to analyze the impacts of a facial recognition system.

6.3. Towards a generic framework for black-box explanation methods

Participants: Daniel Le Métayer, Clément Hénin.

Explainability has generated increased interest during the last decade because the most accurate ML techniques often lead to opaque Algorithmic Decision Systems (ADS) and opacity is a major source of mistrust. Indeed, even if explanations are not a panacea, they can play a key role, not only to enhance trust in the system, but also to allow its users to better understand its outputs and therefore to make a better use of it. In addition, they are necessary to make it possible to challenge the decisions resulting from an ADS. Explanations can take different forms, they can target different types of users and different types of methods can be used to produce them. Our work on this topic [15] focuses on a category of methods, called "black-box", that do not make any assumption about the availability of the code of the ADS or its implementation techniques. Our first contribution is to bring to light a common structure for Black-box Explanation Methods and to define a generic framework allowing us to compare and classify different approaches. This framework consists of three components, called respectively Sampling, Generation and Interaction. Beyond its interest as a systematic presentation of the state of the art, we believe that this framework can also provide new insights for the design of new explanation systems. For example, it may suggest new combinations of Sampling and Generation components or criteria to choose the most appropriate combination to produce a given type of explanation.

6.4. A generic information and consent framework for the IoT

Participants: Daniel Le Métayer, Mathieu Cunche, Victor Morel.

The development of the Internet of Things (IoT) raises specific privacy issues especially with respect to information and consent. People are generally unaware of the devices collecting data about them and do not know the organizations operating them. Solutions such as stickers or wall signs are not effective information means in most situations. As far as consent is concerned, individuals do not have simple means to express and communicate it to the entities collecting data. Furthermore, the devices used to collect data in IoT environments have scarce resources; some of them do not have any user interface, are battery-operated or operate passively. The Working Party 29 (now "European Data Protection Board") advocates the design of new consent mechanisms, such as "privacy proxies", on the devices themselves. Starting from their recommendations, we have defined general requirements that have to be met to ensure that information and consent are managed in a manner that is satisfactory both for data subjects and for data controllers. We have shown in [8] how these requirements can be implemented in different situations, in particular through declaration registers and beacons. Depending on the context and the types of devices involved, not all technical options are always possible. In order to provide guidance to IoT system designers, we have outlined the main choice factors in the design pace are illustrated the framework with several challenging case studies. We have also implemented a Proof of Concept prototype implementation of these techniques.

6.5. Analysis of privacy policies to enhance informed consent

Participant: Daniel Le Métayer.

A privacy policy language must meet a number of requirements to be able to express the valid consent of the data subject for the processing of their personal data. For example, under the GDPR, valid consent must be freely given, specific, informed and unambiguous. Therefore, the language must be endowed with a formal semantics in order to avoid any ambiguity about the meaning of a privacy policy. However, the mere existence of a semantics does not imply that DSs properly understand the meaning of a policy and its potential consequences. One way to enhance the understanding of the data subjects is to provide them information about the potential risks related to a privacy policy. This is in line with Recital 39 of the GDPR which stipulates that data subjects should be "made aware of the risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing". To address this need, we have defined a language in [11], called PILOT, meeting these requirements and shown its benefits to define precise privacy policies and to highlight the associated privacy risks. In order to automatically answer questions related to privacy risks, we use the verification tool SPIN and the modeling language PROMELA. Risk properties are encoded in Linear Temporal Logic properties that can be automatically checked by SPIN.

6.6. Understanding algorithmic decision-making: Opportunities and challenges, Study for the European Parliament (STOA)

Participants: Claude Castelluccia, Daniel Le Métayer.

Algorithms are far from being a recent invention but they are increasingly involved in systems used to support decision making. Algorithmic Decision Systems (ADS) often rely on the analysis of large amounts of personal data to infer correlations or, more generally, to derive information deemed useful to make decisions. Humans may have a role of varying degree in the decision making and may even be completely out of the loop in entirely automated systems. In many situations, the impact of the decision on people can be significant: access to credit, employment, medical treatment, judicial sentences, etc. Entrusting ADS to make or to influence such decisions raises a variety of issues that differ in nature such as ethical, political, legal, technical, etc. and great care must be taken to analyse and address these issues. If they are neglected, the expected benefits of these systems may be offset by the variety of risks for individuals (discrimination, unfair practices, loss of autonomy, etc.), the economy (unfair practices, limited access to markets, etc.) and society as a whole (manipulation, threat to democracy, etc.).

We have written a report for the European Parliament reviewing the opportunities and risks related to the use of ADS. We present existing options to reduce these risks and explain their limitations. We sketch some recommendations to benefit from the tremendous possibilities of ADS while limiting the risks related to their use. Beyond providing an up-to-date and systematic review of the situation, the report gives a precise definition of a number of key terms and an analysis of their differences. This helps clarify the debate. The main focus of the report is the technical aspects of ADS. However, other legal, ethical and social dimensions are considered to broaden the discussion.

6.7. Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism

Participants: Mathieu Cunche, Guillaume Celiosa.

The Bluetooth Low Energy (BLE) protocol is being included in a growing number of connected objects such as fitness trackers and headphones. As part of the service discovery mechanism of BLE, devices announce themselves by broadcasting radio signals called advertisement packets that can be collected with off-the-shelf hardware and software. To avoid the risk of tracking based on those messages, BLE features an address randomization mechanism that substitutes the device address with random temporary pseudonyms,called Private addresses. We analyze the privacy issues associated with the advertising mechanism of BLE, leveraging a large dataset of advertisement packets collected in the wild. First, we identified in [7] that some implementations fail at following the BLE specifications on the maximum lifetime and the uniform distribution of random identifiers. Furthermore, we found that the payload of the advertisement packet can hamper the randomization mechanism by exposing counters and static identifiers. In particular, we discovered that advertising data of Apple and Microsoft proximity protocols can be used to defeat the address randomization scheme. Finally, we discuss how some elements of advertising data can be leveraged to identify the type of device, exposing the owner to inventory attacks

6.8. Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile

Participants: Mathieu Cunche, Guillaume Celiosa.

Bluetooth Low Energy (BLE) is a short range wireless technology included in many consumer devices such as smartphones, earphones and wristbands. As part of the Attribute (ATT) protocol, discoverable BLE devices expose a data structure called Generic Attribute (GATT) profile that describes supported features using concepts of services and characteristics. This profile can be accessed by any device in range and can expose users to privacy issues. We study how the GATT profile can be used to create a fingerprint that can be exploited

to circumvent anti-tracking features of the BLE standard (i.e. MAC address randomization). Leveraging a dataset of more than 13000 profiles, we analyze the potential of this fingerprint and show that it can be used to uniquely identify a number of devices. We also shed light in [6] on several issues where GATT profiles can be mined to infer sensitive information that can impact privacy of users. Finally, we suggest solutions to mitigate those issues.

6.9. Privacy implications of switching ON a light bulb in the IoT world

Participants: Vincent Roca, Mathieu Thiery.

The number of connected devices is increasing every day, creating smart homes and shaping the era of the Internet of Things (IoT), and most of the time, end-users are unaware of their impacts on privacy. We analyze in [23] the ecosystem around a Philips Hue smart white bulb in order to assess the privacy risks associated to the use of different devices (smart speaker or button) and smartphone applications to control it. We show that using different techniques to switch ON or OFF this bulb has significant consequences regarding the actors involved (who mechanically gather information on the user's home) and the volume of data sent to the Internet (we measured differences up to a factor 100, depending on the control technique we used). Even when the user is at home, these data flows often leave the user's country, creating a situation that is neither privacy friendly (and the user is most of the time ignorant of the situation), nor sovereign (the user depends on foreign actors), nor sustainable (the extra energetic consumption is far from negligible). We therefore advocate a complete change of approach, that favors local communications whenever sufficient.

6.10. Security Analysis of Subject Access Request Procedures How to authenticate data subjects safely when they request for their data

Participants: Cédric Lauradoux, Coline Boniface.

With the GDPR in force in the EU since May 2018, companies and administrations need to be vigilant about the personal data they process. The new regulation defines rights for data subjects and obligations for data controllers but it is unclear how subjects and controllers interact concretely. In [4], we try to answer two critical questions: is it safe for a data subject to exercise the right of access of her own data? When does a data controller have enough information to authenticate a data subject? To answer these questions, we have analyzed recommendations of Data Protection Authorities and authentication practices implemented in popular websites and third-party tracking services. We observed that some data controllers use unsafe or doubtful procedures to authenticate data subjects. The most common flaw is the use of authentication based on a copy of the subject's national identity card transmitted over an insecure channel. We define how a data controller should react to a subject's request to determine the appropriate procedures to identify the subject and her data. We provide compliance guidelines on data access response procedures.

6.11. Plausible Deniability for Practical Privacy-Preserving Live Streaming

Participant: Antoine Boutet.

Video consumption is one of the most popular Internet activities worldwide. The emergence of sharing videos directly recorded with smartphones raises important privacy concerns. In this work we propose P3LS, the first practical privacy-preserving peer-to-peer live streaming system. To protect the privacy of its users, P3LS relies on k-anonymity when users subscribe to streams, and on plausible deniability for the dissemination of video streams. Specifically, plausible deniability during the dissemination phase ensures that an adversary is never able to distinguish a user's stream of interest from the fake streams from a statistical analysis (i.e., using an analysis of variance). We exhaustively evaluate P3LS and show that adversaries are not able to identify the real stream of a user with very high confidence. Moreover, P3LS consumes 30% less bandwidth than the standard k-anonymity approach where nodes fully contribute to the dissemination of k streams.

6.12. Protecting motion sensor data against sensitive inferences through an adversarial network approach

Participants: Antoine Boutet, Théo Jourdan.

With the widespread development of the quantified self movement, more and more motion sensor data are captured and transmitted through the intermediary of smartphones. However, granting to applications a direct access to sensor data expose users to many privacy risks, including in particular the possibility of inferring their activities and transportation mode to more sensitive inferences such as their demographic attributes or even mobility deficiency. In this work, we propose a privacy-preserving scheme to protect sensor data for activity recognition while at the same time preventing unwanted sensitive inferences on specific information. To achieve this objective, we leverage on the powerful framework of generative adversarial networks (GANs) to sanitize the sensor data. More precisely in our framework three neural networks are jointly trained, a generator that aim at sanitizing the data given at input as well two discriminators that try to infer respectively the sensitive attributes and the current activity of the user. By letting these neural networks compete against each other, the mechanism improves the protection while providing a good accuracy in terms of activity recognition and limiting sensitive inferences on specified attributes. Preliminary results demonstrate that the approach is promising in terms of achieving a good utility-privacy trade-off.

6.13. Inria white book on Cybersecurity: Current challenges and Inria's research directions

Participant: Vincent Roca.

This book provides an overview of research areas in cybersecurity, illustrated by contributions from Inria teams. The first step in cybersecurity is to identify threats and define a corresponding attacker model. Threats, including malware, physical damage or social engineering, can target the hardware, the network, the operating system, the applications, or the users themselves.

Then, detection and protection mechanisms must be designed to defend against these threats. One of the core mechanisms is cryptography, in order to ensure the confidentiality and integrity of data. These primitives must be the object of continuous cryptanalysis to ensure the highest level of security. However, secure cryptographic primitives alone are not sufficient for secure communications and services: cryptographic protocols, implementing richer interactions on top of the primitives, are needed. These protocols are distributed systems. Ensuring that they achieve their goals in the presence of an adversary requires the use of formal verification techniques, which have been extremely successful in this field.

Additional security services, such as authentication and access control, are needed to enforce a security policy. These security services, usually provided by the operating system or the network devices, can themselves be attacked and sometimes bypassed. Therefore, activities on the information system are monitored in order to detect any violation of the security policy. Finally, as attacks can spread extremely fast, the system must react automatically or at least reconfigure itself to avoid propagating attacks.

Privacy has also become an intrinsic part of cybersecurity. Privacy has its own properties, techniques, and methodology. Moreover, the study of privacy often requires to take legal, economical, and sociological aspects into account.

All these security mechanisms need to be carefully integrated in security-critical applications. These applications include traditional safety-critical applications that are becoming increasingly connected and therefore more vulnerable to security attacks, as well as new infrastructures running in the cloud or connected to a multitude of Things (IoT).

6.14. Inspect what your location history reveals about you - Raising user awareness on privacy threats associated with disclosing his location data

Participant: Antoine Boutet.

Location is one of the most extensively collected personal data on mobile by applications and third-party services. However, how the location of users is actually processed in practice by the actors of targeted advertising ecosystem remains unclear. Nonetheless, these providers have a strong incentive to create very detailed profile of users to better monetize the collected data. End users are usually not aware about the strength and wide range of inference that can be performed from their mobility traces. In this work, users interact with a web-based application to inspect their location history and to discover the inferential power of this kind of data. Moreover to better understand the possible countermeasures, users can apply a sanitization to protect their data and visualize the impact on both the mobility traces and the associated inferred information. The objective of this work is to raise the user awareness on the profiling capabilities and the privacy threats associated with disclosing his location data as well as how sanitization mechanisms can be efficient to mitigate these privacy risks. In addition, by collecting users feedbacks on the personal information revealed and the usage of a geosanitization mechanism, we hope that this work will also be useful to constitute a new and valuable dataset on users perceptions on these questions.

6.15. Pseudonymisation techniques and best practices

Participant: Cédric Lauradoux.

This ENISA report explores further the basic notions of pseudonymisation, as well as technical solutions that can support implementation in practice. Starting from a number of pseudonymisation scenarios, the report defines first the main actors that can be involved in the process of pseudonymisation along with their possible roles. It then analyses the different adversarial models and attacking techniques against pseudonymisation, such as brute force attack, dictionary search and guesswork. Moreover, it presents the main pseudonymisation techniques and policies available today.

7. Partnerships and Cooperations

7.1. Regional Initiatives

7.1.1. 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).

7.1.2. Data Institute

- Title: Data Institute UGA
- Duration: 2017 - .
- Coordinator: TIMC-IMAG.
- Others partners: AGEIS, BIG, CESICE, GIN, GIPSA-lab, IAB, IGE, IPAG, LAPP, LARHRA, LIDILEM, LIG, LISTIC, LITT&ArTS, LJK, LUHCIE, LECA, OSUG, PACTE, TIMC-IMAG

- Abstract: Privatics is leading the WP5 (Data Governance, Data Protection and Privacy). This action (WP5) aims to analyze, in a multi-disciplinary perspective, why and how specific forms of data governance emerge as well as the consequences on the interaction between the state, the market and society. The focus will be on the challenges raised by the collection and use of data for privacy, on the data subjects' rights and on the obligations of data controllers and processors. A Privacy Impact/Risk assessments methodology and software will be proposed. A case study will focus on medical and health data and make recommendations on how they should be collected and processed.

7.1.3. CyberAlps

- Title: CyberAlps
- Duration: 2018 - .
- Coordinator: IF.
- Others partners: CEA LETI, CERAG, CESICE, CREg, G2E lab, GIPSA-lab, GSCOP, IF, LCIS, LIG, LISTIC, LJK, PACTE, TIMC-IMAG, VERIMAG.
- Abstract: The Grenoble Alpes Cybersecurity Institute aims at undertaking ground-breaking interdisciplinary research in order to address cybersecurity and privacy challenges. Our main technical focus is on low-cost secure elements, critical infrastructures, vulnerability analysis and validation of large systems, including practical resilience across the industry and the society. Our approach to cybersecurity is holistic, encompassing technical, legal, law-enforcement, economic, social, diplomatic, military and intelligence-related aspects with strong partnerships with the private sector and robust national and international cooperation with leading institutions in France and abroad.

7.1.4. Antidot

- Title: Antidot
- Type: Fédération Informatique de Lyon (inter laboratories project)
- Duration: September 2018 - 2020.
- Coordinator: Inria.
- Others partners: LIRIS.
- Abstract: The ANTIDOT project is interested in the privacy issues raised by the increasingly ubiquitous collection of mobility data and their exploitation by third-party applications. The objective of this project is to propose solutions and tools to increase the user awareness about the risks of violation of their privacy in the context of the mobile Internet. In order to achieve this objective, ANTIDOT will jointly address the study of information gathering mechanisms, the study of mobility data vulnerabilities and the protection of this personal data.

7.1.5. DARC

- Title: DARC - the Data Anonymization and Re-identification Competition
- Type: Innovation Pédagogique - IDEX LYON
- Duration: September 2019 - 2020.
- Coordinator: INSA.
- Abstract: In order to increase awareness and empower future digital engineers in a fun way on privacy issues, the DARC project offers learning through play through a challenge carried out jointly by three different training courses of INSA students in Bourges and in Lyon. This challenge consists first of all in anonymizing a dataset from an online sales site, then secondly in trying to re-identify the anonymized data of the other groups.

7.2. National Initiatives

7.2.1. ADT PRESERVE

- Title: PRESERVE: Plate-foRme wEb de SEnsibilisation aux pRoblèmes de Vie privéE
- Duration: 2019 - 2020
- Coordinator: INSA.
- Abstract: The goal of this project is to develop a web platform to increase the user awareness on privacy issues. This platform will gather multiple works investigated in the team and will be used to conduct demonstration and stimulate new collaborations and dissemination actions to end users and media.

7.2.2. ANR

7.2.2.1. CISC

Title: Certification of IoT Secure Compilation.

Type: ANR.

Duration: April 2018 - March 2022.

Coordinator: Inria INDES project-team (France)

Others partners: Inria CELTIC project-team (France), College de France (France) (France).

See also: http://cisc.gforge.inria.fr.

Abstract: The objective of the ANR CISC project is to investigate multitier languages and compilers to build secure IoT applications with private communication. A first goal is to extend multitier platforms by a new orchestration language that we call Hiphop.js to synchronize internal and external activities of IoT applications as a whole. CISC will define the language, semantics, attacker models, and policies for the IoT and investigate automatic implementation of privacy and security policies by multitier compilation of IoT applications. To guarantee such applications are correct, and in particular that the required security and privacy properties are achieved, the project will certify them using the Coq proof assistant.

7.2.2.2. SIDES 3.0

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

Type: ANR.

Duration: August 2017 - August 2020.

Coordinator: Uness (France).

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

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

7.2.2.3. DAPCODS/IOTics

Title: DAPCODS/IOTics.

Type: ANR 2016.

Duration: May 2017 - Dec. 2020.

Coordinator: Inria PRIVATICS.

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

Abstract:

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

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

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

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

7.2.3. Inria-CNIL collaboration

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

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

7.3. European Initiatives

7.3.1. Collaborations in European Programs, Except FP7 & H2020

7.3.1.1. UPRISE-IoT

Title: User-centric PRIvacy & Security in IoT

Programm: CHISTERA

Duration: December 2016 - December 2019

Coordinator: SUPSI (Suisse)

Inria contact: Claude Castelluccia

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

7.3.1.2. SPARTA

Title: Strategic Programs for Advanced Research and Technology in Europe (SPARTA)

Programm: H2020-SU-ICT-03-2018

Duration: February 2019 - January 2022

Coordinator: CEA

Inria contact: Thomas Jensen (Inria), Vincent Roca (for PRIVATICS)

SPARTA Cybersecurity European Competence Network. The consortium consists of 44 partners from 14 different countries, with the goal to demonstrate the setup and assessment of a European SPARTA Cybersecurity Competence Network.

7.4. International Initiatives

7.4.1. DATA

Title: Data and Algorithmic Transparency and Accountability

International Partner (Institution - Laboratory - Researcher):

Université du Québec à Montréal (UQAM) (Canada) - Département d'informatique - Sébastien Gambs

Start year: 2018

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

The accelerated growth of the Internet has outpaced our abilities as individuals to maintain control of our personal data. The recent advent of personalized services has lead to the massive collection of personal data and the construction of detailed profiles about users. However, users have no information about the data which constitute its profile and how they are exploited by the different entities (Internet companies, telecom operators, ...). This lack of transparency gives rise to ethical issues such as discrimination or unfair processing.

In this associate team, we propose to strengthen the complementary nature and the current collaborations between the Inria Privatics group and UQAM to advance research and understanding on data and the algorithmic transparency and accountability.

7.5. International Research Visitors

7.5.1. Visits of International Scientists

- Jeremy Decouchant (University of Luxembourg) visited Privatics from 14/10/2019 to 25/10/2019 through the Erasmus Staff Mobility For Teaching program. During the visit, Jeremie Decouchant participated in network programming lectures and practical sessions at the INSA Lyon engineering school at the M1 level. In addition, the existing scientific collaborations with the team have been also extended around the usage of Intel Software Guard Extensions (SGX) to implement a privacy-preserving recommendation systems and genome studies.
- Gergely Acs, assistant professor at Budapest University (Hungary), visited our team in June. He worked together with Claude Castelluccia on the security and privacy of Federated machine learning.
- Rosin Claude Ngueveu (UQAM) visited the team in Lyon in July 2019 for two weeks to increase the DATA collaboration. During the visit, Rosin Claude Ngueveu presented joint work at APVP 2019 and advanced existing collaboration to include fairness in our work on protection of motion sensor data.

8. Dissemination

8.1. Promoting Scientific Activities

8.1.1. Scientific Events Organisation

8.1.1.1. General Chair, Scientific Chair

Antoine Boutet: Workshop on data transparency, 10/10/2018, Lyon, France.

Claude Castelluccia: *AI & Information Disorder* as part of the Global Forum on AI for Humanity forum, October 2019, Paris, France.

8.1.1.2. Member of the Organizing Committees

Antoine Boutet: Workshop on data transparency, 10/10/2019, Lyon, France.

Antoine Boutet: Winter School on Distributed Systems and Networks 2019, 4-8/02/2019, Sept Laux, France.

Antoine Boutet: SRDS 2019, 01-04/10/19 Lyon, France.

Daniel Le Métayer: Panel *Influence or manipulation? What protections in the digital world?*, CPDP 2019, 30/01/2019, Brussels, Belgium.

Claude Castelluccia, *Building trust in AI, building trust with AI*, Global Science Week, 01/06/2019, Grenoble, France.

8.1.2. Scientific Events Selection

8.1.2.1. Member of the Conference Program Committees

Antoine Boutet: Social Network Analysis and Mining 2019, Nature 2019, MDPI 2019, IEEE Transactions on Services Computing 2019, APVP 2019, Compas 2019, Location Privacy Workshop 2019.

Mathieu Cunche: ACM WiSec 2019, APVP 2019, AlgoTel 2019, IEEE WCNC 2019.

Claude Castelluccia: APF 2019.

Cédric Lauradoux: ACM CCSW 2019, Prix Gilles Kahn.

Daniel Le Métayer: XAI 2019, IWPE 2019, CPDP 2019, APF 2019.

Vincent Roca: SPACOMM 2019.

8.1.3. Invited Talks

Claude Castelluccia, *A Risk Analysis Framework for Facial Recognition Applications*, MIAI chair on AI&Ethics (T. Menissier), 04/12/2019, Grenoble, France.

Claude Castelluccia, *Cognitive security*, closing the regulatory gap for consumer neurotechnology" workshop, Brocher Fondation, 25-27/11/2019, Geneva, Switzerland.

Claude Castelluccia, *Influence or manipulation ? What protections in the digital world? (panel)*, CPDP 2019, 30/01/2019, Brussels, Belgium.

Cédric Lauradoux, *Subject Access Request and Proof of Ownership*, SoSySec Seminar, 25/10/2019, Rennes, France.

Cédric Lauradoux, *Influence or manipulation ? What protections in the digital world? (panel)*, CPDP 2019, 30/01/2019, Brussels, Belgium.

Cédric Lauradoux, *Y-aura-t-il un Cambridge Analytica de nos data santé ? (panel)*, FUTUR.E.S, 13/06/2019, Paris, France.

Cédric Lauradoux, *Pseudonymisation*, École de Cybersécurité de l'Université de Nice, 09/07/2019, Nice, France.

Cédric Lauradoux, *Subject Access Right*, Laboratoire d'Innovation Numérique de la CNIL, 12/07/2019, Paris, France.

Cédric Lauradoux, *Subject Access Request and Proof of Ownership*, CyberAlps Workshop on GDPR, 09/10/2019, Grenoble, France.

Daniel Le Métayer, *Inaugural session: How to promote a responsable design and usage of decision making systems ?* , Center for Internet and Society, 27/09/2019, Paris, France.

Daniel Le Métayer and Clément Hénin *Social Responsability of Algorithms*, SRA 2019, 12/12/2019, Paris, France.

Daniel Le Métayer, *HumanAI*, workshop on transparency and accountability for algorithmic decision systems, 11/09/2019, Montreal, Canada.

Mathieu Cunche, *Mécanismes anti-traçage dans les réseaux sans-fil*, journées nationales du GDR sécurité 2019, 12/06/19, Paris, France.

Vincent Roca, *Vers un habitat intelligent... mais fortement indiscret : la maison connectée sous l'angle de la vie privée*, Séminaire "Vie privée, mobile et sécurité", Festival des Libertés Numériques, 06/02/2019, Rennes, France.

8.2. Teaching - Supervision - Juries

8.2.1. Teaching

Master : Antoine Boutet, *Security and Privacy*, 14h, INSA-Lyon, France.

Master : Antoine Boutet, *Security and Privacy 16h*, Polytech Annecy, France.

Undergraduate course: Antoine Boutet, *System and Network*, 160h, L3, INSA-Lyon, France.

Master: Antoine Boutet, *Network, 24h*, Polytech Annecy, France.

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

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

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

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

Master : Mathieu Cunche, *Privacy and Data protection*, 14h, M2, INSA-Lyon, France.

Master : Mathieu Cunche, *Cryptography and Communication Security*, 18h, M1, INSA-Lyon, France.

Master : Cédric Lauradoux, *Advanced Topics in Security*, 20h, M2, Ensimag/INPG, France.

Master : Cédric Lauradoux, *Systems and Network Security*, 30h, M1, Ensimag, France.

Master : Cédric Lauradoux, *Internet Security*, 12h, M2, University of Grenoble Alpes, France.

Master : Cédric Lauradoux, *Cyber Security*, 3h, M2, Laws School of University of Grenoble Alpes, France.

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

Master : Claude Castelluccia, *Cyber Security*, 6h, M2, Laws School of University of Grenoble Alpes, France.

Master : Claude Castelluccia, *Data Privacy*, 6h, M2, Laws School of University of Grenoble Alpes, France.

Master : Daniel Le Métayer, *Privacy*, 12h, M2 MASH, Université Paris Dauphine, France.

Master : Daniel Le Métayer, *Privacy*, 12h, M2, Insa Lyon, France.

Master : Vincent Roca, *On Wireless Communications*, 12h, M1, Polytech' Grenoble, France.

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

Undergraduate course : Vincent Roca, *On Security and Privacy in smartphones*, 3h, L-Pro, University of Grenoble Alpes, France.

Undergraduate course : Vincent Roca, *C-Language Programming*, 24h, L-Pro, University of Grenoble Alpes, France.

Master : Vincent Roca, *On Security and Privacy in smartphones*, 3h, M2, France.

8.2.2. E-learning

MOOC "Protection de la vie privée dans le monde numérique:"

Nataliia Bielova, Cédric Lauradoux, Vincent Roca, Session 3, (open during 2 months), FUN-MOOC, Inria, public targeted: around 30000 for the three sessions since 2018, https://www.fun-mooc.fr/courses/course-v1:inria+41015+session03/about.

8.2.3. Supervision

- PhD in progress : Victor Morel, *IoT privacy*, September 2016, Daniel Le Métayer and Claude Castelluccia.
- PhD in progress : Mathieu Thiery, *IoT privacy* , April 2017, Vincent Roca with Arnaud Legout (DIANA Inria team).
- PhD in progress : Guillaume Celosia, *Wireless Privacy in the Internet of Things* , November 2017, Mathieu Cunche and Daniel Le Métayer.
- PhD in progress : Supryia Adhatarao, *Privacy of E-learning systems* , March 2018, Cédric Lauradoux.
- PhD in progress : Coline Boniface, *Cyberweapons: from bug bounties to zero days* , March 2018, Cédric Lauradoux.
- PhD in progress : Raoul Kerkouche, *Privacy-Preserving Processing of Medical Data* , January 2018, Claude Castelluccia.
- PhD in progress : Clement Henin, *Explainable AI* , September 2018, Claude Castelluccia et Daniel Le Métayer.
- PhD in progress: Théo Jourdan, *Privacy-preserving machine learning in medical domain, October 2018, Antoine Boutet.*
- *PhD in progress : Michale Toth,* Privacy protection of Web users and compliance with GDPR and ePrivacy Regulations *, December 2019, Natallia Bielova and Vincent Roca.*
- *Intern (M2): Michael Toth ,* Analyse et présentation accessible aux utilisateurs de Chartes de Vie Privée dans le contexte du RGPD, Vincent Roca.
- Intern (M2): Piyush Patil, *Privacy Leak Analysis in the Context of Smart Homes, Vincent Roca.*

- *Intern (M1): Jan Aalmoes - Understanding how location data influences personalized content in the mobile context, Antoine Boutet.*
- *Intern (M1): Vincent Prax - Privacy Analysis of Email Providers, Cédric Lauradoux.*
- *Intern (L3): Félix Fonteneau - Activity recognition using federated learning, Antoine Boutet.*
- *Intern (L3): Hilaire Bouaddi - Analysis of mobility traces, Antoine Boutet.*
- *Intern (L3): Amine Bahi - Privacy-preserving and scalable machine learning using homomorphic encryption, Antoine Boutet.*

8.2.4. Juries

HDR: Carole Frindel, *Approche computationnelle de l'imagerie médicale : application en neurosciences*, INSA Lyon, France, 13/12/2019, Claude Castelluccia.

PhD: Pieter Robyns, *Explicit and Implicit Information Leakage in Wireless Communication*, 11/12/19, Hasselt University, Belgium, Mathieu Cunche (reviewer).

PhD: Timothy CLAEYS, *Security for the Internet of Things: A bottom-up approach to the secure and standardized Internet of Things*, 19/12/19, Université de Grenoble Alpes, France, Mathieu Cunche (examiner).

PhD: Antoine Vastel, *Tracking versus security: investigating the two facets of browser fingerprinting*, Université de Lille, France, 23/10/2019, Daniel Le Métayer.

PhD: Julien Loudet, *Distributed and privacy-preserving personal queries on personal clouds*, Universitée Paris-Saclay, thèse préparée à Université de Versailles Saint-Quentin-en-Yvelines, 24/10/2019, France, Vincent Roca (reviewer).

8.3. Popularization

8.3.1. Hearings

- Claude Castelluccia: *audition at the Council of Europe on AI & Human Rights*, European Parliament, 05/2019, Paris, France.

8.3.2. Internal or external Inria responsibilities

- Claude Castelluccia is co-leader of the Worpackage 5 (data governance and privacy) of the Grenoble Data Institute.
- Claude Castelluccia is co-leader of Grenoble CyberAlps (cybersecurity institute of Grenoble).
- Claude Castelluccia is a member of the Grenoble AI institute (MIAI)
- Daniel Le Métayer is a member of the European Commission Multistakeholder expert group to support the application of General Data Protection Regulation (GDPR).
- Daniel Le Métayer is Chair of the CNIL-Inria privacy award.
- Daniel Le Métayer is a member of the steering committee of APVP (Atelier Protection de la Vie Privée).
- Daniel Le Métayer is a member of the steering committee of the chair « Transformation de l'action publique » of Sciences Po Lyon.
- Antoine Boutet is the communication manager of CITI laboratory.
- Antoine Boutet is the manager the Cybersecurity and privacy option of the 5th year of computer science at INSA-Lyon.
- Cédric Lauradoux is a representative of Inria ethical committee COERLE at Inria Grenoble Rhone-Alpes.
- Cédric Lauradoux is a member of the scientific committee of the research action "Cyber-Physical System" of Labex Persyval (Grenoble).

- Cédric Lauradoux is a member of the ethics committee of ComUE Université Grenoble Alpes.
- Cédric Lauradoux is a member of Inria Grenoble Rhône-Alpes committee for technological development.
- Vincent Roca is the PRIVATICS Team Leader (since Nov. 2020).
- Vincent Roca is the co-chair of the NWCRG ("Coding for Efficident Network Communications" Research Group), Internet Research Task Force (IRTF) / IETF.
- Vincent Roca is the ANR 2017 DAPCODS/IOTics project leader.
- Vincent Roca is the chair of the CUMI ("Commision des Utilisateurs des Moyens Informatiques") of Inria Grenoble Rhone-Alpes.
- Vincent Roca is a member of Inria ethical committee COERLE.
- Vincent Roca is co-editor (with Ludovic Mé and Steve Kremer) of a series of articles dedicated to cybersecurity on the Blog Binaire, Le Monde.

8.3.3. Articles and contents

- Antoine Boutet et Mathieu Cunche: *Souriez, vous êtes géolocalisés !*, "Tout compte fait", 06/05/2019
- Antoine Boutet: *L'algorithme : cette formule arbitraire, miroir de l'intention humaine*, En Vue (INSA Lyon newsletter), 18/12/2019 .
- Claude Castelluccia: *Manipulation informationnelle et psychologique*, Le blog binaire du Monde, 05/2018.
- Mathieu Cunche: *Des chercheurs français découvrent des fuites d'informations sensibles sur les appareils Apple*, Science et Avenir.fr, 16/12/2019.
- Mathieu Cunche, *Vers une reconnaissance faciale généralisée*, Techniques de l'ingénieur, 05/12/2019.
- Cédric Lauradoux, *Bientot un identifiant numérique pour tous*, Les Echos, 07/05/2019.
- Cédric Lauradoux, *Facebook, mon fil d'actu, ma bataille*, Mediapart, 05/12/2019.
- Daniel Le Métayer and Claude Castelluccia: *Algorithmic decision making : risks and opportunities for society*, Inria Interview, 25/06/2019.
- Daniel Le Métayer: *Interview about algorithmic decision systems.*, Atlantico, 21/09/2019.
- Vincent Roca and Cédric Lauradoux: *Prêts à tout pour protéger leurs données*, 01NET, 02/10/2019.
- Vincent Roca: *Suite au Livre Blanc Inria sur la cybersécurité : L'ordinateur quantique est une menace pour une partie des techniques de chiffrement actuellement utilisée*, L'Hebdo, BFM Business, 09/02/2019.
- Vincent Roca: *Les objets connecte´s nous espionnent-ils ?*, "Les Idées Claires", France Culture, 12/03/2019.
- Vincent Roca: *Rencontre Sciences et Politique : Cybersécurité*, Acade´mie des sciences - Acade´mie nationale de me´decine - Office parlementaire d'e´valuation des choix scientifiques et technologiques (OPECST), Sénat, 19/06/2019.
- Vincent Roca: *Objets connectés et vie privée*, Les Echos, 20/03/2019.
- Vincent Roca: *Nouvelles technologies : tous espionnés*, Journal de 20 Heures, France 2, 12/04/2019.
- Vincent Roca: *Vie privée et maison intelligente*, Café des Sciences, 14/05/2019, Grenoble, France.

8.3.4. Education

- Nataliia Bielova: *Animation du forum du MOOC Protection de la vie privée dans le monde numérique*, May-June 2019.
- Antoine Boutet: Contest of data anonymization between three different groups of INSA students (from Lyon and Bourges), 25-26/11/19.

- Cédric Lauradoux: *Action vie privée*, Maison pour la science, 14/02/2019, Grenoble, France.
- Cédric Lauradoux: *Protéger sa vie privée*, DIU EIL (enseignant d'informatique au lycée), 12/04/2019, Grenoble, France.
- Cédric Lauradoux: *Animation du forum du MOOC Protection de la vie privée dans le monde numérique*, May-June 2019.
- Vincent Roca: : *Animation du forum du MOOC Protection de la vie privée dans le monde numérique*, May-June 2019.

8.3.5. Interventions

- Mathieu Cunche: *Cybersécurité: Protéger ses objets physiques*, Pint of science, 22/05/2019, Lyon, France.
- Cédric Lauradoux: *Procès du robot 42*, Festival TRANSFO, 24/01/2019, Grenoble, France.
- Cédric Lauradoux: *Challenges de cryptologie*, Printemps du numérique, 08/04/19, Die, France.
- Cédric Lauradoux: *Challenges de cryptologie*, MathC2+ internship, 25/06/19, Grenoble, France.
- Cédric Lauradoux: *Atelier cryptographie*, Fête de la Science, 10/10/2019, Grenoble, France.
- Cédric Lauradoux: *Procès du robot 42*, Fête de la Science, 12/10/2019, Grenoble, France.
- Cédric Lauradoux: *Les données en question*, Festival Imaginascience, 16/10/2019, Annecy, France.
- Cédric Lauradoux: *Le Numérique nous menace-t-il ?*, Telecom Saint Etienne, 03/12/2019, Saint Etienne, France.
- Cédric Lauradoux: *Vie privée et Liberté dans le monde numérique*, Collège Les Dauphins, 03/12/2019, Saint Jean de Soudain, France.
- Cédric Lauradoux: *Challenges de cryptologie*, Cité scolaire Jean PREVOST, 12/12/2019, Villard de Lans, France.
- Cédric Lauradoux: *Avoir un usage Internet éclairé*, UIAD, 18/12/2019, Grenoble, France.
- Vincent Roca: *Maison intelligente : le point de vue du respect de la vie privée*, Café des Sciences, 14/05/2019, Grenoble, France.
- Vincent Roca: *Habitat intelligent, service de vélo partagé et vie privée*, Fête de la Science, 12/10/2019, Grenoble, France.

8.3.6. Internal action

- Cédric Lauradoux: *Formation Éthique*, Inria Paris, 26/01/2019, Paris, France.
- Cédric Lauradoux: *Formation Éthique*, Inria Saclay, 25/04/2019, Saclay, France.
- Cédric Lauradoux: *Formation Éthique*, Inria Grenoble - Rhône-Alpes, 13/05/2019, Lyon, France.
- Cédric Lauradoux: *Rules of Cyber Engagement*, Inria JSI, 07/06/2019, Lyon, France.
- Cédric Lauradoux: *Privacy: Understanding the GDPR*, Inria Grenoble - Rhône-Alpes, 15/10/2019, Grenoble, France.
- Vincent Roca: *Sécurité numérique : technique, éthique, juridique : qui s'y frotte s'y pique (moderator)*, Inria JSI, 07/06/2019, Lyon, France.

9. Bibliography

Publications of the year

Articles in International Peer-Reviewed Journals

[1] G. ACS, L. MELIS, C. CASTELLUCCIA, E. DE CRISTOFARO. *Differentially Private Mixture of Generative Neural Networks*, in "IEEE Transactions on Knowledge and Data Engineering", June 2019, vol. 31, n^{o} 6, pp. 1109-1121, A shorter version of this paper appeared at the 17th IEEE International Conference on Data Mining (ICDM 2017). This is the full version, publishedin IEEE Transactions on Knowledge and Data Engineering (TKDE) [*DOI :* 10.1109/TKDE.2018.2855136], https://hal.inria.fr/hal-01921923

[2] G. CELOSIA, M. CUNCHE. *Discontinued Privacy: Personal Data Leaks in Apple Bluetooth-Low-Energy Continuity Protocols*, in "Proceedings on Privacy Enhancing Technologies", July 2020, vol. 2020, pp. 26 - 46 [*DOI :* 10.2478/POPETS-2020-0003], https://hal.inria.fr/hal-02394619

[3] T. JOURDAN, A. BOUTET, C. FRINDEL. *Vers la protection de la vie privée dans les objets connectés pour la reconnaissance d'activité en santé*, in "Revue des Sciences et Technologies de l'Information - Série TSI : Technique et Science Informatiques", 2019, pp. 1-27, forthcoming [*DOI :* 10.3166/RIA.28.1-27], https://hal.inria.fr/hal-02421854

International Conferences with Proceedings

[4] C. BONIFACE, I. FOUAD, N. BIELOVA, C. LAURADOUX, C. SANTOS. *Security Analysis of Subject Access Request Procedures How to authenticate data subjects safely when they request for their data*, in "APF 2019 - Annual Privacy Forum", Rome, Italy, June 2019, pp. 1-20, https://hal.inria.fr/hal-02072302

[5] A. BOUTET, S. GAMBS. *Demo: Inspect what your location history reveals about you Raising user awareness on privacy threats associated with disclosing his location data*, in "CIKM 2019 - 28th ACM International Conference on Information and Knowledge Management", Beijing, China, ACM, November 2019, pp. 2861-2864 [*DOI :* 10.1145/3357384.3357837], https://hal.inria.fr/hal-02421828

[6] G. CELOSIA, M. CUNCHE. *Fingerprinting Bluetooth-Low-Energy Devices Based on the Generic Attribute Profile*, in "IoT S&P 2019 - 2nd International ACM Workshop on Security and Privacy for the Internet-of-Things", London, United Kingdom, ACM Press, November 2019, pp. 24-31 [*DOI :* 10.1145/3338507.3358617], https://hal.inria.fr/hal-02359914

[7] G. CELOSIA, M. CUNCHE. *Saving Private Addresses: An Analysis of Privacy Issues in the Bluetooth-Low-Energy Advertising Mechanism*, in "MobiQuitous 2019 - 16th EAI International Conference on Mobile and Ubiquitous Systems: Computing, Networking and Services", Houston, United States, December 2019, pp. 1-10 [*DOI :* 10.1145/3360774.3360777], https://hal.inria.fr/hal-02394629

[8] M. CUNCHE, D. LE MÉTAYER, V. MOREL. *A Generic Information and Consent Framework for the IoT*, in "TRUSTCOM 2019 - 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications", Rotorua, New Zealand, August 2019, pp. 1-8, https://hal.inria.fr/hal-02166181

[9] J. DECOUCHANT, A. BOUTET, J. YU, P. ESTEVES-VERISSIMO. *P3LS: Plausible Deniability for Practical Privacy-Preserving Live Streaming*, in "SRDS 2019 - 38th International Symposium on Reliable Distributed Systems", Lyon, France, October 2019, pp. 1-10, https://hal.inria.fr/hal-02421820

[10] A. KASSEM, G. ACS, C. CASTELLUCCIA, C. PALAMIDESSI. *Differential Inference Testing: A Practical Approach to Evaluate Sanitizations of Datasets*, in "SPW 2019 - 40th IEEE Symposium on Security and Privacy Workshops", San Francisco, United States, IEEE, May 2019, pp. 72-79 [*DOI :* 10.1109/SPW.2019.00024], https://hal.archives-ouvertes.fr/hal-02422992

[11] R. PARDO, D. LE MÉTAYER. *Analysis of Privacy Policies to Enhance Informed Consent*, in "DBSEC 2019 - 33rd Annual IFIP WG 11.3 Conference on Data and Applications Security and Privacy", Charleston, SC, United States, S. N. FOLEY (editor), Data and Applications Security and Privacy XXXIII, Springer International Publishing, July 2019, vol. LNCS-11559, pp. 177-198, Part 3: Privacy [*DOI :* 10.1007/978-3-030-22479-0_10], https://hal.inria.fr/hal-02384593

Scientific Books (or Scientific Book chapters)

[12] S. KREMER, L. MÉ, D. RÉMY, V. ROCA. *Cybersecurity : Current challenges and Inria's research directions*, Inria white book, Inria, January 2019, n° 3, 172 p. , https://hal.inria.fr/hal-01993308

[13] S. KREMER, L. MÉ, D. RÉMY, V. ROCA. *Cybersécurité : Défis actuels et axes de recherche à l'Inria*, Inria white book, Inria, May 2019, n° 3, 18 p. , https://hal.inria.fr/hal-02414281

Research Reports

[14] C. CASTELLUCCIA, D. LE MÉTAYER. *Analyse des impacts de la reconnaissance faciale - Quelques éléments de méthode*, Inria Grenoble Rhône-Alpes, November 2019, https://hal.inria.fr/hal-02373093

[15] C. HENIN, D. LE MÉTAYER. *Towards a Generic Framework for Black-box Explanation Methods (Extended Version)*, Inria Grenoble Rhône-Alpes ; Ecole des Ponts ParisTech, May 2019, n° RR-9276, pp. 1-28, https://hal.inria.fr/hal-02131174

[16] V. MOREL, R. PARDO. *Three Dimensions of Privacy Policies*, Inria - Research Centre Grenoble – Rhône-Alpes ; CITI - CITI Centre of Innovation in Telecommunications and Integration of services, August 2019, n° RR-9287, https://arxiv.org/abs/1908.06814 , https://hal.inria.fr/hal-02267641

[17] R. PARDO, D. LE MÉTAYER. *Analysis of Privacy Policies to Enhance Informed Consent (Extended Version)*, Inria Rhône-Alpes, March 2019, n° RR-9262, pp. 1-22, https://arxiv.org/abs/1903.06068 - Extended Version, https://hal.inria.fr/hal-02067924

Other Publications

[18] G. AVOINE, C. LAURADOUX, T.-R. ROLANDO. *Should Chess Players Learn Computer Security ?*, February 2019, pp. 1-11, HACKING IT SECURITY MAGAZINE, https://hal.inria.fr/hal-02082837

[19] G. CELOSIA, M. CUNCHE. *DEMO: Himiko: A human interface for monitoring and inferring knowledge on Bluetooth-Low-Energy objects*, ACM Press, May 2019, pp. 292-293, WiSec 2019 - 12th Conference on Security and Privacy in Wireless and Mobile Networks, Poster [*DOI :* 10.1145/3317549.3326297], https://hal.inria.fr/hal-02154148

[20] V. ROCA, A. BEGEN. *Forward Error Correction (FEC) Framework Extension to Sliding Window Codes (RFC 8680)*, RFC Editor (https://www.rfc-editor.org/), January 2020, RFC 8680, Standards Track, TSVWG (Transport Area) working group of IETF (Internet Engineering Task Force), https://www.rfc-editor.org/rfc/rfc8680.html, https://hal.inria.fr/hal-01345125

[21] V. ROCA, B. TEIBI. *Sliding Window Random Linear Code (RLC) Forward Erasure Correction (FEC) Schemes for FECFRAME (RFC 8681)*, RFC Editor (https://www.rfc-editor.org/), January 2020, RFC 8681, Standards Track, TSVWG (Transport Area) working group of IETF (Internet Engineering Task Force), https://www.rfc-editor.org/rfc/rfc8681.html, https://hal.inria.fr/hal-01630089

[22] M. SAITO, M. MATSUMOTO, V. ROCA, E. BACCELLI. *TinyMT32 Pseudorandom Number Generator (PRNG) (RFC 8682)*, RFC Editor (https://www.rfc-editor.org/), January 2020, RFC 8682, Standards Track, TSVWG (Transport Area) working group of IETF (Internet Engineering Task Force), https://www.rfc-editor.org/rfc/rfc8682.html, https://hal.inria.fr/hal-02449210

[23] M. THIERY, V. ROCA, A. LEGOUT. *Privacy implications of switching ON a light bulb in the IoT world*, July 2019, working paper or preprint, https://hal.inria.fr/hal-02196544