FIC

Forum International
de la Cybersécurité

ALLISTENE

l'alliance des sciences
et technologies du numérique

ALLISTENE 2022
MASTER CLASS PROGRAM

cdefi
Conférence des Directeurs
des Écoles Françaises
d'Ingénieurs

cea

cnrs

INVESTIR L'AVENIR

IMPACT
DIGITRUST

France
Universités

Inria

Institut Mines-Télécom

ALLISTENE
l'alliance des sciences
et technologies du numérique

Allistene Alliance

Allistene is the alliance of digital sciences and technologies; it supports the economic and social changes related to the diffusion of digital technologies. The aim of the alliance is to coordinate the various actors involved in digital science and technology research in order to develop a coherent and ambitious program of research and technological development. It allows to identify common scientific and technological priorities and to strengthen partnerships between public operators (universities, schools, institutes), while creating new synergies with companies.

The Allistene alliance has a "Cybersecurity" working group (WG), whose mission is to assist the Coordination Committee in addressing the various issues related to cybersecurity:

- Forecasting cybersecurity research topics, specifying the research challenges, the application impacts and the relevant actors in the French community;
- Elaboration of programmatic elements at the national and European levels
- Cybersecurity watch and development of a collaborative strategy, in interaction with the CSF Security Industries.

This WG brings together representatives of the main EPSTs, France Université, engineering schools and the private sector.

ALLISTENE
l'alliance des sciences
et technologies du numérique

DATE: June 7th, 2022

11:00 - 11:30 AM

Lattice-based cryptography and NIST finalists

Adeline Roux-Langlois / **CNRS**

The goal of cryptography is to safely communicate, and it is widely used when connecting to a website or during a banking transaction for example. But some cryptographic constructions used today could be attacked given a powerful enough quantum computer. Even if such a computer does not exist yet, it is important to anticipate its possible construction and to prepare a transition to cryptographic tools having a security resistant against attacks from quantum computers.
Among all the possibilities of post-quantum constructions that we observed during the NIST competition (which aim to find standards in post-quantum cryptography), lattice-based cryptography seems to be the most promising. Indeed, 5 over the 7 finalists has their security relying on hypothesis from lattices.
In this talk, I will introduce lattice-based cryptography. I will first describe the main ideas and the hard problems on which is based the security of the cryptographic constructions. Then I will give a high-level idea of the encryption schemes and signature schemes finalists at the NIST competition.

Adeline Roux-Langlois is a tenured research fellow at CNRS, in the CAPSULE team of the IRISA laboratory, in Rennes. She obtained her PhD at ENS de Lyon in 2014, and worked one year as a post-doctoral researcher at EPFL, Switzerland. Her research focuses on foundations of lattice-based cryptography, in particular she works on cryptographic constructions and their security proofs, and on the theoretical difficulty of the problems used to study this security.

cnrs

DATE: June 7th, 2022

11:30 AM - 12:00 PM

Biometric authentication: how to (re) reconcile security, usability and privacy?

Estelle Cherrier **/ ENSICAEN / GREYC**

When looking at biometric authentication, it is now essential to consider the following three complementary aspects: security, usability and respect for privacy (or data protection). This, in order to avoid security abuses and preserve individual freedoms. Thus, the security provided by biometrics implies high confidence in the identity claimed by the user and allows the deployment of strong authentication applications to access many digital services. These services are accessible via strong authentication, either within the sovereign framework or within a private commercial framework. Usability allows, for its part, a real acceptance of biometrics by the general public - we can cite the recognition of the face or the fingerprint for example -, in addition to or even sometimes replacing more traditional means of authentication such as PIN codes or passwords that clutter our memories. Finally, the protection of biometric data constitutes an essential protection of individual freedoms, in the sense that it is sensitive personal data according to the CNIL. More broadly, the protection of personal data has been highlighted for a year by the entry into force of the GDPR in all member countries of the European Union, placing them in the forefront of countries concerned with protecting the data of their citizens.

Estelle Cherrier has been an HDR lecturer since 2007 at the National School of Engineers of Caen, attached to the GREYC laboratory. Her current research themes are centered on data: biometric data (their security, their protection), the collection of data that respects the privacy of users, authentication on smartphones, the usability of authentication applications, the evaluation of community detection algorithms in multi-graphs.

ALLISTENE
l'alliance des sciences
et technologies du numérique

DATE: June 7th, 2022

03:00 - 03:30 PM

Attacks and Protection Mechanisms in Federated Learning
Vlad Nitu / **CNRS**

Thanks to Collaborative Learning (also called Federated Learning), a large number of mobile devices can collectively train a model on their private data, without having to send the raw data to external service providers. To this end, workers iteratively update a global model using their local training data and send only these updates to a central party called aggregation server that orchestrates the training process. Federated Learning (FL) was rapidly adopted in multiple thriving application domains such as the next-word prediction in the Android keyboard, healthcare, banking, and many more. However, the FL protocol exposes a fairly large attack surface for two main reasons. First, edge workers can both access model parameters and influence their value through the model updates sent to the aggregation server. On the server side, defining how a malicious update looks like and how to distinguish it from benign ones is not straightforward due to the low interpretability of the ML models. Second, multiple attacks demonstrated that, in some conditions, ML models can be inverted so that an attacker can potentially recover sensitive information about the training data. In this talk, we will discuss the state-of-the-art attacks on both the privacy and the robustness of Federated Learning as well as the protection mechanisms which aim to deal with these vulnerabilities.

Vlad Nitu is a junior researcher at The French National Centre for Scientific Research (CNRS), assigned to the LIRIS laboratory, Lyon. His main research interests are the Security and the Energy-efficiency of Collaborative Edge AI, as well as its applicability to different fields such as the Industry 4.0. Previously, Vlad was a Postdoctoral Researcher at the Swiss Federal Institute of Technology Lausanne, working in the Distributed Computing Laboratory. Vlad obtained his PhD in 2018 from Toulouse University, on the Energy-efficiency and the performance of virtualised cloud datacenters. He is the recipient of the Léopold Escande prize and the ASF/GDR prize for the best PhD theses defended in 2018. During his career, Vlad also collaborated with big-tech companies (Facebook, IBM, Huawei, etc.) or other international academic research partners (ETH Zurich, George Washington University, Virginia Tech, etc.).

cnrs

DATE: June 7th, 2022

03:30 - 04:00 PM

KRAKEN: A Knowledge-Based Recommender system for Analysts, to Kick Exploration up a Notch

Romain Brisse / Inria / Malizen

Nowadays, Intrusion Detection and log visualization systems are the most commonly used tools to detect and characterize attacks. At the center of their use, we find the security analyst, who faces complicated issues such as quantity and heterogeneity of data. Despite the existing solutions, their work is increasingly difficult because of the ever-growing number of attacks and organized attack groups. Some attacks can go as far as being spread over very long periods of time, sometimes months, to increase their stealth. These are some reasons we chose to focus our effort on facilitating the analyst's work.

Our main goal is to make the analyst's tasks easier and more efficient by helping them select the next step of their investigation by contextualizing their discoveries. To do so, we present KRAKEN, a recommender system based on expert knowledge and investigation context, that offers relevant exploration recommendations in the shape of fields of data. KRAKEN is implemented as part of a thesis and integrated to the product ZeroKit developed by the startup Malizen.

In this project, we have implemented a knowledge base using the projects MITRE ATT&CK and Elastic Common Schema as well as two decision-making processes, one based on similarity between objects and the other one on a method called Multi-Attribute Decision-Making. We have then gathered 7 security experts to test our prototype integrated into ZeroKit, a threat-hunting tool. This evaluation yielded rich qualitative results regarding our approach.

In the near future, we will be working on conducting a more quantitative evaluation by integrating the feedback we got, such as history of recommendation, improving recommendation explicability, learning, and various interface changes.

Being currently a CIFRE PhD student within Inria and Malizen, Romain is a member of the Inria CIDRE team (joint team Inria, CentraleSupélec, CNRS and Univ. Rennes 1). His work focuses on the use of recommender systems applied to the investigation of security incidents.

DATE: June 7th, 2022

04:00 - 04:30 PM

Study on Domain Name System (DNS) abuse

Maciej Korczyński **/ Grenoble INP / Grenoble Alpes Cybersecurity Institute / KOR Labs**

Domain Name System (DNS) abuse is any activity that makes use of domain names or the DNS protocol to carry out harmful or illegal activity. Malicious activities on the DNS have been a frequent and serious issue for years, affecting online security, causing harm to users and third parties and undermining trust in the Internet. The study assessed the scope, magnitude and impact of DNS abuse and provided input for possible policy measures. To this end the contractors conducted technical measurements focused on the health of DNS ecosystems, and surveyed experts and stakeholders though questionnaires, in-depth interviews and workshops involving a wide spectrum of actors (registries, registrars, hosting providers, DNS infrastructure providers) and interested parties in the field of consumer protection, IP rights, cyber security and public policy. The study proposes a set of recommendations in the field of prevention, detection and mitigation of DNS abuse addressed to DNS operators (TLD registries, registrars, resellers and hosting providers, depending on their role in the DNS chain) but also to international, national and EU institutions and coordination bodies. The study also recommends actions in the field of DNS metadata, WHOIS and contact information, abuse reporting, protection of the DNS operations, awareness, knowledge building and mitigation collaboration at EU level.

Maciej is an Associate Professor of computer networks and cybersecurity at Grenoble INP and co-founder of KOR Labs. His main interests revolve around large-scale passive and active measurements for cybersecurity, with a focus on DNS. Since 2015, he co-authored over 30 research papers about domain name abuse, DNS vulnerabilities, DNS reputation metrics, economic incentives for improving security of the DNS ecosystem, IP spoofing, DDoS attacks, botnets, and vulnerability notifications.

ALLISTENE
l'alliance des sciences
et technologies du numérique

DATE: June 7th, 2022

04:30 - 05:00 PM

Rigorous development of secure architecture within the negative and positive statements

Brahim HAMID / **IRIT/ University Toulouse Jean-Jaurès**

Security experts, practitioners, and researchers from different international organizations, associations, and academia have agreed that for security, "it's not just the code." The most popular and well-known software security vulnerabilities are design issues. The existence of security threats in software designs can significantly impact their safe and reliable operation. As a result, there are challenges regarding ways to identify, analyse, and prepare for threats, mitigate vulnerabilities, and minimize impact and consequences. Our work aims to address these challenges by developing an integrated approach for specifying, detecting, and treating security threats at the software architecture design time in an effort to build-in security. Achieving this objective can help system designers to rework their designs to eliminate or mitigate the identified threats and/or to aid in selecting appropriate security and reliability controls to ensure the safe, secure, and reliable operations of their systems. Notions such as patterns, properties, models, analysis and experimental evaluations can help in the development of well-designed, properly modelled, accurately documented, and well-understood secure systems. The general idea of the approach is to: (1) specify threats as properties of a modelled system in a technology-independent specification language; (2) express conditions that reveal these threats in a suitable language with automated tool support for threat detection through model verification; and (3) suggest a set of security policies as abstract security solutions to protect against detected threats. The formalized threats and security policies are then provided as formal model libraries to foster reuse. Furthermore, we defined a similar approach to handle security requirements from the positive perspective as security objectives. We employ Model-Driven Engineering (MDE) and formal techniques (model reuse and automatic verification) to support the approach. To validate our work, we explore a set of representative threats from categories based on Microsoft's STRIDE classification and objectives from categories based on CIAA classification in the context of secure component-based software architecture.

Brahim HAMID is a professor of computer science at the University of Toulouse Jean-Jaurès, Toulouse, France, and he has been a member of the IRIT-ARGOS team from 2019 to present. He works on security, dependability, software architectures, formalization, validation and verification. Emphasis of his work lies in developing tools to model and analyse secure and dependable Software architecture of critical infrastructures. Contact him at brahim.hamid@irit.fr.

France Universités

DATE: June 8th, 2022

11:00 - 11:30 AM

Vulnerability and Attack Repository for IoT

Anna Felkner / **NASK** and Gregory Blanc / **Télécom SudParis**

The overall objective of the Vulnerability and Attack Repository for IoT (VARIoT) project' is to create a service that provides actionable information regarding Internet of Things devices that can be processed manually or automatically and that can be used to ensure their cybersecurity. Relevant data is made available through the official portal for European data (data.europa.eu), as well as through other interfaces, such as the Malware Information Sharing Platform (MISP), and through Shadowserver's free daily remediation feeds. The VARIoT project is co-financed by the Connecting Europe Facility of the European Union and by the program of the Polish Minister of Science and Higher Education.
Main outcomes of the Project are 1) a database of information on vulnerabilities and exploits of IoT devices, 2) mechanisms of correlation of various types of information, 3) a vulnerability information search engine, 4) catalogues of IoT device types and of IoT related malware, 5) Internet scanning campaigns to identify vulnerable, publicly available IoT devices, 6) a system for IoT devices network anomaly detection, 7) Internet Draft documents describing the open data with its implementation in MISP, and 8) aggregated and anonymized statistics on infected and vulnerable IoT devices.

Anna Felkner is the coordinator of the VARIoT project. She is an Assistant Professor and Head of the Information Security Methods Department in the Center of Research and Development at Research and Academic Computer Network (NASK PIB). Her interests include access control, trust modeling, risk analysis and vulnerability management, trust frameworks, national cybersecurity management and cooperation in the context of cybersecurity. She holds a PhD in information technology from the Warsaw University of Technology. Has taken part in several national and EU-funded research projects, author of over forty publications, has spoken at many conferences.

Gregory Blanc is responsible for VARIoT's workpackage 4 on IoT Device and Malware Behavior Analysis. He is an Associate Professor at Télécom SudParis, and in charge of the Networks and Systems Security curriculum. His interests include intrusion detection, attack mitigation, virtualized network security and the application of AI to cybersecurity. He holds a PhD in computer science from Nara Institute of Science and Technology.

DATE: June 8th, 2022

11:30 AM - 12:00PM

The security of the communication protocols of IoT: BLE example

Romain Cayre **Apsys Lab** / **LAAS-CNRS** and Vincent Nicomette **/ INSA Toulouse** / **LAAS-CNRS**

The Bluetooth Low Energy (BLE) protocol is one of the most popular and widespread wireless communication protocols of the Internet of Things (IoT). Unfortunately, several attacks targeting this protocol or its implementations have been recently published, showing both the increasing interest for this technology and its fragility from a security point of view. This presentation aims at first at presenting a panorama of diverse attacks targeting this protocol and then describing a new vulnerability discovered in the context of the research work of Romain Cayre's PhD. The attack, so-called InjectaBLE, allows to inject some malicious traffic inside an already established BLE connection, which was until now considered as a difficult technological challenge. The exploited weakness is especially critical because it is inherent to the specification of the protocol itself and as a consequence, potentially concerns any BLE communication, whatever the devices used. In this presentation, we describe the principle of the attack and its implementation in the context of concrete offensive scenarios.

Romain Cayre is currently a PHD student, in the context of a CIFRE collaboration between APSYS Lab and LAAS-CNRS. He is a member of the TSF (Dependable Computing and Fault Tolerance) research team of LAAS. His research work focuses on the security of the communication protocols of the IoT, both from the offensive and defensive perspective. He has developed several open-source tools, and proofs of concept, such as Mirage, Injectable and RadioSploit (see https://github.com/RCayre).

Vincent Nicomette is currently professor at INSA Toulouse and LAAS-CNRS in the TSF team. His main research topics concern the security of operating systems, of critical embedded systems, of network (most specifically the IoT networks).

ALLISTENE
l'alliance des sciences
et technologies du numérique

DATE: June 8th, 2022

12:00 - 01:00 PM

All your code belongs to us: a tale of adversarial users

Grégoire Menguy and Sébastien Bardin / **CEA**

Software contain valuable assets, such as secret algorithms, business logic or cryptographic keys, that attackers may want to retrieve. The so-called "Man-At-The-End" attacks scenario (MATE) considers the case where the software users themselves are adversarial and try to extract such information from the code. These attackers may leverage diverse methods like symbolic analysis, code emulation and binary rewritting. Code obfuscation aims at protecting codes against such attacks, by transforming a sensitive program P into a functionally equivalent program P' that is more "difficult" (e.g., in money or time) to understand or to modify. On the flip side, code deobfuscation aims to extract information from obfuscated programs. Thus, obfuscation and deobfuscation confront themselves. Just like in many other cybersecurity domains, it is essential to be familiar with existing obfuscation and deobfuscation methods, as well as their evolution, in order to efficiently protect intellectual property held in software. In this presentation, we will first describe the MATE scenario. Second, we will give an overview of usual obfuscation and deobfuscation methods. Finally, we will present the latest progresses in deobfuscation, notably symbolic methods and black box attacks, and discuss mitigations.

Sébastien Bardin is a senior researcher at CEA LIST, where he has founded and now leads the BINSEC team devoted to security-oriented formal analysis of programs – with applications to vulnerability analysis, reverse, deobfuscation and code protection. Notably, Sébastien has performed pioneering work in the field of symbolic deobfuscation, and he is now interested in machine learning -based approaches to reverse engineering and deobfuscation. His results have been published in the best international security venues from academia (S&P, CCS) and industry (Black Hat). Sébastien holds a PhD in Computer Science from Ecole Normale Supérieure de Cachan. He is ACM Senior Member and CEA Fellow.

Grégoire Menguy is an engineer specialised in cybersecurity and certified ESSI by the ANSSI. He is actually a PhD student at CEA LIST, in the Binsec team, under the supervision of Sébastien Bardin. His research focuses on designing artificial intelligence and machine learning based methods for reverse engineering and deobfuscation. Especially, his work on black box deobfuscation has been published at the leading academic venue ACM CCS.

cea

DATE: June 8th, 2022

03:00 - 03:30 PM

Using Data-centric AI to stop attacks targeting data

Belkacem Teibi / **Inria / Daspren** and Mathieu Thiery / **Inria / Daspren**

Today, the first target of cyber-attacks is data. Increasingly sophisticated ransomware is demonstrating this every day. Existing protection solutions, massively based on binary or behavior analysis, are challenged over and over by new and unknown threats. Their defense strategy is insufficient. One thing is constantly neglected: data itself. Indeed, the first goal of ransomware is to alter data so that it becomes unusable. Yet very few solutions take this into consideration, and when they do, they use rudimentary techniques. There is an obvious answer to this issue: data-centric artificial intelligence. We use machine learning to generate models that are able to recognize sane data and legitimate modifications. When a malicious data manipulation occurs, the model diverges, allowing the detection of unknown attacks.

Being an R&D Engineer in cybersecurity with experience in industrialization and innovation transfer at Inria. Belkacem Teibi also holds an Executive MBA from Rennes School Business. He is currently CEO of Daspren.

Doctor in security and privacy, Mathieu Thiery worked in a startup where he developed a cryptographic driver in the Linux kernel. He is currently CTO of Daspren.

ALLISTENE
l'alliance des sciences
et technologies du numérique

DATE: June 8th, 2022

03:30 - 04:00 PM

HEIR - A holistic cyber-intelligence platform for secure healthcare environments

Michalis Smyrlis **/ SPHYNX** and Hervé Debar **/ Institut Mines Télécom**

HEIR (Grant Agreement 883275 – heir2020.eu) is a RIA project that aims to provide a thorough threat identification and cybersecurity knowledge base system addressing both local (in the hospital/ medical center) and global (including different stakeholders) levels. HEIR's threat hunting capabilities, incorporated in the final HEIR framework, will provide real time intelligent services, facilitated by advanced machine learning technologies, supporting the identification of the most common threats in electronic medical systems. The findings of the threat hunting capabilities, will be aggregated and will create an innovative benchmarking approach based on the calculation of the Risk Assessment of Medical Applications (RAMA) score. The latter will measure the security status of every medical device and provide thorough vulnerability assessment of hospitals and medical centers.

Michalis Smyrlis is the Chief Software Engineer at SPHYNX TECHNOLOGY SOLUTIONS AG. His interests revolve around the software security, privacy, cyber insurance, and big data. He has expertise in the development of security solutions for platforms supporting big data analytics and has worked in multiple H2020 EU projects. His research, as part of his Ph.D., is on cybersecurity risk assessment for cyber systems based on continuous and hybrid assurance assessment schemes.

Hervé Debar has been active in the cybersecurity domain for over 30 years, leading research and development activities in the private and public sector. He is one of the inventors of the Security Information and Event Management domain, which is now largely used for operational security purposes in many companies worldwide. He is the author of over a hundred scientific papers on cybersecurity, holds several patents, and has served as an editor for the IETF standard document on security message exchange format.

Institut Mines-Télécom

ALLISTENE
l'alliance des sciences
et technologies du numérique

DATE: June 8th, 2022

04:00 - 04:30 PM

Laser Fault Injection in MicroController

Jean-Luc Danger / **Télécom Paris**

This talk presents how a 32-bit Microcontroller (MCU) can be faulted by Laser Fault Injection (LFI). The fault can then be exploited to unveil secrets both from the software executed by the MCU and from the device architecture. Experiences have been carried out on an ARM Cortex M0+ processor in a SAMD21 MCU. The first operation for fault generation is to locate points of vulnerability in the MCU architecture, from The Flash memory to the processor execution pipeline via the internal bus and the cache. It is notably shown that the faults can be creating along this path and are particularly easy to generate on the Flash interface buffer. The fault model can be either “instruction skip” equivalent to a replacement by a NOP instruction, and a “instruction replay” where the current instruction is replayed and the new instruction is not executed. The study also presents the impact of the laser pulse width and the laser power. It shows that it is possible to inject multiple faults by increasing the pulse width. Two software countermeasures are presented to be resilient or detect the “instruction skip” fault type. One relies on code duplication, the other on the use of a sensitive instruction.

Jean-Luc Danger is a professor at Télécom Paris. He is in charge of the SSH research team whose research topics are security/safety of embedded systems, configurable architectures, implementation of complex algorithms in ASICs or FPGAs. Jean-Luc is the author of more than 250 scientific publications, 25 patents, has supervised 18 theses and co-founded the company Secure-IC.

DATE: June 8th, 2022

04:30 - 05:00 PM

Browser fingerprinting: past, present and possible future

Pierre Laperdrix **/ CNRS**

Browser fingerprinting has grown a lot since its debut in 2010. By collecting specific information in the browser, one can learn a lot about a device and its configuration. It has been shown in previous studies that it can even be used to track users online, bypassing current tracking methods like cookies. In this presentation, we will look at how this technique works and present an overview of the research performed in the domain over the past decade. We will see how this technique is currently used online before looking at its possible future.

Pierre Laperdrix is currently a research scientist for CNRS in the Spirals team in the CRIStAL laboratory in Lille, France. Previously, he was a postdoctoral researcher in the PragSec lab at Stony Brook University and, after, in the Secure Web Applications Group at Cispa. His research interests span several areas of security and privacy with a strong focus on the web. One of his main goal is to understand what is happening on the web to ultimately design countermeasures to better protect users online.

ALLISTENE
l'alliance des sciences
et technologies du numérique

DATE: June 9th, 2022

10:00 - 11:00 AM

Safe and secure: from safety analysis to process-oriented intrusion detection in industrial systems

Stéphane Mocanu / **Inria CTRL-A**

This talk aims to provide a cross domain view of safety and cybersecurity of industrial systems. Based of definition provided by industrial standards we position the problem of process-oriented attacks detection. Process oriented cyber-attacks are targeting directly the safety properties of physical processes. They are “stealth” attacks in the sense that they will not violate the communication protocol specifications but they will force process variables in order to bring the process into a dangerous state. Accordingly, intrusion detection techniques have to integrate the physical process property in order to detect malicious controls.
In this talk we provide the state of the art in the field of process-oriented intrusion detection, some recent advances, current challenges and limits.

Stéphane Mocanu obtained a Ph.D in Control Systems in 1999 from Grenoble-INP. He is assistant professor in Grenoble-INP and in Laboratoire d'Informatique de Grenoble (LIG, UMR 5217 CNRS/G-INP/UGA) in the joint Inria CTRL-A team. He starts working on industrial control systems cybersecurity in 2012 and he's running a large size experimental lab for industrial systems cybersecurity pentesting and vulnerability research (http://lig-g-ics.imag.fr/).

ALLISTENE
l'alliance des sciences
et technologies du numérique

DATE: June 9th, 2022

11:00 - 11:30 AM

Context-aware 6G security: the role of the physical layer

CHORTI Arsenia **/ ETIS / UMR8051 /CYU / ENSEA / CNRS**

Quality of security (QoSec) is envisioned as a flexible framework for future networks with highly diverse non-functional requirements (delays, energy consumption, massive connectivity / scalability, computational power, etc.). In parallel, the integration of communications and sensing, along with embedded artificial intelligence, can provide the foundations for building autonomous and adaptive security protocols. Mirroring the differentiated services (DiffServ) networking paradigm, different security levels could be conceptualized, moving away from static security controls, captured currently in zero-trust security architectures. In 6G, we envision autonomous and adaptive security controls, orchestrated by a vertical security plane in coordination with a vertical semantic plane, dubbed as context-aware 6G security. It is in this framework, that we envision the incorporation of physical layer security (PLS) schemes in 6G security protocols, introducing security controls at all layers, for the first time. In this talk, we will discuss how physical layer security (PLS), being naturally adaptive, fits in the QoSec framework; we will further propose a comprehensive roadmap for its incorporation in 6G, by leveraging adaptation of the transmission parameters to underlying security assumptions. Finally, we will present examples for RF fingerprinting based authentication and secret key generation (SKG) in real datasets and we will discuss the possibility of lightweight, distributed anomaly detection at the hardware layer for large scale Internet of Things (IoT) networks of constrained devices.

Arsenia (Ersi) Chorti is a Professor at the École Nationale Supérieure de l'Électronique et de ses Applications (ENSEA), Joint Head of the Information, Communications and Imaging (ICI) Group of the ETIS Lab UMR 8051 and a Visiting Scholar at Princeton and Essex Universities. Her research spans the areas of wireless communications and wireless systems security for 5G and 6G, with a particular focus on physical layer security. She is a Senior IEEE Member, member of the IEEE INGR on Security, the Competitive Pole Systematic and of the PhD Thesis GdR ISIS Award Committee. Since October 2021 she is chairing the IEEE Focus Group on Physical Layer Security.

DATE: June 9th, 2022

11:30 AM - 12:00 PM

Zero in on zero-day attacks at industrial scale using a model of coherent program behavior

Byron Hawkins / **Inria / Introspicion**

According to a study conducted by researchers at MIT, the year 2021 saw 66 zero-day vulnerabilities in active use by malicious parties, compared to just 37 in 2020. On the black market, a zero-day can go for a million dollars or more, and both cyber criminals and governments investigators have invested millions to acquire them. Damage caused by exposed zero-days reaches into the billions. Attacks have targeted the range of vulnerable parties, from Fortune 500 companies to SMBs to public and private institutions and even individuals.

These attacks largely exploit vulnerabilities that arise from the increasing complexity of software, which is being ever more deeply integrated into organizational operations. Among current techniques for vulnerability detection, those capable of reliably identifying potential zero-day attacks require astronomical computing resources. For this reason, dynamic surveillance of software interfaces has become the defense of choice--but advanced attacks are often invisible at the interface layer, whereas monitoring systems have limited ability to evaluate the internal behavior within an executing program. To address this problem, the software security tool Introspicion can rapidly analyze binary executions at high precision. We propose two usage models: (1) Introspicion Reactive integrates into an EDR to raise alerts when untrusted execution paths and data flows are observed, and (2) Introspicion Proactive broadens the range of program vulnerabilities that can be detected in an offline analysis. Both tools rely on an innovative technique for modeling trusted execution paths and data flows in binary executables.

A central challenge of this approach is the vast number of possible program execution paths and data flows, making a pure-software implementation impractical. For this reason, the Introspicion analysis relies on the CPU trace module (Intel PT, Arm CoreSight) to provide complete execution paths and efficient data flow samples at a runtime overhead of just 1% for typical programs.

Byron Hawkins received a PhD from the University of California with an innovative approach to the detection of zero-day attacks that target arbitrary code execution. As a doctoral intern, he developed innovative security tools at Google (guided fuzzing under Dr. Memory) and Microsoft (encryption of sensitive pointers in the Visual Studio compiler). After joining Inria, his work has focused on graph algorithms and compression of software execution traces. In 2021 the project transitioned to Inria's Startup Studio under the name Introspicion.

DATE: June 9th, 2022

03:00 - 03:30 PM

Nijta: A voice anonymization solution to protect speaker's privacy

Brij Mohan Lal Srivastava **/ Inria**

Today's definition of a customer centric business model is very often incomplete without automatic speech processing components which aim to serve the clients' needs efficiently. However, deploying these components results in large-scale voice data collection containing private, sensitive, and personally identifiable information about the speakers. European privacy laws such as the GDPR require data anonymization and removal of the biometric information from the collected speech data.

We address this challenge by providing a robust and secure voice anonymization platform, Nijta, which quickly removes speaker's personally identifiable information from their voice data. The process of anonymization grants wide access of this data to the organizations, while allowing them to have trustful GDPR-compliant user interaction with their customers. Moreover, it enhances the usefulness of customer's data to optimize dominant business components like speech transcription systems, leading to more accurate extraction of metadata from voice, like customer preferences, emotions, etc.

Brij Mohan Lal Srivastava is the project holder of Nijta at Inria Startup Studio located in Lille. Previously during his PhD at Inria Lille and Nancy, he worked with Magnet and Multispeech teams to investigate the topic of privacy in speech processing. He, along with his collaborator Nathalie Vauquier and Seyed Ahmed Hosseini, is currently working towards creating a startup to provide commercial voice anonymization service to call centers and media organizations.

ALLISTENE
l'alliance des sciences
et technologies du numérique

DATE: June 9th, 2022

03:30 - 04:00 PM

The resilience of post-quantum cryptography to physical attacks

Mikael Carmona / **CEA**

The transition from classical cryptography to post-quantum cryptography is launched. The first cryptosystems standardized by NIST will be known in 2022 and products integrating this new cryptography are already on the market. The NIST standardization process has tested the resistance of these new cryptosystems to quantum attacks, what about their resilience to physical attacks? In this presentation, we will present the panorama of post-quantum cryptosystems selected by the NIST as well as the identified vulnerabilities to physical attacks. A particular focus will be proposed on the SIKE and HQC schemes whose vulnerabilities to physical attacks have been revealed by CEA-Leti and published at international congresses including the 3rd PQC conference organized by NIST in 2021.

Mikael Carmona is a graduate engineer from the INPG (2007), agrégé in mathematics (2007) and a graduate doctor from the INPG in signal processing (2011). Engineer-Researcher at CEA-Leti from 2011 to 2015 on the theme of sensor networks and the digital twin of structures, he co-founded the start-up Morphosense as CTO in which he contributes to the establishment and execution Technological and Operational roadmaps. In 2021, he joined the Cybersecurity department of CEA Leti in the field of post-quantum cryptography and random number generators. He is currently Head of the Security of Components Laboratory.

cea

ALLISTENE

l'alliance des sciences
et technologies du numérique