RESEARCH CENTRE

Grenoble - Rhône-Alpes

2021 ACTIVITY REPORT

Project-Team PRIVATICS

Privacy Models, Architectures and Tools for the Information Society

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

DOMAIN

Algorithmics, Programming, Software and Architecture

THEME

Security and Confidentiality

Contents

Project-Team PRIVATICS

Creation of the Project-Team: 2014 July 01

Keywords

Computer sciences and digital sciences

A1.2.5. – Internet of things

A1.3.1. – Web

A4.8. – Privacy-enhancing technologies

A9.2. – Machine learning

Other research topics and application domains

B2.3. – Epidemiology

B6. – IT and telecom

B6.2.2. – Radio technology

B6.3.1. – Web

B6.3.2. – Network protocols

B6.3.4. – Social Networks

B6.4. – Internet of things

B6.6. – Embedded systems

B7.2. – Smart travel

B7.2.1. – Smart vehicles

B7.2.2. – Smart road

B8.1.2. – Sensor networks for smart buildings

B8.2. – Connected city

B9.1.1. – E-learning, MOOC

B9.5.6. – Data science

B9.6.2. – Juridical science

B9.9. – Ethics

B9.10. – Privacy

1 Team members, visitors, external collaborators

Research Scientists

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

Faculty Members

- Antoine Boutet [INSA Lyon, Associate Professor]
- Mathieu Cunche [INSA Lyon, Associate Professor, HDR]

Post-Doctoral Fellow

- Mohamed Maouche [Ecole de l'aménagement durable des territoires, From Dec 2021, co-supervised post-doc)]

PhD Students

- Jan Aalmoes [INSA Lyon, from Sep 2021]
- Supriya Sreekant Adhatarao [Inria, until Jun 2021]
- Coline Boniface [Univ Grenoble Alpes (until Nov 2021) then Inria (until Apr 2022)]
- Imane Fouad [Inria, until Sep 2021]
- Clement Henin [Ministère de l'Ecologie, de l'Energie, du Développement durable et de la Mer, until Aug 2021]
- Theo Jourdan [INSERM, until Oct 2021]
- Raouf Kerkouche [Univ Grenoble Alpes, until Jun 2021]
- Suzanne Lansade [Inria]
- Thomas Lebrun [Inria, from Oct 2021]
- Samuel Pelissier [INSA Lyon, from Sep 2021]
- Michael Toth [Inria]

Technical Staff

- Jan Aalmoes [INSA Lyon, Engineer, from Jun 2021 until Jul 2021]
- Adrien Baud [Inria, Engineer, until Sep 2021]
- Thomas Lebrun [Inria, Engineer, from Apr 2021 until Sep 2021]

Interns and Apprentices

- Jan Aalmoes [INSA Lyon, from Feb 2021 until May 2021]
- Julien Bracon [Inria, from May 2021 until Aug 2021]
- Brandon Da Silva Alves [INSA Lyon, from Jun 2021 until Aug 2021]
- Yann Lafaille [INSA Lyon, from May 2021 until Aug 2021]
- Sophanna Ngov [INSA Lyon, from Jun 2021 until Aug 2021]
- Tom Perrillat Collomb [INSA Lyon, from Jun 2021 until Aug 2021]
- Son Tung Tran [INSA Lyon, from Jun 2021 until Aug 2021]
- Valeria Valdes Rios [Inria, from Sep 2021 until Nov 2021]
- Sylvain Vaure [Inria, from May 2021 until Aug 2021]

Administrative Assistant

- Helen Pouchot-Rouge-Blanc [Inria]

External Collaborator

- Cristiana Teixeira Santos [Université d'Utrecht - Pays bas, 2021]

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.

3 Research program

Privacy is essential to protect individuals, but also to protect the society, for instance to avoid the misuse of personal data to surreptitiously manipulate individuals in elections. In this context, the PRIVATICS team carries out a broad range of research activities: some of them aim at understanding the domain and its evolution, both from the theoretical and practical viewpoints, while others aim at designing privacy-enhancing tools and systems.

Examples of the PRIVATICS team research activities, always with privacy as a common denominator, include: federated machine learning; explainability of automatic decision making systems; user manipulation through dark patterns; identification and protection against web tracking; privacy leaks in IoT, smartphone applications and wireless networks; PDF document sanitization; privacy in digital health tools; digital contact tracing in the TousAntiCovid system; legal considerations in privacy; societal considerations, for instance in the context of video-surveillance systems; and theoretical foundations for privacy, for instance with formal languages for privacy policies.

The domain of privacy and personal data protection is clearly fundamentally multifacted, from scientific and technical aspects to legal, economic, sociological, ethic and cultural aspects. Whenever it makes sense, PRIVATICS will continue to favor interdisciplinarity, through collaborations with colleagues from other disciplines.

4 Application domains

4.1 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 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.

4.2 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 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 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.

5 Social and environmental responsibility

5.1 Environmental impacts of research results

The activities of PRIVATICS are not directly related to environmental considerations. However, promoting privacy in a connected world sometimes leads us to promote local data processing, as opposed to massive data collection and big data (e.g., in the case of Internet of Things systems). From this point of view, we believe that our research results are aligned with environmental considerations.

5.2 Societal impacts of research results

Several of PRIVATICS works had major societal impacts. One can cite:

- The ROBERT Exposure Notification Protocol and the CLEA Cluster Exposure Verification Protocol, both of them being at the core of the StopCovid/TousAntiCovid application;
- The work on tracking technologies and the use of consent banners in web browsers. This work helped revealing practices in the field, sometimes highlighting illegal practices, and therefore it helped promoting a more privacy friendly society;
- The popular *"Protection de la vie privée dans le monde numérique"* Massive Online Course (MOOC) on the FUN platform;

Additionally, several PRIVATICS members are part of several ethical committees:

- Vincent Roca is member of the Inria COERLE (commité d'évaluation des risques légaux et éthiques);

- Cédric Lauradoux represents the Inria COERLE (commité d'évaluation des risques légaux et éthiques) in the Grenoble research center, helping local researchers to fill in their application form;
- Cédric Lauradoux is member of the University of Grenoble Alps (UGA) ethical committee;
- Mathieu Cunche is member of *Comité d'éthique de la recherche (CER)* of Lyon University.

6 Highlights of the year

6.1 Awards and distinctions

- Nomination as Knight of the "Ordre National du Mérite" for Claude Catelluccia and Vincent Roca: During the ceremony, Jean-Pierre Verjus congratulated them as well as all the members of the PRIVATICS team for their commitment to the TousAntiCovid project. Inria news.
- IEEE Standards Association "Certificate of Appreciation for outstanding contributions" granted to Mathieu Cunche, as an acknowledgment of his contributions to the development of IEEE Standard 802E 2020, IEEE Recommended Practice for privacy considerations for IEEE 802 technologies.

6.2 PhD and HDR defenses of the year

In 2021 **five** PRIVATICS students brillantly defended their PhD on topics ranging from Federated ML, ML for digital health, web tracking, personal data leaks in PDF documents, understandability and accountability of automated decision systems (AKA algorithms).

Additionally, **Nataliia Bielova and Mathieu Cunche** brillantly defended their HDR in June 2021, respectively entitled:
"Protecting Privacy of Web Users"
and:
"Privacy issues in wireless networks - Every frame you send, they'll be watching you".

6.3 PRIVATICS working more and more with the CNIL

In 2021, two PRIVATICS permanent researchers joined the French Data Protection Agency (DPA), CNIL:

- On July 23, 2021, Claude Castelluccia was appointed commissioner of the CNIL in order to reinforce the CNIL competence in computer science. Inria news
- On September 2021, Nataliia Bielova joined the CNIL's Digital Innovation Laboratory (LINC) as a Senior Privacy Fellow for one year. CNIL news

These two nomminations are great achievements that highlight the quality of their competences and contributions to the domain of privacy and data protection.

6.4 The CLEA presence tracing protocol added to TousAntiCovid

The CLuster Exposure verificAtion (CLEA) protocol, designed by the PRIVATICS team, has been added on June 9th, 2021 to the TousAntiCovid French app, adding presence tracing features to the set of services already provided, including the initial ROBERT contact tracing service deployed one year earlier on June 2nd, 2020. See the New Results section.

In parallel, the TousAntiCovid app progressively became the most popular app in 2021 in terms of number of donwloads in France, with more than 50 Million first downloads on different devices in the AppStore and PlayStore on January 7th, 2022. On December 28th, 2021, 1 Million TAC users have been notified as being "at risk" thanks to the digital tracing features of the app.

7 New software and platforms

PRIVATICS designed several new softwares and platforms in 2021.

7.1 New software

7.1.1 DÉSIRÉ

Name: DÉSIRÉ: a third way for a European exposure notification system

Keywords: COVID-19, Contact tracing

Functional Description: On April 2020, the PRIVATICS Inria team (FR) and the Fraunhofer (DE) colleagues designed the CNIL-approved ROBERT privacy preserving exposure notification protocol, used by the French StopCovid/TousAntiCovid national app, and available since June 2nd. The PRIVATICS team also designed the DESIRE protocol on May 2020, as an advanced solution.

The present software is a Proof of Concept of the DÉSIRÉ protocol for Android smartphones.

Publication: hal-02570382

Contact: Antoine Boutet

Participants: Adrien Baud, Pierre-Guillaume Raverdy, Christophe Braillon, Antoine Boutet, Mathieu Cunche, Vincent Roca, Claude Castelluccia

7.1.2 ernie

Keywords: Privacy, Web, Plug-in

Functional Description: Ernie is a browser extension (Firefox and Chrome) we designed to visualise six state-of-the-art tracking techniques based on cookies. The goal is to facilitate the detection of tracking based on cookies.

Authors: Vera Wesselkamp, Imane Fouad, Nataliia Bielova, Arnaud Legout

Contact: Arnaud Legout

7.1.3 IBEX Interactive Black box EXplanation

Name: IBEX Interactive Black box EXplanation

Keywords: Algorithm, Explainability, Explainable Artificial Intelligence

Functional Description: Explanations for algorithmic decision systems can take different forms, they can target different types of users with different goals. One of the main challenges in this area is therefore to devise explanation methods that can accommodate this variety of situations. A first step to address this challenge is to allow explainees to express their needs in the most convenient way, depending on their level of expertise and motivation. This IBEX software offers a solution to this problem based on a multi-layered approach allowing users to express their requests for explanations at different levels of abstraction.

Authors: Clément Henin, Daniel Le Metayer

Contact: Vincent Roca

7.1.4 Algocate

Name: Algocate, a tool for justifying and questioning decisions

Keywords: Algorithm, Explainability, Explainable Artificial Intelligence

Functional Description: The possibility of contesting the results of Algorithmic Decision Systems (ADS) is a key requirement for ADS used to make decisions with a high impact on individuals. While the goal of an explanation is to make it possible for a human being to understand, the goal of a justification is to convince that the decision is good or appropriate. To claim that a result is good, it is necessary (1) to refer to an independent definition of what a good result is (the norm), and (2), to provide evidence that the norm applies to the case. Based on these definitions, Algocate is a software that presents a challenge and justification framework including three types of norms.

Authors: Clément Henin, Daniel Le Metayer

Contact: Vincent Roca

7.2 New platforms

PRESERVE (Plate-foRme wEb de SEnsibilisation aux pRoblèmes de Vie privéE):

Participants: Antoine Boutet, Adrien Baud.

This platform aims to raise users' awareness of privacy issues. It aims to be used as a front for several works of the Privatics team as well as for collaborations and actions. The first version implements tools in order to inspect location history. Specifically, this version implements [hal-02421828] where a user is able to inspect the private and sensitive information inferred from its own location data. This platform will be enriched with new functionalities in the future.

8 New results

8.1 The Cluster Exposure Verification (CLÉA) Protocol

Participants: Vincent Roca, Antoine Boutet, Claude Castelluccia.

On March 2021, PRIVATICS proposed the CLuster Exposure verificAtion (CLÉA) protocol, meant to warn the participants of a private event (e.g., wedding or private party) or the persons present in a commercial or public location (e.g., bar, restaurant, sport center) of a risk because a certain number of people who were present at the same time have been tested COVID+ [32]. It is based:

- on a central server, in order to automatically detect potential clusters. This server is under the responsibility of the health authority;
- on the display a QR code at the location or on a ticket, either in a static (e.g., printed) or dynamic manner (e.g., via a dedicated device (e.g., smartphone);
- and on a smartphone application (in our case the TousAntiCovid French official app).

This smartphone application is used to scan a QR code, to store it locally for the next 14 days, and to perform periodic risk analyses, in a decentralized manner, on the smartphone. In order to enable this decentralized risk analysis, information about clusters (i.e., the location pseudonyms and timing information) needs to be disclosed. We believe this is an acceptable downside because this information is not per se sensitive health data (it does not reveal any user health information to an eavesdropper),

although it can be considered as personal data (it is indirectly linked to the location manager). The CLÉA version being deployed is limited to the synchronous scan of a QR code, for situations where a user scans a QR code upon entering an event or location (e.g., a restaurant). Asynchronous scans where the QR code is for instance associated to a transportation or event ticket are not considered.

Finally, the CLÉA protocol is also meant to be used by the location employees in order to warn them if their work place is qualified as cluster, or on the opposite to let them upload information to the server if they are themselves tested COVID+.

Beginning of January 2022, nineteen months after its launch, the TousAntiCovid application has been downloaded more than 50 Million times (making it the most popular app in France ever), registered (required to benefit from contact tracing) more than 40 Million times, 1.5 Million users uploaded their contact proximity, and more than 1.8 Million users have received an "at risk" notification. This success makes the TousAntiCovid app a central component of the French health strategy in the COVID-19 fight, as a multi-service application for the service of the French citizen.

More information: CLEA gitlab repository (specifications and reference implementation), and [8]

8.2 Differentially Private Federated Learning for Bandwidth and Energy Constrained Environments

Participants: Raouf Kerkouche, Claude Castelluccia.

In Machine Learning, several entities may want to collaborate in order to improve their local model accuracy. In traditional machine learning, such collaboration requires to first store all entities' data on a centralized server before training the model on it. Such data centralization might be problematic when the data are sensitive and data privacy is required. Instead of sharing the training data, Federated Learning shares the model parameters between a server, which plays the role of aggregator, and the participating entities. More specifically, the server sends at each round the global model to some participants (downstream). These participants then update the received model with their local data and sends back the updated gradients' vector to the server (upstream). The server then aggregates all the participants' updates to obtain the new global model. This operation is repeated until the global model converges. Although Federated Learning improves privacy, it is not perfect. In fact, sharing gradients computed by individual parties can leak information about their private training data. Several recent attacks have demonstrated that a sufficiently skilled adversary, who can capture the model updates (gradients) sent by individual parties, can infer whether a specific record or a group property is present in the dataset of a specific party. Moreover, complete training samples can also be reconstructed purely from the captured gradients. Furthermore, Federated Learning is not only vulnerable to privacy attacks, it is also vulnerable to poisoning attacks which can drastically decrease the model accuracy. Finally, Federated Learning incurs large communication costs during upstream/downstream exchanges between the server and the parties. This can be problematic for applications based on bandwidth and energy-constrained devices as it is the case for mobile systems, for instance. In this work, we propose three bandwidth efficient schemes to reduce the bandwidth costs up to 99.9

Bibliography: [6]

8.3 DYSAN: Dynamically sanitizing motion sensor data against sensitive inferences through adversarial networks

Participants: Antoine Boutet, Théo Jourdan.

With the widespread adoption of the quantified self movement, an increasing number of users rely on mobile applications to monitor their physical activity through their smartphones. Granting to applications a direct access to sensor data expose users to privacy risks. Indeed, usually these motion sensor data are transmitted to analytics applications hosted on the cloud leveraging machine learning

models to provide feedback on their health to users. However, nothing prevents the service provider to infer private and sensitive information about a user such as health or demographic attributes. In this work, we present DySan, a privacy-preserving framework to sanitize motion sensor data against unwanted sensitive inferences (i.e., improving privacy) while limiting the loss of accuracy on the physical activity monitoring (i.e., maintaining data utility). To ensure a good trade-off between utility and privacy, DySan leverages on the framework of Generative Adversarial Network (GAN) to sanitize the sensor data. More precisely, by learning in a competitive manner several networks, DySan is able to build models that sanitize motion data against inferences on a specified sensitive attribute (e.g., gender) while maintaining a high accuracy on activity recognition. In addition, DySan dynamically selects the sanitizing model which maximize the privacy according to the incoming data. Experiments conducted on real datasets demonstrate that DySan can drasticallylimit the gender inference to 47% while only reducing the accuracy of activity recognition by 3%.

Bibliography: [15]

8.4 DyPS: Dynamic, Private and Secure GWAS

Participant: Antoine Boutet.

Genome-Wide Association Studies (GWAS) identify the genomic variations that are statistically associated with a particular phenotype (e.g., a disease). The confidence in GWAS results increases with the number of genomes analyzed, which encourages federated computations where biocenters would periodically share the genomes they have sequenced. However, for economical and legal reasons, this collaboration will only happen if biocenters cannot learn each others' data. In addition, GWAS releases should not jeopardize the privacy of the individuals whose genomes are used. We introduce DyPS, a novel framework to conduct dynamic privacy-preserving federated GWAS. DyPS leverages a Trusted Execution Environment to secure dynamic GWAS computations. Moreover, DyPS uses a scaling mechanism to speed up the releases of GWAS results according to the evolving number of genomes used in the study, even if individuals retract their participation consent. Lastly, DyPS also tolerates up to all-but-one colluding biocenters without privacy leaks. We implemented and extensively evaluated DyPS through several scenarios involving more than 6 million simulated genomes and up to 35,000 real genomes. Our evaluation shows that DyPS updates test statistics with a reasonable additional request processing delay (11% longer) compared to an approach that would update them with minimal delay but would lead to 8% of the genomes not being protected. In addition, DyPS can result in the same amount of aggregate statistics as a static release (i.e., at the end of the study), but can produce up to 2.6 times more statistics information during earlier dynamic releases. Besides, we show that DyPS can support a larger number of genomes and SNP positions without any significant performance penalty.

Bibliography: [16]

8.5 Privacy Assessment of Federated Learning using Private Personalized Layers

Participants: Antoine Boutet, Théo Jourdan.

Federated Learning (FL) is a collaborative scheme to train a learning model across multiple participants without sharing data. While FL is a clear step forward towards enforcing users' privacy, different inference attacks have been developed. In this work, we quantify the utility and privacy trade-off of a FL scheme using private personalized layers. While this scheme has been proposed as local adaptation to improve the accuracy of the model through local personalization, it has also the advantage to minimize the information about the model exchanged with the server. However, the privacy of such a scheme has never been quantified. Our evaluations using motion sensor dataset show that personalized layers speed up the convergence of the model and slightly improve the accuracy for all users compared to a standard

FL scheme while better preventing both attribute and membership inferences compared to a FL scheme using local differential privacy.

Bibliography: [19]

8.6 Anonymizing motion sensor data through time-frequency domain

Participant: Antoine Boutet.

The recent development of Internet of Things (IoT) has democratized activity monitoring. Even if the data collected can be useful for healthcare, sharing this sensitive information exposes users to privacy threats and re-identification. This work presents two approaches to anonymize the motion sensor data. The first is an ex-tension of an earlier work based on filtering in the time-frequency plane and convolutional neural network; and the second is based on handcrafted features extracted from the zeros distribution of the time-frequency representation. The two approaches are evaluated on a public dataset to assess the accuracy of activity recognition and user re-identification. With the first approach we obtained an accuracy rate in activity recognition of 73% while limiting the identity recognition to an accuracy rate of 30% which corresponds to an activity identity ratio of 2.4. With the second approach we succeeded in improving the activity and identity ratio to 2.67 by attaining an accuracy rate in activity recognition of 80% while maintaining there-identification rate at 30%.

Bibliography: [hal-03354723]

8.7 Multi-layered Approach for Tailored Black-box Explanations

Participants: Clément Henin, Daniel Le Metayer.

Explanations for algorithmic decision systems can take different forms, they can target different types of users with different goals. One of the main challenges in this area is therefore to devise explanation methods that can accommodate this variety of situations. A first step to address this challenge is to allow explainees to express their needs in the most convenient way, depending on their level of expertise and motivation. This work presents a solution to this problem based on a multi-layered approach allowing users to express their requests for explanations at different levels of abstraction. We illustrate the approach with the application of a proof-of-concept system called IBEX to two case studies.

Bibliography: [18]

8.8 Framework to Contest and Justify Algorithmic Decisions

Participants: Clément Henin, Daniel Le Metayer.

In this work, we argue that the possibility of contesting the results of Algorithmic Decision Systems (ADS) is a key requirement for ADS used to make decisions with a high impact on individuals. We discuss the limitations of explanations and motivate the need for better facilities to contest or justify the results of an ADS. While the goal of an explanation is to make it possible for a human being to understand, the goal of a justification is to convince that the decision is good or appropriate. To claim that a result is good, it is necessary (1) to refer to an independent definition of what a good result is (the norm) and (2) to provide evidence that the norm applies to the case. Based on these definitions, we present a challenge and justification framework including three types of norms, a proof-of-concept implementation of this framework and its application to a credit decision system.

Bibliography: [12]

8.9 Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective

Participants: Nataliia Bielova, Cristiana Santos, Michael Toth.

We have set up a collaboration with a legal scholar Cristiana Santos (University of Utrecht, The Netherlands) to understand the gaps and inconsistencies between law and technology – in particular, we set up an interdisciplinary collaboration on GDPR & ePrivacy compliance for consent banners and tracking technologies. Additionally, we have collaborated with the researher in Design/UX, Colin M. Gray (Purdue University, USA) to study how legal and technical requirements for valid consent can be implemented in the design of consent banners.

User engagement with data privacy and security through consent banners has become a ubiquitous part of interacting with inter- net services. While previous work has addressed consent banners from either interaction design, legal, and ethics-focused perspec- tives, little research addresses the connections among multiple disciplinary approaches, including tensions and opportunities that transcend disciplinary boundaries. In this paper, we draw together perspectives and commentary from HCI, design, privacy and data protection, and legal research communities, using the language and strategies of "dark patterns" to perform an interaction criticism read- ing of three different types of consent banners. Our analysis builds upon designer, interface, user, and social context lenses to raise tensions and synergies that arise together in complex, contingent, and conflicting ways in the act of designing consent banners. We conclude with opportunities for transdisciplinary dialogue across legal, ethical, computer science, and interactive systems scholarship to translate matters of ethical concern into public policy.

Bibliography: [17]

8.10 Consent Management Platforms under the GDPR: processors and/or controllers?

Participants: Nataliia Bielova, Cristiana Santos, Michael Toth, Vincent Roca.

Consent Management Platforms under the GDPR: processors and/or controllers? Consen Management Providers(CMPs) provide consent pop- ups that are embedded in ever more websites over time to enable stream- lined compliance with the legal requirements for consent mandated by the ePrivacy Directive and the General Data Protection Regulation (GDPR). They implement the standard for consent collection from the Trans- parency and Consent Framework (TCF) (current version v2.0) proposed by the European branch of the Interactive Advertising Bureau (IAB Europe). Although the IAB's TCF specifications characterize CMPs as data processors, CMPs factual activities often qualifies them as data controllers instead. Discerning their clear role is crucial since compliance obligations and CMPs liability depend on their accurate characteriza- tion. We perform empirical experiments with two major CMP providers in the EU: Quantcast and OneTrust and paired with a legal analysis. We conclude that CMPs process personal data, and we identify multiple scenarios wherein CMPs are controllers.

Bibliography: [33]

8.11 In-Depth Technical and Legal Analysis of Tracking on Health Related Websites with ERNIE Extension

Participants: Nataliia Bielova, Cristiana Santos.

Searching the Web to find doctors and make appointments online is a common practice nowadays. However, simply visiting a doctors website might disclose health related information. As the GDPR only allows processing of health data with explicit user consent, health related websites must ask consent

before any data processing, in particular when they embed third party trackers. Admittedly, it is very hard for owners of such websites to both detect the complex tracking practices that exist today and to ensure legal compliance. In this work, we present ERNIE [38], a browser extension we designed to visualise six state-of-the-art tracking techniques based on cookies. Using ERNIE, we analysed 385 health related websites that users would visit when searching for doctors in Germany, Austria, France, Belgium, and Ireland. More specifically, we explored the tracking behavior before any interaction with the consent pop-up and after rejection of cookies on websites of doctors, hospitals, and health related online phone-books. We found that at least one form of tracking occurs on 62% of the websites before interacting with the consent pop-up, and 15% of websites include tracking after rejection. Finally, we performed a detailed technical and legal analysis of three health related websites that demonstrate impactful legal violations. This work shows that while, from a legal point of view, health related websites are more privacy-sensitive than other kinds of websites, they are exposed to the same technical difficulties to implement a legally compliant website. We believe EX, the browser extension we developed, to be an invaluable tool for policy-makers and regulators to improve detection and visualization of the complex tracking techniques used on these websites.

9 Partnerships and cooperations

Participants: Nataliia Bielova, Antoine Boutet, Claude Castelluccia, Mathieu Cunche, Cédric Lauradoux, Daniel LeMetayer, Vincent Roca.

9.1 International initiatives

Pack Ambition International / Face Foundation TJF

Title: *Trusty IA: Enabling Privacy Preserving in Federated Learning*

Duration: 2021 - *(2023)*

Coordinator: Antoine Boutet

Partners: University de Pennsylvanie

Inria contact: Antoine Boutet

Summary: Federated learning is a promising on-device machine learning scheme and new research topic on privacy-preserving machine learning. Federated learning becomes a paradigm shift in privacy-preserving AI and offers an attractive framework for training large-scale distributed learning models on sensitive data. However, federated learning still faces many challenges to fully preserve data privacy. This project tackles the cybersecurity challenges of federated learning systems in terms of data privacy. Specifically, the goal is to extend different federated learning approaches to consider their limitations in terms of accuracy, confidentiality, robustness, explainability and fairness.

9.1.1 FP7 & H2020 projects

SPARTA

Title: Special projects for advanced research and technology in Europe

Duration: *2019 - 2021*

Coordinator: *COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES (France)*

Partners:

- Commissariat à l'Energie Atomique et aux Energies Alternatives (leader)
- 43 other partners (not listed here), including Inria and INSA.

Summary: SPARTA will launch and execute four Programs validating the operation of the network and performing ground-breaking advances in key areas for Europe's strategic autonomy:

- Full Spectrum Situational Awareness;
- Continuous Assessment in Polymorphous Environments;
- High-Assurance Intelligent Infrastructure Toolkit;
- Secure and Fair AI Systems for Citizen.

9.1.2 Other european programs/initiatives

PIVOT: Privacy-Integrated design and Validation in the constrained IoT

- Type: German-French joint call on cybersecurity - ANR - Bundesministerium für Buildung und Forschung
- Duration: 2021 - 2024
- Coordinator: French coordinator: AFNIC, German coordinator: Freie Universität Berlin
- Others partners: Hamburg Univ of Applied Science, Lobaro Industrial Solutions, INSA Lyon, Inria
- Abstract: The overall objective of the PIVOT project lies in assuring privacy of data and metadata in the Internet of Things (IoT). PIVOT will consider both low-end devices and low-power radio networks of the ultra-constrained IoT. The project will focus on four core goals: 1. A cryptographic framework for privacy-friendly service primitives on ultra-constrained IoT devices; 2. Protocols that integrate decentralized object security; 3. Minimal trust anchor provisioning on IoT devices to enable object security; 4. And multi-stakeholder name management that preserves privacy requirements and generates, allocates, and resolves names globally, regardless of the IoT applications or networks. A demonstrator based on RIOT will verify our solutions in ultraconstrained IoT networks such as LoRaWAN.

9.2 National initiatives

9.2.1 ANR

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).
- 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.

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 .

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 the Internet, citizens became more and more exposed to personal information leakage in their digital lives. This trend begun 20 years ago with the development of Internet. The advent of smartphones, our personal assistant always connected and equipped with many sensors, further reinforced the tendency. Today the craze for quantified-self wearable devices, smart home appliances and more generally connected devices, enable the collection of personal information – sometimes very sensitive – 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 end-user as well as the regulator are therefore prisoner of a highly asymmetric system.

  The IOTics project gathers four research teams working on security, privacy and digital economy, plus the CNIL, the French data protection agency. It focusses on connected devices and follows three directions: the analysis of the internal behavior in terms of personal information leakage of a set of connected devices; the analysis of the privacy policies provided (or not) by the device manufacturers; and the analysis of the underlying ecosystem. By giving transparent information of hidden behaviors, by highlighting good and bad practices, the IOTics project aims at reducing information asymmetry, at giving back control to the end-users and hopefully encouraging stakeholders to change practices.

PMR: Privacy-preserving methods for Medical Research

- Type: ANR
- Duration: 2020 - 2024
- Coordinator: Inria
- Others partners: Inria Magnet, Creatis

- Abstract: Given the growing awareness of privacy risks of data processing, there is an increasing interest in privacy-preserving learning. However, shortcomings in the state of the art limit the applicability of the privacy-preserving learning paradigm. First, most approaches assume too optimistically a honest-but-curious setting. Second, most approaches consider one learning task in isolation, not accounting for the context where querying is a recurring activity. In this project, we will investigate new algorithms and models that address these shortcomings. Among others, (i) our algorithms will combine privacy-preserving properties of differential privacy with security offered by cryptography and (ii) based on models of information flows in integrated data handling processes, we will build more refined models analyzing the implications of repeated querying. We will demonstrate the utility of our new theory and algorithms by proposing strategies to realistically apply them in significant real-world problems illustrated through use cases in the medical domain.

PrivaWEB: Privacy Protection and ePrivacy Compliance for Web Users

- Type: ANR JCJC
- Duration: 2018 - 2023
- Coordinator: Inria
- Abstract: PrivaWEB aims at developing new methods for detection of advanced Web tracking technologies and new tools to integrate in existing Web applications that seamlessly protect privacy of users. In this project, we will integrate three key components into Web applications: privacy, compliance and usability. Our research will address methodological aspects (designing new detection methods and privacy protection mechanisms), practical aspects (large-scale measurement of Web applications, integration in existing Web browsers), and usability aspects (user surveys to evaluate privacy concerns and usability of existing and new protection tools).

9.2.2 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.

9.2.3 Inria Action de Dévelopement Technologique (ADT)

PRESERVE (Plate-foRme wEb de SEnsibilisation aux pRoblèmes de Vie privéE):

Participant: Antoine Boutet, Adrien Baud. The goal of the PRESERVE ADT is to design a platform whose goal is to raise users' awareness of privacy issues. The first version implements tools in order to inspect location history. Specifically, this version implements [hal-02421828] where a user is able to inspect the private and sensitive information inferred from its own location data.

10 Dissemination

Participants: all team members.

10.1 Promoting scientific activities

10.1.1 Scientific events: organisation

General chair, scientific chair

- Mathieu Cunche, co-organizer of the 11th edition of *Atelier sur la Protection de la Vie Privée*
- Antoine Boutet, Organizer of the Health PPML Workshop *Health and Privacy-Preserving Machine Learning Workshop 2021*
- Nataliia Bielova, organizer and moderator of the panel *"Standard for consent: still a dream or a soon-to-be reality?"* at the CPDP 2021 conference.

10.1.2 Scientific events: selection

Chair of conference program committees

- Mathieu Cunche, co-chair of jury for CNIL-Inria privacy award

Member of the conference program committees

- Cédric Lauradoux: APF 2021
- Antoine Boutet: IWPE 2021, LPW 2021
- Nataliia Bielova: IEEE S&P 2021, MADWeb 2021, ConPro 2021

10.1.3 Journal

Member of the editorial boards

- Nataliia Bielova: PoPETs 2021

Reviewer - reviewing activities

- Mathieu Cunche, Computer Networks (Elsevier)
- Antoine Boutet, PLOS ONE, ACM Digital Threats

10.1.4 Invited talks

- Claude Castelluccia was audited on “Online Brain Hacking” by the Académie Nationale de Médecine, January 2021
- Vincent Roca was invited by the Académie de Médecine, April 2021, for a seminar: "De ROBERT à CLÉA, du traçage numérique de contacts à la gestion des historiques de lieux : gros plan sur deux fonctionnalités clefs de l’application souveraine TousAntiCovid"
- Vincent Roca was invited by the GDR C2 - GDR - PVP, Table ronde, June 30 2021: "TousAntiCovid (TAC), ROBERT, DÉSIRÉ et CLÉA : le point de vue PRIVATICS"
- Vincent Roca was invited for the WeHealth seminar, September 28th, 2021: "TousAntiCovid app (FR): focus on the CLÉA presence tracing protocol"
- Vincent Roca was invited by the Sustainable Computing Lab Serie of Seminars, Oct. 1st, 2021: "Smart Bulbs and Privacy: Lost in the Smart Jungle"
- Vincent Roca was invited by the Inria Workshop on Systems (WOS), October 12th, 2021: "TousAntiCovid : gros plan sur les fonctions de traçage nume‘rique de contacts (ROBERT) et de pre‘sence (CLÉA)"

- Vincent Roca was invited by the Alliance Nationale pour les Sciences de la Vie et de la Santé (AVIESAN), 12eme journe'e ITS, Nov. 23rd, 2021: "TousAntiCovid : gros plan sur les deux protocoles de traçage numérique de l'application"

- Vincent Roca was invited by the Digital Tech Conference, Rennes, Dec. 3rd, 2021, for a Table ronde: "Les choix technologiques sont l'affaire de tous, l'exemple de l'application TousAntiCovid"

- Claude Castelluccia participated to the CCNPE (Comité Consultatif National Pilote d'Ethique du Numérique) workshop on Contact Tracing, June 2021.

- Claude Castelluccia participated in a panel at CPDP 2021 on "Contact Tracing and European Sovereignty", January 2021.

- Antoine Boutet was invited to present DARC, the Data Anonymization and Re-identification Challenge at the French Japanese Cybersecurity Workshop, February 2021.

- Nataliia Bielova was an invited speaker at the Security & Privacy track of ICT OPEN, Netherlands, February 2021.

- Nataliia Bielova was invited by the The Organisation for Economic Co-operation and Development (OECD) in March 2021 to present her work on dark patterns and standartisation of consent.

- Nataliia Bielova was invited to be a member of a panel "Regulating digital platforms: convergence or divergence?" at the TILTing Perspectives event, May 2021.

- Imane Fouad was invited by the Federal Trade Commission (FTC) to present her work at the PrivacyCon conference, July 2021.

10.1.5 Leadership within the scientific community

- Mathieu Cunche, co-chair of the Privacy Protection (PVP) Working Group of *GDR Sécurité*

10.2 Responsibilities in Public Authorities

- Claude Castelluccia was nominated at the CNIL (French Data Protection Agency) as one of its commissioners , August 2021.

- Nataliia Bielova has joined the CNIL (French Data Protection Authority) for 1 year as *Senior Privacy Fellow*, September 2021.

10.3 Standardisation activities

- Vincent Roca is co-chair of the "Coding for Efficient Network Communications" (NWCRG) Internet Research Task Force (IRTF): (nwcrg site). As such, he co-organized the IETF110 and IETF111 research group meetings, he shephered several standard candidate documents, organized the work within the group.

- Vincent Roca is member and reviewer of the IETF Security Directorate (SecDir), and member of the Internet Research Steering Group (IRSG). (IETF site).

- Mathieu Cunche is Delegate chair of the "MAC Address Device Identification for Network and Application Services" (MADINAS) IETF Working Group. (madinas site).

10.4 Teaching - Supervision - Juries

10.4.1 Teaching

Most of the PRIVATICS members' lectures are given at INSA-Lyon (Antoine Boutet and Mathieu Cunche are associated professor at INSA-Lyon), at Grenoble Alps University (Claude Castelluccia, Vincent Roca and Cédric Lauradoux), and Université Côte d'Azur (Nataliia Bielova).

Most of the PRIVATICS members' lectures are on the foundations of computer science, security and privacy, as well as networking. The lectures are given to computer science students but also to business school students and to laws students. The Privatics members have created original content for security (ressi2019 site) and for anonymisation (ressi2020 site).

Details of lectures:

- Master: Nataliia Bielova, *Privacy, Security and ethical aspects of Data*, 18h, Universite Cote d'Azur, France.
- Master: Nataliia Bielova, *Privacy on the Internet*, 15h, SKEMA Business School, France.
- Master : Antoine Boutet, *Privacy*, 80h, INSA-Lyon, France.
- Master : Antoine Boutet, *Security*, 40h, INSA-Lyon, France.
- Master : Antoine Boutet, *Security and Privacy*, 40h, Polytech Annecy, France.
- Master : Antoine Boutet, *Network*, 110h, INSA-Lyon, France.
- Undergraduate course : Mathieu Cunche, *Introduction to computer science*, 120h, L1, INSA-Lyon, France.
- Master : Mathieu Cunche, *Wireless Security*, 6h, M2, INSA-Lyon, France.
- Undergraduate course : Mathieu Cunche, *On Wireless Network Security*, 10h, L1, IUT-2 (UPMF - Grenoble University) , France.
- Undergraduate course : Mathieu Cunche, *Systems and Networks Security* , 10h, M2, INSA-Lyon, France.
- Master : Mathieu Cunche, *Privacy and Data protection*, 26h, 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 : Claude Castelluccia, *Data Privacy*, 12h, SKEMA Business School, Sophia-Antipolis, France.
- Master : Daniel Le Métayer, *Privacy*, 12h, M2 MASH, Université Paris Dauphine, France.
- Master : Daniel Le Métayer, *Privacy*, 12h, M2, Insa Lyon, France.

- Master : Daniel Le Métayer, *Digital ethics*, 8h, M2, Insa Lyon, France.
- Master : Vincent Roca, *Wireless Communications*, 16h, M2, Polytech, University of Grenoble Alpes, France.
- Undergraduate course : Vincent Roca, *C Programming and Security*, 24h, L-Pro, IUT-2 (University of Grenoble Alpes), France.
- Undergraduate course : Vincent Roca, *Privacy in Smartphones and Internet of Things*, 3h, L-Pro, University of Grenoble Alpes, France.
- Master : Vincent Roca, *Privacy in Smartphones and Internet of Things*, 3h, M2, Ensimag/INPG, France.
- Master : Vincent Roca, *Privacy in Smartphones*, 1.5h, M2 (University of Cote-d'Azur), France.

10.4.2 Supervision

PhD defended in 2021:

- PhD defended: Imane Fouad, *"Detection and Measurement of advanced Web tracking techniques"* , June 2021, Nataliia Bielova and Arnaud Legout
- PhD defended: Raouf Kerkouche, *"Federated learning privacy"*, July 2021, Claude Castelluccia and Pierre Geneves
- PhD defended: Supriya Adhatarao, *"PDF file sanitization, IP based subject access"*, July 2021, Cédric Lauradoux and Claude Castelluccia
- PhD defended: Clément Henin, *"Explanations and justifications of algorithmic decisions"*, Oct. 2021, Daniel LeMetayer and Claude Castelluccia
- PhD defended: Théo Jourdan, *"sanitizing motion sensor data against sensitive inferences"*, Oct. 2021, Antoine Boutet and Carole Frindel

On-going PhDs:

- Coline Boniface, *"Attribution of cyber attacks"*, co-supervised by Cédric Lauradoux and Karine Bannelier
- Michael Toth, co-supervised by Nataliia Bielova and Vincent Roca
- Samuel Pelissier, co-supervised by Mathieu Cunche and Vincent Roca
- Suzanne Lansade, co-supervised by Cédric Lauradoux and Vincent Roca
- Jan Aalmoes, co-supervised by Antoine Boutet, Carole Frindel and Mathieu Cunche
- Thomas Lebrun, co-supervised by Antoine Boutet, Claude Castellucccia and Mathieu Cunche

10.4.3 Juries

- Vincent Roca was reviewer for Iulian Sandu Popa HDR defense ("Preserving individual privacy with personal data management systems"), Univ. Versailles St Quentin-en-Yvelines, Dec. 10th, 2021.
- Vincent Roca was examiner for Hira Malik PhD defense ("Efficient Network Coding Protocols for Information-Centric Networks"), Univ. Paris Saclay, Nov. 22nd, 2021.
- Mathieu Cunche was examiner for Clémence Mauger PhD defense ("Optimisation de l'utilité des données lors d'un processus de k-anonymisation"), Université de Picardie, 6th December 2021.
- Claude Castelluccia was president for Aurelien Bellet HDR ("Contributions to Decentralized and Privacy-Preserving Machine Learning"), Nov. 2021.

10.5 Popularization

10.5.1 Articles and contents

- Claude Castellucccia was interviewed by **France 3 Corse** on the French Contact Tracing App, January 2021.
- Mathieu Cunche interviwed on **LCI**, "Nos smartphones nous écoutent-ils ?", 27/09/2021
- Mathieu Cunche interviewed by **Le Figaro**, "Pourquoi les QR codes du passe sanitaire sont dits «infalsifiables»", , 24/08/2021

10.5.2 Interventions

- Fête de la Science, Oct. 2021, Grenoble: création et animation d'un "Jeu à débattre : surveillance et vie privée, quel équilibre ?", Cédric Lauradoux
- Fête de la Science, Oct. 2021, Grenoble: création et animation d'un atelier "Vie privée, anonymisation et open-data, dark pattenrs et manipulation", Vincent Roca, Michael Toth
- Fête de la Science, Oct. 2021, Grenoble: animation d'un atelier "Cryptographie": Suzanne Lansade

11 Scientific production

11.1 Major publications

[1] S. Adhatarao and C. Lauradoux. 'Exploitation and Sanitization of Hidden Data in PDF Files: Do Security Agencies Sanitize Their PDF Files?' In: IH&MMSec '21: ACM Workshop on Information Hiding and Multimedia Security. Virtual Event Belgium, Belgium: ACM, 22nd June 2021, pp. 35–44. DOI: 10.1145/3437880.3460405. URL: https://hal.inria.fr/hal-03528949.

[2] A. Boutet, C. Castelluccia, M. Cunche, C. Lauradoux, V. Roca, A. Baud and P.-G. Raverdy. 'DESIRE: Leveraging the best of centralized and decentralized contact tracing systems'. In: *Digital Threats: Research and Practice* (5th Aug. 2021). DOI: 10.1145/3480467. URL: https://hal.inria.fr/hal-03476799.

[3] C. M. Gray, C. Santos, N. Bielova, M. Toth and D. Clifford. 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective'. In: CHI 2021 - ACM CHI Conference on Human Factors in Computing Systems. Yokohama, Japan, 8th May 2021, pp. 1–18. DOI: 10.1145/3411764.3445779. URL: https://hal.inria.fr/hal-03117307.

[4] C. Henin. 'Confier une décision vitale à une machine'. In: *Réseaux*. L'action publique au prisme de la gouvernementalité numérique 225 (1st Feb. 2021), pp. 187–213. DOI: 10.3917/res.225.0187. URL: https://hal.archives-ouvertes.fr/hal-03551778.

[5] C. Henin and D. Le Métayer. 'A Framework to Contest and Justify Algorithmic Decisions'. In: *AI and Ethics* (4th May 2021). URL: https://hal.inria.fr/hal-03127932.

[6] R. Kerkouche, G. Ács, C. Castelluccia and P. Genevès. 'Compression Boosts Differentially Private Federated Learning'. In: EuroS&P 2021 - 6th IEEE European Symposium on Security and Privacy. Vienna, Austria: IEEE, 6th Sept. 2021, pp. 1–15. URL: https://hal.archives-ouvertes.fr/hal-03066941.

[7] R. C. Ngueveu, A. Boutet, C. Frindel, S. Gambs, T. Jourdan and C. Rosin. *DYSAN: Dynamically sanitizing motion sensor data against sensitive inferences through adversarial networks*. RR-9325. inria, 21st Feb. 2020, p. 27. URL: https://hal.inria.fr/hal-02512640.

[8] V. Roca, A. Boutet and C. Castelluccia. *The Cluster Exposure Verification (CLEA) Protocol: Specifications of Protocol Version 0*. Inria Grenoble - Rhône-Alpes, 8th June 2021. URL: https://hal.inria.fr/hal-03146022.

11.2 Publications of the year

International journals

[9] A. Boutet, C. Castelluccia, M. Cunche, C. Lauradoux, V. Roca, A. Baud and P.-G. Raverdy. 'DESIRE: Leveraging the best of centralized and decentralized contact tracing systems'. In: *Digital Threats: Research and Practice* (5th Aug. 2021). DOI: 10.1145/3480467. URL: https://hal.inria.fr/hal-03476799.

[10] A. Boutet and M. Cunche. 'Privacy Protection for Wi-Fi Location Positioning Systems'. In: *Journal of information security and applications* (1st May 2021), pp. 1–9. DOI: 10.1016/j.jisa.2020.102635. URL: https://hal.inria.fr/hal-03045102.

[11] C. Henin. 'Confier une décision vitale à une machine'. In: *Réseaux*. L'action publique au prisme de la gouvernementalité numérique 225 (1st Feb. 2021), pp. 187–213. DOI: 10.3917/res.225.0187. URL: https://hal.archives-ouvertes.fr/hal-03551778.

[12] C. Henin and D. Le Métayer. 'A Framework to Contest and Justify Algorithmic Decisions'. In: *AI and Ethics* 1 (4th May 2021), pp. 463–476. DOI: 10.1007/s43681-021-00054-3. URL: https://hal.inria.fr/hal-03127932.

[13] C. Henin and D. Le Métayer. 'Beyond explainability: justifiability and contestability of Algorithmic Decision Systems'. In: *AI & Society: Knowledge, Culture and Communication* (30th July 2021). DOI: 10.1007/s00146-021-01251-8. URL: https://hal.inria.fr/hal-03165232.

International peer-reviewed conferences

[14] S. Adhatarao and C. Lauradoux. 'How are PDF files published in the Scientific Community?' In: WIFS 2021 - IEEE International Workshop on Information Forensics and Security. Montpellier, France: IEEE, 7th Dec. 2021, pp. 1–6. DOI: 10.1109/WIFS53200.2021.9648374. URL: https://hal.inria.fr/hal-03528956.

[15] A. Boutet, C. Frindel, S. Gambs, T. Jourdan and R. C. Ngueveu. 'DYSAN: Dynamically sanitizing motion sensor data against sensitive inferences through adversarial networks'. In: ACM ASIACCS 2021 - 16th ACM ASIA Conference on Computer and Communications Security. Hong Kong (Virtuel), China, 1st May 2021. URL: https://hal.inria.fr/hal-02512640.

[16] A. Boutet, T. Pascoal, J. Decouchant and P. Esteves-Verissimo. 'DyPS: Dynamic, Private and Secure GWAS'. In: PETS 2021 - 21st Annual Privacy Enhancing Technologies Symposium. Online, France, 12th July 2021, pp. 1–19. URL: https://hal.inria.fr/hal-03354937.

[17] C. M. Gray, C. Santos, N. Bielova, M. Toth and D. Clifford. 'Dark Patterns and the Legal Requirements of Consent Banners: An Interaction Criticism Perspective'. In: CHI 2021 - ACM CHI Conference on Human Factors in Computing Systems. Yokohama, Japan, 8th May 2021, pp. 1–18. DOI: 10.1145/3411764.3445779. URL: https://hal.inria.fr/hal-03117307.

[18] C. Henin and D. Le Métayer. 'A Multi-layered Approach for Tailored Black-box Explanations'. In: ICPR 2020 - Workshop Explainable Deep Learning - AI. Vol. Pattern Recognition. ICPR International Workshops and Challenges. Lecture Notes in Computer Science 12663. Virtual Event, Italy, 21st Feb. 2021, pp. 5–19. DOI: 10.1007/978-3-030-68796-0_1. URL: https://hal.inria.fr/hal-03127926.

[19] T. Jourdan, A. Boutet and C. Frindel. 'Privacy Assessment of Federated Learning using Private Personalized Layers'. In: MLSP 2021 - IEEE International Workshop on Machine Learning for Signal Processing. Queensland, Australia, 25th Oct. 2021, pp. 1–5. URL: https://hal.inria.fr/hal-03354722.

[20] R. Kerkouche, G. Acs, C. Castelluccia and P. Genevès. 'Privacy-Preserving and Bandwidth-Efficient Federated Learning: An Application to In-Hospital Mortality Prediction'. In: CHIL 2021 - ACM Conference on Health, Inference, and Learning. virtual event, France: ACM, 8th Apr. 2021, pp. 1–11. URL: https://hal.inria.fr/hal-03160473.

[21] R. Kerkouche, G. Ács, C. Castelluccia and P. Genevès. 'Compression Boosts Differentially Private Federated Learning'. In: EuroS&P 2021 - 6th IEEE European Symposium on Security and Privacy. Vienna, Austria: IEEE, 6th Sept. 2021, pp. 1–15. URL: https://hal.archives-ouvertes.fr/hal-03066941.

[22] R. Kerkouche, G. Ács, C. Castelluccia and P. Genevès. 'Constrained Differentially Private Federated Learning for Low-bandwidth Devices'. In: *Proceedings of Machine Learning Research*. UAI 2021 - 37th Conference on Uncertainty in Artificial Intelligence. Online, United States, 26th July 2021, pp. 1–18. URL: https://hal.archives-ouvertes.fr/hal-03266004.

[23] C. Lagneau-Donzelle and M. Cunche. 'On the process of fixing privacy issues in Wi-Fi enabled devices'. In: WSA 2021 - 25th International ITG Workshop on Smart Antennas. Sophia-Antipolis, France, 10th Nov. 2021, pp. 1–6. URL: https://hal.inria.fr/hal-03411842.

[24] P. Rougé, A. Moukadem, A. Dieterlen, A. Boutet and C. Frindel. 'Anonymizing motion sensor data through time-frequency domain'. In: MLSP 2021 - Machine Learning for Signal Processing. Queensland, Australia, 25th Oct. 2021, pp. 1–6. URL: https://hal.inria.fr/hal-03354723.

[25] V. Toubiana and M. Cunche. 'No need to ask the Android: Bluetooth-Low-Energy scanning without the location permission'. In: WiSec 2021 - 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks. Abu Dhabi, United Arab Emirates: ACM, 28th June 2021, pp. 1–6. URL: https://hal.inria.fr/hal-03265556.

Conferences without proceedings

[26] V. Wesselkamp, I. Fouad, C. Santos, Y. Boussad, N. Bielova and M. Lorenzi. 'In-Depth Technical and Legal Analysis of Tracking on Health Related Websites with ERNIE Extension'. In: 20th Workshop on Privacy in the Electronic Society. Seoul, South Korea, 15th Nov. 2021. URL: https://hal.archives-ouvertes.fr/hal-03241333.

Doctoral dissertations and habilitation theses

[27] I. Fouad. 'Detection and measurement of web tracking'. Université Côte d'Azur, 29th June 2021. URL: https://tel.archives-ouvertes.fr/tel-03278529.

[28] C. Henin. 'Explain and Justify Algorithmic Decision Systems'. Université de Lyon, 13th Oct. 2021. URL: https://tel.archives-ouvertes.fr/tel-03551798.

[29] R. Kerkouche. 'Differentially Private Federated Learning for Bandwidth and Energy Constrained Environments'. Université Grenoble Alpes [2020-....], 7th July 2021. URL: https://tel.archives-ouvertes.fr/tel-03467131.

Reports & preprints

[30] A. Boutet, T. Lebrun, J. Aalmoes and A. Baud. *MixNN: Protection of Federated Learning Against Inference Attacks by Mixing Neural Network Layers*. RR-9411. INRIA Grenoble, 11th June 2021, pp. 1–21. URL: https://hal.inria.fr/hal-03354724.

[31] I. Fouad, C. Santos, M. Lorenzi and N. Bielova. *Did I delete my cookies? Cookies respawning with browser fingerprinting*. 5th May 2021. URL: https://hal.archives-ouvertes.fr/hal-03218403.

[32] V. Roca, A. Boutet and C. Castelluccia. *The Cluster Exposure Verification (CLEA) Protocol: Specifications of Protocol Version 0*. Inria Grenoble - Rhône-Alpes, 8th June 2021. URL: https://hal.inria.fr/hal-03146022.

[33] C. Santos, M. Nouwens, M. Toth, N. Bielova and V. Roca. *Consent Management Platforms under the GDPR: processors and/or controllers?* 12th Apr. 2021. URL: https://hal.inria.fr/hal-03169436.

Other scientific publications

[34] M. Cunche. 'Le traçage cyberphysique des personnes et la vie privée'. In: *Annales des Mines - Enjeux Numériques*. Des objets connectés aux objets communicants 16 (1st Dec. 2021). URL: https://hal.inria.fr/hal-03471223.

[35] T. Pascoal, J. Decouchant, A. Boutet and P. Esteves-Verissimo. *DyPS: Dynamic, Private and Secure GWAS (Summary)*. Online, France, 22nd Sept. 2021. URL: https://hal.inria.fr/hal-03354910.

[36] C. Santos, M. Nouwens, M. Toth, N. Bielova and V. Roca. *Consent management platforms under the GDPR: processors and/or controllers?* online, France, 17th June 2021. URL: https://hal.inria.fr/hal-03264392.

11.3 Other

Scientific popularization

[37] M. Cunche. 'Le traçage cyberphysique des personnes et la vie privée'. In: *Interstices* (28th Jan. 2022). URL: https://hal.inria.fr/hal-03589575.

Softwares

[38] [SW] V. Wesselkamp, I. Fouad, A. Legout and N. Bielova, *Ernie Extension*, 16th Nov. 2021. LIC: GNU General Public License v3.0 only. HAL: ⟨hal-03413044⟩, URL: https://hal.archives-ouvertes.fr/hal-03413044, VCS: https://github.com/vwesselkamp/ernie-extension, SWHID: ⟨swh:1:dir:6cf9d69e8467428628b93fd5e91b2c5f1684e7e7;origin=https://hal.archives-ouvertes.fr/hal-03413044;visit=swh:1:snp:69b5f385b8f53f754ddbc6174b9d6cefc869e8fa;anchor=swh:1:rev:55f6308a857dd97100e4b06a5d6647d5330eadaf;path=/⟩.