End-to-end Cybersecurity

J. Münther
Head of Security Engineering
ams OSRAM AG, Information Security, Berlin, Germany

Biography
Session Chair

References

Taming the IoT Cybersecurity Wicked Challenge

J. Moor
Managing Director
IoT Security Foundation, Livingston, United Kingdom

Abstract
This talk addresses the critical challenges of managing product cybersecurity throughout the lifecycle, and across applications. Aimed at designers, developers, and manufacturers with a blend of technical and management skills, the presentation will elucidate the multifaceted nature of IoT security challenges. It will emphasize the need for fit-for-purpose security that aligns with application requirements, regulatory compliance, and lifecycle management. The conclusion underscores the importance of a collaborative and evolving security methodology to address the dynamic challenges of IoT security, inviting all stakeholders to participate.

Biography
John Moor is co-founder and Managing Director of the IoT Security Foundation (IoTSF).

He has over 30 years of experience in electronic systems and microelectronics industries and holds executive leadership and general manager responsibilities for IoTSF. Previously John served as a vice-

president at the UK's National Microelectronics Institute (NMI) where he was tasked with formulating strategy and leading key innovation initiatives. Before NMI, John was one of the founders of Bristol-based start-up ClearSpeed Technology (formerly PixelFusion Ltd). During this time he led engineering operations at the vice-president level. He was responsible for technology acquisitions, establishing international supply chain operations and acquiring capability in the UK, USA and Taiwan.

John holds an MA (Distinction) in Strategic Marketing Management from Kingston University London and a Master of Business Administration from the University of Leicester. John’s formative embedded systems engineering career centred on leading-edge microprocessor-based systems (substantially parallel systems) and used in data communications, high-performance computing, graphics and virtual reality applications.

References

Total Defense High Tech

A. Reijmer
Chief Security Officer
ASML, Veldhoven, Netherlands

Abstract
Our industry is increasingly confronted with cybercrime and corporate espionage activities, attempting to exfiltrate intellectual property, engineering information, and customer confidential information for commercial gain or to disrupt business operations. These attacks extend beyond corporate boundaries to our supplier and customer ecosystems. The geopolitical relevance of cyber security has grown tremendously in the recent years in our sector, looking at the nefarious interest to obtain intellectual property and knowledge required for manufacturing high tech products.

This presentation proposes a collaborative approach to reduce Cyber Risk in the High Tech / Semi and Defense industry.

Biography
•As CISO at ASML, Aernout implemented significant security capabilities for ASML (including a 10 fold increase in investments and even more for organization) in the domain of Information, IT, Human and Physical Security.
•Executed for 8 consecutive years the Security Roadmap, running a portfolio of security projects, working away a historic backlog and achieving decent maturity level.
•Spearheaded SIA's and SEMICON CISO workgroup (US), the same for multinationals in NL, with the NL CISO Circle of Trust.
•Became CISO of BT Global Services at the early age of 33 through a track record of solid execution and delivery.
•While at BT, responsible for global security outside the UK. Brought security maturity to operational excellence level in 30 (mostly newly acquired) entities

References

Empowering the semiconductor industry with advanced cybersecurity

P. Lisci
Regional Sales Director
HCLTech, Düsseldorf, Germany

Abstract
The presentation on ‘Cybersecurity in the Semiconductor Industry’ by HCLTech highlights the key challenges and solutions for securing semiconductor manufacturing environments. It focuses on vulnerabilities in fab environments, notably those arising from the use of outdated operating systems and legacy ports, which pose significant security risks. The presentation also explores impact of cybersecurity breaches on OEM after-sales services and discusses the evolving regulations from the Bureau of Industry and Security of the U.S. Department of Commerce. HCLTech's approach emphasizes compliance with the latest SEMI security standards, such as E187 and the implementation of DevSecOps practices for cloud applications. It stresses the importance of secure collaboration within the global supply chain and the integration of Digital Rights Management solutions. Furthermore, it outlines HCLTech's holistic cybersecurity services, which includes audits, vulnerability management, incident response and secure software development – tailored to meet the requirements of the European Cyber Resilience Act (CRA).

Biography
Philipp Lisci is an accomplished IT professional with over two decades of experience in the technology sector, specializing in network security, performance management and virtualization solutions. He has made significant contributions at leading organizations, where he played pivotal roles in advancing cybersecurity, optimizing application performance and enabling cloud transformation. Philipp's extensive technical expertise, specifically in cloud security and enterprise networking, has enabled organizations to strengthen their security postures and IT efficiency. Renowned for his leadership and mentoring skills, he is passionate about fostering talent and sharing his knowledge within the IT community. His strategic vision and commitment to innovation continue to drive significant value in the tech industry.

References

Cybersecurity for Next Generation Critical Instructure Systems

A. Marnerides
Asst. Professor
University of Cyprus, Department of Electrical & Computer Engineering, KIOS Centre of Excellence, Nicosia, Cyprus

Abstract

Critical Infrastructure Systems (CIS) composing Critical National Infrastructures (CNIs) enabling sectors such as power, manufacturing, nuclear, defence, space and transport are underpinned by Industrial Control Systems (ICS) that have recently been exposed to the Internet and the Internet-of-Things (IoT) technologies by virtue of urging business models. Evidently, this relatively recent interface of such traditionally isolated setups with the IoT has resulted to a rapid surge of sophisticated and targeted Advanced Persistent Threats (APTs) causing significant safety as well as monetary effects on a global scale. Such attack vectors are stealthy, and they target hardware and logical processes that are typically resource-constrained and unprotected. Moreover, they are used frequently in several malicious cyber operations such as nation-sponsored cyberwarfare and cybercrimes. Therefore, a great challenge and need exists on developing and evaluating defence and mitigation mechanisms within realistic setups that also adhere to ICS vendor-oriented and proprietary software nature. In this talk, we will focus on illustrating the vulnerability spectrum of ICS devices as well as on-going activities on how generalised vendor-independent solutions can be developed via real use cases in the context of the power, utilities and defence sectors.

Biography

Dr. Angelos K. Marnerides is an Asst. Professor of Cyber Physical Systems Security at the University of Cyprus, in the Department of Electrical & Computer Engineering and a faculty member leading activities in cybersecurity research at the KIOS Research and Innovation Centre of Excellence. Previously, he was a Assoc. Professor at the University of Glasgow (UofG), leading the Glasgow Cyber Defence Group and all the cybersecurity research activities across all research sections in the School of Computing Science at UofG. His research focuses on applied security and resilience for Internet-enabled cyber physical systems using data-driven approaches with focus on critical national infrastructures in various sectors including energy, defence, manufacturing and water utilities. Dr. Marnerides' research has received significant funding in excess of €8M+ from the industry (e.g., Fujitsu, BAE, Raytheon, EDF), governmental bodies (e.g., EU, IUK, EPSRC) as well as UK national security and defence agencies (e.g., NCSC, GCHQ, MoD Dstl). Dr. Marnerides is currently the project coordinator for the €5.8M COCOON project funded by the EU Horizon Innovation Action (IA) being the first ever EU IA project coordinated by UCY KIOS and UCY in general. He is a malware detection patent author and has published extensively in top-tier IEEE/ACM conferences and journals. Moreover, he is a Senior Member (SMIEEE) of the IEEE and a member of the ACM since 2007. Dr. Marnerides has also played significant roles in various IEEE conferences, earning IEEE ComSoc contribution awards in 2016 and 2018. He obtained his PhD in Computer Science from Lancaster University in 2011 and has held lectureships and postdoctoral positions at institutions including Carnegie Mellon University, University of Porto, University College London, and Lancaster University.

References

Product Security for Trusted Electronics: A Holistic Approach

K. Papapanagiotou
Advisory Services Director
Census S.A., Athens, Greece

Abstract
Electronics are more prevalent than ever in our lives. We are becoming more and more dependant on them as they play a signicant role in critical domains such as healthcare, communications, automotive, and even defense. Undoubtedly, the regulatory compliance landscape is becoming more complex and strict, aiming to protect the society from risks related to the use of such electronic devices. Regulations like NIS 2 and the EU Cyber Resilience Act set specific requirements for manufacturing trusted electronics. At the same time attacks occur, which demonstrate that the industry is not well prepared or mature enough. Furthermore, new technologies that are introduced bring about exiting capabilities but also challenges for cybersecurity.
In this presentation we will provide an outline of the steps that need to be taken to create trusted electronics. The approach that we will present takes into account lessons learned from other sectors, such as medical devices, to introduce security activities throughout the product development lifecycle. Starting from security reqiurements and threat modeling, and continuing until product validation, testing, and field operation, we will present how you can ensure that a secure product can be built without interruptions or delays in the production timeframe.

Biography
Dr Konstantinos Papapanagiotou is the Advisory Services Director at Census Labs S.A. Prior to that, he worked for OTE S.A. (member of Deutsche Telekom Group) where he was responsible for the cyber security solutions offered to corporate customers. In the past he has led cyber security consulting teams in other private sector organizations.
Dr Papapanagiotou has more than 20 years of experience in the field of cyber security both as a corporate consultant and as a researcher. During that time, he participated in numerous cyber security projects in public and private sector organizations, in Greece, Europe, and the Middle East.
He holds a PhD and BSc from the Department of Informatics and Telecommunications at the University of Athens, Greece, as well as a MSc in Information Security with distinction from Royal Holloway, University of London. For more than 10 he served as an Adjunct Lecturer at the Hellenic American University, as well as the University of Athens and University of Piraeus, teaching Information Security to postgraduate and undergraduate students.

References

From Full Product to Nanometers: Risks and Mitigations of Hardware-Based Attacks

F. Courbon
CEO
Ethicronics, Cambridge, United Kingdom

Abstract
The semiconductor industry is the backbone of modern electronics, but it faces unique challenges in cybersecurity. With increasing complexities in semiconductor design and manufacturing, the risks posed for instance by counterfeit, compromised or not secure hardware are greater than ever. This is especially true for fabless companies operating in sectors like defence, telecoms, aerospace, automotive, critical infrastructure and consumer electronics. This talk will present some practical attacks, highlight the need of a scalable solution for electronics hardware assurance and present the journey of Ethicronics to bring one of the missing puzzle piece for digital security - hardware assurance at scale.

Biography
Franco-British Dr Franck Courbon graduated from 3 Masters in 2011/2012 (Glasgow University MPhil., INSA Lyon MRes., Saint-Etienne University MEng.) and a PhD. in 2015 in microelectronics/hardware security from the School of Mines of Saint-Etienne).

Franck spent 3.5 years at Gemalto Security Labs (now Thales-DIS where he undertook his MRes/Meng project and PhD.) working on image processing, laser fault attacks and hardware reverse engineering. From 2015 to 2022, Franck worked at the University of Cambridge (Postdoc, Fellowship, EPSRC IAA project leader) on electronics low level reverse engineering, memory content extraction, laser fault attacks and supply chain security.

Franck has 100% publication success rate, has supervised more than 120 University of Cambridge Computer Science and Engineering students and mentored/lectured dozens of Cambridge Judge Business School students. Last but not least, Franck introduced to +1000 13 to 16years old Cambridgeshire students the world of hardware-based cybersecurity, opportunities with starting a company, chances of doing long studies and working in electronics/cybersecurity no matter their starting poing, current grades and differences.

Franck is Founder & CEO of Ethicronics (Central Cambridge, UK, 06/2022) -full time since November 2022. Ethicronics specialises in scalable software solutions to address complex electronics hardware security challenges. The company develops a tamper-proof, transparent, ready-to-use software that eliminates counterfeit and compromised electronics hardware.

This is particularly vital for fabless companies in sectors including Defence, Telecoms, Aerospace, Automotive, Critical Infrastructure, and Consumer Electronics. Part of an InnovateUK Semiconductor Delegation in Switzerland and Germany made of some of the most ambitious innovative UK Businesses, Ethicronics -with value co-creation in mind, is looking for leading scientific institutions, semiconductors players, fabless companies and cybersecurity authorities to explore partnerships opportunities.

Franck has brought together key grant funding, skilled and impact-driven team, unique technology and world-leading partners**.** The Cambridge-based company has been supported by Cambridge Accelerate, NCSC for Startups, Defence And Security Accelerator (DASA)/Thales, and Innovate UK (including a £2.5M UK/APAC collaborative project), Ethicronics is a 2024 finalist in multiple prestigious awards (Infosecurity Europe, NATO, IET, Cambridge Independent Technology and Science Awards) and received the 2024 Business Weekly Graduate Business of the Year Award, positioning itself as a world leader in hardware assurance.

References