28th IEEE International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE-2019)

Conference Program

Key Note Speakers

Dr. Jesus Luna Garcia has a PhD in Computer Architecture from the "Technical University of Catalonia" (UPC, Spain 2008) and was a postdoctoral researcher with the CoreGRID NoE (Greece/Cyprus, 2008-2009). He has more than 20 years of experience in the field of computer security working with both public and private sector companies and universities, in America and Europe. His professional experience includes Robert Bosch GmbH (Germany), Cloud Security Alliance (U.K.), and the Technical University of Darmstadt (Germany). Jesus Luna has co-authored more than 40 publications including scientific papers, ISO/IEC and NIST standards, and a patent. Currently, he works with Robert Bosch GmbH where he contributes to the security governance of its cloud ecosystem. His topics of interest include security assessment, security automation, trust management, and risk management.

Holistic IoT security as a digital transformation's enabler
In the so-called "digital transformation", industries all over the world are nowadays moving towards an ecosystem of pervasive computing characterized by the notion that "everything is connected" in an Internet of Things (IoT). In this "hyper-connected world", there is interactive intelligence all around us: physical products and infrastructure are no longer mere objects, but sensible things that can in many cases understand our human intentions and adapt accordingly. Actuators adapt to the environment through the application of machine learning and natural language interfaces, together with cloud-based information resources.
Unfortunately, recent examples of IoT- related security breaches show us that the immense promise of "connected everything" is counterbalanced by the equally immense challenge of securing billions of devices (some of which are not always designed or set up to function securely when connected to the internet). The correct handling of IT security is key to unlocking the full potential of the digital transformation, which composes well-known challenges related to underlying technologies and complex IT systems.
This presentation will offer IT security recommendations for establishing end-to-end trust in these complex ecosystems, in particular by providing answers to the following:
1. Why it is essential to consider the security aspects of the full technology stack from back-end solution components (e.g., cloud) to edge networks, gateways, and devices? 2. Why the full security life-cycle must be taken into account, from conception and design, to continuous operation, and end-of-life decommissioning?
Finally, this presentation will also discuss some positive implications of the holistic IoT security approach in relationship to the upcoming European Cybersecurity Act, in particular related to the continuous security certification of cloud back-ends.

Christian Banse is the head of the department "Service and Application Security" at Fraunhofer AISEC. The primary focus of the department is to develop and research tools and technologies to analysis and strengthen the security of software. This includes mobile application as well as Cloud and Edge Computing. Christian has been an employee of Fraunhofer AISEC since 2011. He has a Master of Science degree in Management Information Systems from the University in Regensburg and is the author of several publications in the field of network and Cloud security.

Establishing Continuous Security in Multi-Cloud Environments
Security is still regarded as the most inhibiting factor for companies moving into the Cloud. While recent trends show that Cloud vendors are increasingly aware of this and are providing the necessary tools to secure the Cloud workloads of their customers, it is still a challenge to continuously ensure security in environments involving multiple Cloud providers. This is especially the case if multiple Cloud offerings include different service levels ranging from IaaS to SaaS, since the shared responsibilities regarding security between Cloud consumer and cloud customer are often not clearly defined. Additionally, further research has to be done in regards to the meaning of continuous in the context of Cloud security. What are sensible intervals to check certain security configuration settings? While it might suffice to check the expiration of a password on a daily basis, the firewall configuration of a virtual machine might need checks in a per-hour interval or even less. Furthermore, new paradigms such as serverless computing can be leveraged to check security settings on change rather than in a regular interval. Another big challenge the community is facing, is the comparison of evidences generated from different heterogeneous ders because of their heterogeneous nature. While there are some Cloud computing standards in the on-premise world, such as OpenStack, the commercial Cloud providers rarely follow these standards and technologies need to be developed to quickly adapt to different APIs of different Cloud providers. On the other hand, the rise of containers and especially the establishment of Kubernetes as the de-facto container management solution can be used to mitigate this to a certain degree.
This talk will highlight how the research department "Service and Application Security" of Fraunhofer AISEC is tackling those questions, especially in the context of Cloud service certification. It will give insight into the works conducted at the Fraunhofer AISEC laboratories, especially Clouditor, which is currently being piloted on a European level in the Horizon 2020 project EU-SEC (www.sec-cert.eu). Clouditor follows a test-based certification approach and can be used to check the security configuration of different Cloud workloads, for example in the course of an compliance audit. To compare security settings of different Cloud providers and even different service offerings, Fraunhofer AISEC is currently developing a domain-specific language based on a context-free grammar to easily model security requirements of Cloud resources.

June 12 – Room 1

June 12	Room 1	
8.00		**Registration**
9.00	**Opening**	**Welcome**
9.15		**Key Note Speaker – Jesus Luna**
10.00	**CDCGM Track**	
		Roberto Melo and Douglas Macedo **A Cloud Immune Security Model Based on Alert Correlation and Software Defined Network** Mario Barbareschi, Alessandra De Benedictis, Erasmo La Montagna, Antonino Mazzeo and Nicola Mazzocca **PUF-enabled Authentication-as-a-Service in Fog-IoT systems** Mario Antonio Dantas, Paulo Bogoni and Paulo Freitas **An Application Study Case Tradeoff Between Throughput and Latency on Fog-Cloud Cooperation**
11.15	**Coffee break**	
11.35	**CDCGM Track**	
		Georgia Garani, Andrey Chernov, Ilias Savvas and Maria Butakova **A Data Warehouse Approach for Business Intelligence** Salvatore Venticinque, Beniamino Di Martino, Rocco Aversa, Marit Natvig, Shanshan Jiang and Regina Enrich Sard **Evaluating Technology Innovation for E-Mobility** Rao Mikkilineni and Giovanni Morana **Post-Turing Computing, Hierarchical Named Networks and a New Class of Edge Computing**
12:50	**Lunch Break**	
14:30	**CDCGM Track**	
		Dorian Knoblauch and Christian Banse **Reducing implementation efforts in continuous auditing certification via an Audit API** Enrico Russo, Luca Verderame and Alessio Merlo **Towards Policy-driven Monitoring of Fog Applications** Luciano Ocone, Massimiliano Rak and Umberto Villano **Benchmark-based Cost Analysis of Auto Scaling Web Applications in the Cloud**
15:45	**Coffee break**	
16:15	**ACEC Track**	
		Nicola Bicocchi, Giacomo Cabri, Letizia Leonardi and Giulio Salierno **A Survey of the Use of Software Agents in Digital Factories** Wissem Eljaoued, Nesrine Ben Yahia, Narjès Bellamine Ben Saoud and Chihab Hanachi **A Hybrid Recommendation Approach for Agent Organizational Structures** Claudia Di Napoli, Silvia Rossi and Emanuela Del Grosso **Robotic Entertainments as Personalizable Workflow of Services: a Home-Care Case Study** Carmelo Fabio Longo, Corrado Santoro and Federico Fausto Santoro **Meaning Extraction in a Domotic Assistant Agent Interacting by means of Natural Language**

June 12 – Room 2

June 12	Room 2	
8.00		**Registration**
10.00	**AROSA Track**	
		Guido Perboli, Alessandro Manfredi, Stefano Musso and Mariangela Rosano **A decentralized marketplace for M2M economy for Smart Cities** Marwa Mdimagh and Sami Bhiri **Towards Automated and Fine-grain Reuse of Configurable Business Process models**
11.15	**Coffee break**	
11.35	**AROSA Track**	
		Mouna Rekik, Abderrahim Ait Wakrime, Nasreddine Cheniki and Yacine Sam **On the Fly Reconfiguration of BPaaS based on SaaS Services Federation and SAT Solving Techniques** Zakaria Afkir, Hatim Guermah, Mahmoud Nassar and Sophie Ebersold **Machine learning based approach for context aware system**
12:50	**Lunch Break**	
14:30	**FISA Track**	
		Mouna Rhahla and Mouna Rhahla **A GDPR controller for IoT systems: Application to e-health** Wided Mathlouthi, Chahrazad Labba, Walid Gaaloul and Narjès Bellamine Ben Saoud **SoS paradigm benefits SaaS Integration: novel approach and first results** Fatma Raissi, Sami Yangui and Frederic Camps **Autonomous Cars, 5G and Smart Cities: Beyond the Hype**
15:45	**Coffee break**	
16:15	**FISA Track**	
		Amina Brahem, Nizar Messai, Yacine Sam, Sami Bhiri, Thomas Devogele and Walid Gaaloul **Blockchain's fame reaches the execution of personalized touristic itineraries** Nasredine Cheniki, Marwa Boulakbech, Hamza Labbaci, Yacine Sam, Nizar Messai and Thomas Devogele **A Linked Open Data Approach for Touristic Service Recommendation**

June 13 – Room 1

June 13	Room 1	
9.15		**Key Note Speaker – Christian Banse**
10.00	**Web2Touch Track**	
		Marbilia Sergio, Talita Sousa Costa, Marcelo S. P. Pessoa and Paulo S. M. Pedro **Semantic approach as support in the analysis of abstracts in the literary review** Nabil Badr, Maddalena Sorrentino, Marco De Marco and Mariagrazia Fugini **Improving Interaction in Integrated Chronic Care Management** Mariagrazia Fugini, Jacopo Finocchi, Paolo Locatelli, Filippo Leccardi and Alfredo Lupi **A Text Analytics Architecture for Smart Companies**
11.15	**Coffee break**	
11.35	**Web2Touch Track**	
		Pasquale Ardimento, Mario Luca Bernardi, Marta Cimitile and Giuseppe De Ruvo **Mining developer's behavior from web-based IDE logs** Allan Mazimwe, Imed Hammouda and Anthony Gidudu **Content Ontology Design Patterns for Representing Knowledge in the Disaster Risk Domain** Julio Cesar Dos Reis, Rodrigo Bonacin and Luma Lombello **Soft Ontologies as Fuzzy RDF Statements** Christian Esposito and Oscar Tamburis **An Effective Retrieval Approach for Documents related to Past Civil Engineering Projects**
12:50	**Lunch Break**	
14:30		**EU SPACE Special Session**
15:45	**Coffee break**	
16:15	**Web2Touch Track**	
		Marcos Vinícius Borges, Julio Cesar dos Reis and Guilherme Gribel **Empirical Analysis of Semantic Metadata Extraction from Video Lecture Subtitles** Amira Mouakher, Rami Belkaroui, Aurélie Bertaux, Ouassila Labbani, Clementine Hugol-Gential and Christophe Nicolle **An Ontology-Based Monitoring System in Vineyards of the Burgundy Region**
19:00		**Social Dinner**

June 13 – Room 2

June 13	Room 2	
10.00	**VSC Track**	
		Konstantin Scherer, Tobias Pfeffer and Sabine Glesner **I/O Interaction Analysis of Binary Code** Fabio Martinelli, Francesco Mercaldo and Antonella Santone **Real-Time SCADA Attack Detection by means of Formal Methods** Andrea Fornaia, Stefano Scafiti and Emiliano Tramontana **JSCAN: Designing an easy to use LLVM-based Static Analysis Framework**
11.15	**Coffee break**	
11.35	**VSC Track**	
		Emiliano Tramontana and Gabriella Verga **Mitigating Privacy-related Risks for Android Users** Antonio Borrelli, Giuseppe Antonio Di Lucca, Vittoria Nardone and Antonella Santone **Formal Verification of Radio Communication Management in Railway Systems Using Model Checking Technique**
12:50	**Lunch Break**	
14:30	**CONESEC Track**	
		Piotr Bienias, Grzegorz Kołaczek and Arkadiusz Warzyński **Architecture of Anomaly Detection Module for the Security Operations Center** Hassan Mokalled, Rosario Catelli, Valentina Casola, Daniele Debertol, Ermete Meda and Rodolfo Zunino **The applicability of a SIEM solution: Requirements and Evaluation**
15:45	**Coffee break**	
16:15	**WETICE Track**	
		Luigi Sgaglione, Luigi Coppolino, Salvatore D'Antonio, Luigi Romano, Giovanni Mazzeo, Domenico Cotroneo and Andrea Scognamiglio **Privacy preserving Intrusion Detection via Homomorphic Encryption** Meriem Guerar, Luca Verderame, Mauro Migliardi and Alessio Merlo **2GesturePIN: Securing PIN-based Authentication on Smartwatches**
19:00		**Social Dinner**

June 14 – Room 1

June 14	Room 1	
9.00	**DEW Track**	
		George Pacheco Pinto and Cassio Prazeres **Web of Things Data Visualization: From Devices to Web via Fog and Cloud Computing** Stefanie Urchs, Lorenz Wendlinger, Michael Granitzer and Jelena Mitrović **MMoveT15: A Twitter Dataset for Extracting and Analysing Migration-Movement Data of the European Migration Crisis 2015** Barbara Pes **Handling class imbalance in high-dimensional biomedical datasets** Roberto Cocco, Maurizio Atzori and Carlo Zaniolo **Machine Learning of SPARQL Templates for Question Answering over LinkedSpending** Cecilia Di Ruberto, Andrea Loddo and Giorgia Campanile **An Open Source Plugin for Image Analysis in Biology**
11.15	**Coffee break**	
11.35	**WETICE Track**	
		Valentina Casola, Rosario Catelli and Alessandra De Benedictis **A first step towards an ISO-based Information Security Domain ontology** Vincenzo Norman Vitale, Sergio Di Martino, Adriano Peron and Alberto Riccabone **Industrial Internet of Things: Persistence for Time Series** Riccardo Di Pietro, Marco Scarpa and Antonio Puliafito **How much enhancing Confidentiality and Integrity on data can affect Mobile Multi-Cloud: The ARIANNA Experience** Fahad Anwaar, Naima Iltaf, Hammad Afzal and Haider Abbas **A Deep Learning Framework to Predict Rating using Item Metadata for Cold Start Item**
12:50	**Lunch Break**	

June 14 – Room 2

June 14	Room 2	
9.00	**SSTM Track**	
		Mathias Morbitzer **Scanclave: Verifying Application Runtime Integrity in Untrusted Environments** Abhinav Khare, Giovanni Merlino, Francesco Longo, Antonio Puliafito and Om Prakash Vyas **Toward a Trust-less Smart City: The #SmartME Experience** Mourad Benmalek, Yacine Challal and Abdelouahid Derhab **Authentication for Smart Grid AMI systems: Threat models, Solutions, and Challenges** Farah Saleem, Naima Iltaf, Hammad Afzal and Mobeena Shahzad **Using Trust in Collaborative Filtering for Recommendations**
11.15	**Coffee break**	
11.35	**COMETS Track**	
		Mamadou Lakhassane Cissé, Hanh Nhi Tran, Samba Diaw, Bernard Coulette and Alassane Bah **Using Patterns to parameterize the execution of Collaborative Tasks** Saloua Bennani, Sophie Ebersold, Mahmoud El Hamlaoui, Bernard Coulette and Mahmoud Nassar **A collaborative decision approach for alignment of heterogeneous models** Jalal Possik, Andrea D'ambrogio, Gregory Zacharewicz, Aicha Amrani and Bruno Vallespir **A BPMN/HLA-Based Methodology for Collaborative Distributed DES**
12:50	**Lunch Break**	

European Projects Special Session

CLASS is an H2020 European founded research project in big data analytics. The vision of CLASS is that the pressure that the newest smart systems requiring big data analytics and real-timerequirements will put on the compute continuum (composed by Edge, Fog and Cloud computing), can be efficiently addressed by devising a full distributed system architectures in which a combined data-in-motion and data-at-rest analytics can be efficiently performed by coordinating edge and cloud computing resources.CLASS aims then to develop a novel software architecture to help programmers and big data practitioners to combine data-in-motion and data-at-rest analysis, by efficiently distributing data and process mining along the compute continuum, while providing real-time guarantees.
Moreover, CLASS aims to take full advantage of novel parallel hardware and software architectures for an efficient usage of computing resources to achieve the level of performance required by future smart systems. To demonstrate the feasibility of such architecture, a heterogeneous set of big data analytics tools are planned to be deployed, providing integrated services to consumers. CLASS aims to implement its innovative framework on a use-case based on a real Smart City scenario, the Modena Automotive Smart Area (MASA), for next-generation automotive applications, adopting innovative distributed architectures from the high-performance computing (HPC) domain, as well as highly-parallel and energy efficient hardware platforms from the embedded domain. In order to do so, it plans to combine multi-dimensional and multidisciplinary contexts, from artificial intelligence, data storage and data mining, to address the big data challenge of future smart cities.

Website:
https://class-project.eu/

PRYSTINE (PRogrammable sYSTems for INtelligence in automobilEs) is a Horizon 2020 project funded by the ECSEL programme. Its start date is April 1, 2018, and it lasts three years.

PRYSTINE aims to develop an innovative technological stack named FUSION (electronic components, embedded hardware and software/networking systems) for Autonomous Driving (AD) and advanced driver assistance, as well as to enhance consciousness and knowledge of both end-users and industry about this technology.
PRYSTINE partners form a consortium with heterogeneous competences. These competences can be grouped to work on logically affine tasks in what are called Supply Chains (SCs) to achieve a given result (e.g. produce a piece of the technological stack, or a demonstrator).
The High-performance Real-Time Lab (HiPeRT) from UNIMORE is are actively involved in four SCs

- SC2: develop the next-generation HW/SW model architecture (using also the embedded components developed by SC1) to enable integration of conventional control theory and signal processing solutions with AI models into AD embedded intelligent agents;
- SC4: develop fail-operational robust sensor-fusion and decision-making models (embedded intelligent agents);
- SC6: use FUSION technological stack to set up a demonstrator of a passenger vehicle;
- SC7: develop a “co-driver” model to study feasibility of shared control between the driver and the AI agent;

Website:
https://prystine.eu/

The project “vF Interoperation suppoRting buSiness innovaTion” (**FIRST**) provides new technology and methodologies to describe manufacturing assets; to compose and integrate existing services into collaborative virtual manufacturing processes, and to deal with the evolution of changes.
The aim of the project is to provide a foundation for innovations to contribute to virtual interoperation of smart manufacturing in the area of Factory of the Future/Manufacturing 2.0 to improve the competitiveness of our industrial partners and sustainability of Europe manufacturing sector. Within this research programme, industrial researchers will get the opportunity to gather knowledge in academia while academic researchers will get knowledge in industries.
The consortium involves the Bournemouth University (UK), the University of Groningen (NL), the Sapienza University of Rome (IT), the Second Shanghai Polytecnic University (CN), the Università di Modena e Reggio Emilia (IT), the GK Software (DE) and the KMSoft (CN).

Website:
https://www.h2020first.eu/

The project “European Security Certification Framework” (**EU-SEC**) aims to create a European framework for certification schemes and evaluation concepts to secure cloud infrastructures. Within this framework, existing national and international certifications can co-exist. EU-SEC will improve the business value as well as the effectiveness and

efficiency of existing cloud security certification schemes.

In the WETICE EU Project space we are presenting the EU-SEC approach for adopting Continuous Auditing based Certification scheme for Cloud Services. This will include a demo session showing the tools currently piloted as part of the project with a Spanish bank and Austrian Cloud Service Provider.

Website:
https://www.sec-cert.eu

ARTICONF researches and develops a novel set of trustworthy, resilient, and globally sustainable decentralised social media services. ARTICONF addresses issues of trust, time-criticality and democratisation for a new generation of federated infrastructure, to fulfil the privacy, robustness, and autonomy related promises that proprietary social media platforms have failed to deliver so far. Namely, its goals are to:

- simplify the creation of open and agile social media ecosystem with trusted participation using a two-stage permissioned blockchain;
- automatically detect interest groups and communities using graph anonymization techniques for decentralised and tokenized decision-making and reasoning;
- elastically auto scale time-critical social media applications through an adaptive orchestrated Cloud edge-based infrastructure meeting application runtime requirements; and
- enhance monetary inclusion in collaborative models through cognition and knowledge supply chains.

Website:
https://articonf.eu/

Defending the European Energy Infrastructures (**DEFENDER**) aims to model CEIs as distributed Cyber-Physical Systems for managing the potential reciprocal effects of cyber and physical threats. Moreover, it aims to deploy a novel security governance model, which leverages on lifecycle assessment for cost-effective security management over the time. Finally, it aims to bring people at centre stage by empowering them as virtual sensors for threat detection, as first level emergency responders to attacks, or by considering workforce as potential threats.
With these aims, DEFENDER will adapt, integrate, upscale, deploy and validate a number of different technologies and operational blueprints with a view to develop a new approach to safeguard existing and future European CEI operation over cyber-physical-social threats, based on a) novel protective concepts for lifecycle assessment, resilience and self-healing offering "security by design" and b) advanced intruder inspection and incident mitigation systems. DEFENDER framework will combine a range of devices/technologies for situational awareness (fixed sensors, like PMUs, smart meters, laser fence sensors, and mobile devices, like drones and advanced video surveillance) based on an intelligent processing for cyber-physical threat detection with a toolbox for incident mitigation and emergency response and Human- In-The-Loop for managing people interaction with CEI, while leveraging on blockchain technology for peer-to-peer trustworthiness.
The effectiveness of DEFENDER will be extensively validated on 4 real life demonstrators (in France, Italy and Slovenia) fully covering the overall energy value chain, ranging from a bulk generation plant (ENGIE SA), to a decentralized RES generation (BFP), a TSO High Voltage network (ELES), a DSO Medium/Low Voltage network (ASM) and a business prosumer.
DEFENDER provides a CEI threat analysis and classification, including a holistic threat agents taxonomy as a further basis for threat modelling and analysis of unknown threats. Also, the analysis and validation of the DEFENDER key design objectives, namely CEI Security Lifecycle Assessment by design, Resilience by design, CEI Survivability by design and CEI Data Privacy by design are carried out.
DEFENDER offers incidents mitigation via a number of technology innovations. The DEFENDER Incident and Mitigation Detection provides a clear set of models for manage incidents and countermeasures. The DEFENDER CEI Security Control Centre allows CEI operators to overview the security state of the CEI areas of their responsibilities and react while the Incidents Mitigation Decision Support System proposes a number of mitigation actions and technological countermeasures taking into account specific DS-SLAs and priorities in order to minimize downtime and cascading effects.
DEFENDER aims to build a platform for incidents and countermeasures information exchange at European level. The resulting architectural design has a clear big-data orientation and is managed via a set of state-of-the-art open source services. DEFENDER creates a Culture of Security, where trusted information exchange between trained employees and volunteers will complement cyber-physical protection, while preserving the privacy of the citizens involved. The promotion of the results of DEFENDER at the level of scientific research, with a clear industry focus is one of the main goals of the project.

Website:
http://defender-project.eu/