



# IoT Security Foundation Virtual Conference

1st - 4th December 2020

## Proceedings Booklet

### Conference Sponsors





Welcome to the 2020 IoT Security Foundation Virtual Conference where we aim to illuminate and educate delegates with an update on the threat landscape, standards & regulations, best practice, next-practice and the latest developments in IoT cyber security.

In this Conference Proceedings Booklet you will find Agendas for all 4 Days, Sponsor Speaker Profiles & Sponsor Adverts. [The Agendas are linked to the speakers respective profile pages on the IoTSF Conference Website, as well as logo's throughout, so make sure to click on them to learn more!](#)

Don't forget to visit our Sponsorship Page on the [IoTSF Conference Website](#) to enter our [Gold Sponsors Prize Draw!](#)

## About

Hardwear.io is a security conference for the hardware and security community. The conference revolves around the objective of four primary concerns (BETA) – backdoors, exploits, trusts, and attacks – in hardware, firmware, and associated protocols. We are invested in nurturing people through the sharing of information and knowledge.

All Hardwear.io events (Netherlands, US, and Berlin editions) are known for providing high-quality knowledge via technical talks and practical training sessions. Since our first event in 2015 we strive to offer talks on the latest research in hardware security by renowned security professionals across the globe – nothing shows it better than the rich assortment of Hardwear.io NL 2020 talks ranging between Side Channel Attacks, Countermeasures, Attacks on heterogeneous FPGA-CPU, and Telecom Security.

What distinguishes us is our passion for giving back and contributing to the hardware security community. This encourages us to be more than a hardware security training and conference, but a platform to share, exchange, and collaborate via various workshops/villages/CTF/HardPwn contest etc. among various stakeholders like the Government, Industry, Academia and community.

Our upcoming online edition of Berlin Hardwear.io Trainings 2021 is scheduled between 27-30 January 2021. For more information, visit: <https://hardwear.io/berlin-2021/online-training.php>.

# hardwear.io

Hardware Security Conference and Training

## CONTACT

[info@hardwear.io](mailto:info@hardwear.io)

+91 9922900657

<https://hardwear.io/>

# hardwear.io

Hardware Security Conference and Training

## Security Training Berlin 2021

Training: 27th to 30th January: 9:00 AM - 2:00 PM CET @Zoom

Registration: <https://www.eventbrite.com/e/hardweario-online-security-training-berlin-2021-tickets-127984110921>

## Hardware Security Trainings:

1. Assessing and Exploiting Control Systems & IIoT by Justin Searle
2. Breaking Practical WhiteBox Crypto Training by Guillaume Vinet
3. Advanced Microcontrollers Firmware Exploitation by Alexander Bolshev & Tao Sauvage
4. EMFI and Voltage Fault injection attacks with Raiden by Adam Laurie & Grzegorz Wypych

December 1  
09:00 - 10:30

# Security by Design



Introduction

**John Moor**

*Managing Director, IoT Security Foundation*

“We’re All in This Together”

**Keynote Speaker - Stephen Pattison**

*Chairman of IoT Security Foundation & VP Public Affairs, Arm*

“IoT Security Reference Architecture”

**Prof Kwok Yan LAM**

*Professor of Computer Science  
National Technological University (NTU)*

“IoT Security, and it’s Disturbing Status”

**Pieter Meulenhoff**

*Advisor*

*Euofins Cyber Security Netherlands (Qbit Cyber Security)*

BREAK - 10:30 - 10:40

10:40 - 11:55

“The Consumer IOT Attack Surface – an Architectural Deep Dive on the Threats and Mitigations for Real World IoT Deployments”

**Nick Allott**

*CEO, NquiringMinds*

“ManySecured Collaborative Intelligent IoT Gateway”

**Peter Shearman**, Head of Innovation, Cisco

&

**Duncan Purves**, Projects & Operations Manager, IoT Security Foundation

“Secure by Design, Still a USP in a Competitive Environment”

**Ivan Reedman**

*Hardware Security Capability Practice Lead, NCC Group*

BREAK - 11:55 - 12:05

12:05 - 13:20

“Security Best Practice - Why and How?”

**Jeff Day**

*Chair of the IoT Security Foundation Best Practice Working Group, Security Lead, BT*

“Practical Physical Attacks Against Embedded Systems and Their Secure Design to Mitigate Them”

**Rohini Narasipur**

*Product security engineer and incident handler, Bosch PSIRT*

“Secure by Design: What is it and why do IoT use cases need it?”

**Rob Dobson**

*VP Technology Partners, Device Authority*

MEET THE EXPERTS- 13:20 - 13:50





AUTOMOTIVE



CONSUMER



DEFENCE



INDUSTRIAL



MEDICAL



SMART GRID



TELECOMS

# SECURING THE INTERNET OF THINGS

**SAFE, RELIABLE, SECURE.**

For more than 38 years the world's leading companies have trusted Green Hills Software's secure and reliable high performance software for safety-critical applications.

For the connected car, consumer and medical devices, industrial telemetry, smart grid, telecoms hubs and more, our software and services deliver proven secure, reliable underpinning technology for the Internet of Things.

To develop devices for the Internet of Things with the highest levels of security and reliability, call **01844 267 950** or visit [www.ghs.com/secureIoT](http://www.ghs.com/secureIoT)

December 1  
13:50 - 15:05

# Security by Design



“Side Channel Attacks; an Imminent Threat”

**Vincent Lyles**

CEO, Pugged Code Limited

“Securing the Industrial IoT”

**Simon Butcher**

Principal Embedded Security Engineer, Arm

“Protecting IoT data and providing trusted connectivity via eSIM – leveraging the eSIM as Root of Trust for your IoT applications”

**Zofia Domanska**

Product Manager, G+D Mobile Security

BREAK - 15:05 - 15:15

15:15 - 16:30

Software Provenance – Where Do We Draw the Line?

**Matt Wyckhouse**

Founder & CEO, Finite State

“PKI Certificates: a Ticking Time-Bomb in Your IoT System?”

**Matthew Dickie**

CTO, Group-BMC

“Secure Onboarding for IoT Devices: the FIDO approach”

**Dr. Giridhar D. (Giri) Mandyam**

Chair of FIDO Alliance IoT Technical Working Group, Chief Security Architect – IoT and Automotive, Qualcomm

**David Turner**, Director of Standards Development, FIDO Alliance

16:40 - 17:30

BREAK - 16:30 - 16:40

“When One Size Solution Doesn’t Fit All”

**Keynote Speaker - Katerina Megias**

Program Manager, NIST Cybersecurity for IoT Program, NIST

Conference Day 1 Closing Remarks

**John Moor**

Managing Director, IoT Security Foundation

DAY 1 CONFERENCE CLOSE





**Robert Dobson**  
**Vice President, Device Authority**

*“Secure by Design: What is it and why do IoT use cases need it?”*



## **Biography**

Rob has over two decades of applied industry experience, across a wide range of industry verticals, with a strong network and understanding of application markets from Edge Compute, Cloud Service, Industrial, Semiconductors, Wireless and Software Architecture. With focus on cyber security and IoT for the past 10 years. Rob has worked on many complex IoT projects and use cases for TEIR 1 OEMs in the areas of Health Care (IoMT), Industrial and Automotive.

## **Abstract**

The envisioned compelling economic and social benefits with IoT adoption are at risk as the current security model has evolved as an afterthought from IT, focusing on a detect and respond model with network centric models, failing to protect critical IoT solutions and use cases.

We now have an opportunity to redefine the IoT cybersecurity model with a Security by Design and Privacy by Design approach. Solving the trust and safety issues, realizing the full potential of the IoT ecosystem, and avoiding potentially disastrous impacts. Everyone, including Governments, regulatory bodies and standards groups are being forced to rethink this issue.

From this session, you will learn:

Why/How a Root of Trust and device bound identity are the core foundational components for trust and automation

How use cases span across disparate entities including IoT platforms, and why a security automation layer becomes an important component

What is Data centric security and why device bound data security is required – independent of network or human is required for any critical use cases.

What is Automated PKI – Standards driven and proven trust fabric

Review applied use case examples across Medical, Automotive and Industrial



# Security for Industrial Internet of Things

Device Authority provides solutions to address the challenges of Identity and Access Management for the Internet of Things (IoT) – helping customers simplify the process of establishing trust for the IoT through our innovative technology platform: KeyScaler.

KeyScaler has a proven track record for Industrial and Medical/Healthcare industries.

Find out more at  
[www.deviceauthority.com](http://www.deviceauthority.com)  
[info@deviceauthority.com](mailto:info@deviceauthority.com)

 — Device Trust

 — Data Trust

 — Operationalizing the Trust

 — Enabling Compliance

 — Delivering Performance





## Introduction

**John Moor**

*Managing Director, IoT Security Foundation*

## “IoT Security Challenges and Opportunities in the 5G Era”

**Keynote Speaker - Mihoko Matsubara**

*Chief Cybersecurity Strategist, NTT Corporation*

## “Cybersecurity Labelling Scheme (CLS) & Beyond”

**Mr Lim Soon Chia**

*Director, Cyber Security Agency of Singapore*

## “The Evolution of Chip to Cloud Security and Future Threats”

**Satyajit Sinha**

*Senior Analyst, IoT Analytics*

**BREAK - 10:30 - 10:40**

**10:40 - 12:00**

## “What is a Smart Built Environment, and why it matters?”

**Sarb Sembhi**

*CTO & CISO, and Co-Chair of Smart Built Environment Group  
Virtually Informed*

## “New Guidance and Best Practices on the security of Smart Built Environments, IoTSE”

**James Willison** - Unified Security, **Nick Morgan** - Derwent London, **Tony Wood** - Honeywell  
**Michael Monaghan** - Consultant, **Dave Cooke** - Consultant, **Jason Shaw** - Hilson Moran

## “A Brief Introduction to Vulnerability Disclosure from the Researcher Perspective”

**Jen Ellis**

*Vice President of Community and Public Affairs, Rapid7*

**BREAK - 12:00 - 12:10**

**12:10 - 13:25**

## “IoT Security and the Supply Chain: Real-World Problems and Solutions”

**David Mudd**

*Global Digital & Connected Product Certification Director, BSI*

## “Supply Chain Integrity”

**Amyas Phillips**

*IoT Consultant and Security Scientist, Chair of the IoTSE Supply Chain Working Group  
Ambotec*

## “One way or another, they’re going to get you: Threats to press freedom from the Internet of Things”

**Anjuli R. K. Shere**

*Doctoral researcher in Cyber Security, University of Oxford*

**MEET THE EXPERTS - 13:25 - 14:20**

# IC INTELLECTUAL CAPITAL RESOURCES

recruitment partner to the global technology community

Securing talented professionals  
for your organisation,  
since 1999

**WIN** a **\$100**  
**donation** to the  
**CHARITY** of your choice!

*\*click for details*

HARDWARE  
SOFTWARE  
CREATIVE  
SALES AND MARKETING  
SUPPLY CHAIN  
IT

**W:** [ic-resources.com](http://ic-resources.com)  
**E:** [enquiry@ic-resources.com](mailto:enquiry@ic-resources.com)  
**T:** +44 (0)118 988 1150



**Ian Pearson**  
Principal Embedded Solutions Engineer,  
Microchip

*“Is Consumer Radically Different to High-Reliability? Leveraging Hi-Reliability Product Design Flows”*



## **Biography**

Ian has 20+ years' experience designing embedded systems. For the last 10+ years he has supported connected embedded systems focusing originally on Ethernet and TCP/IP and has since been active in bringing Microchip Wireless Solutions in Wi-Fi, Bluetooth and LoRa® technology into the embedded space. Ian has been active in IoT since the early days and is a vocal advocate for the design of secure IoT systems

## **Abstract**

Electronic design, in the new security conscious world, is hard. Device complexity and software content increase unabated, yet price appears to constantly drive lower. How is it, when the majority of processes are equal, one vendor can provide solutions far cheaper than another? Is it just market economics or is something being compromised?

Have we graded security as a function of the product end cost and market sector rather than at the potential fiscal impact when scaled up risk of millions of devices is considered?

What lessons can we learn and adapt from the hi-reliability, less cost sensitive sectors and bring these to the highly scaled, potentially higher total risk, sectors? Equally, can we apply knowledge from consumer security to other sectors?





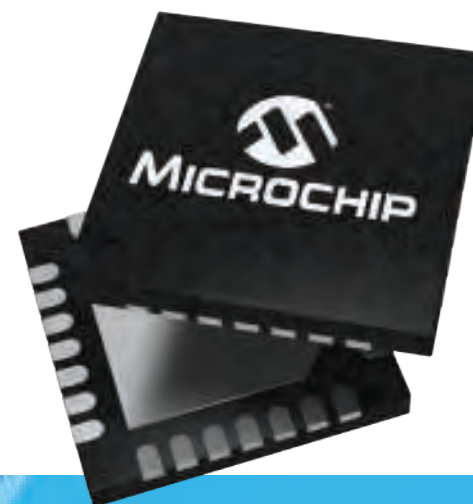
## Is Consumer radically different to High-Reliability?

If you have a requirement to ensure your product designs meet the current challenges with respect to security then join Microchip at the IoTSF Conference to Learn about Leveraging Hi-Reliability Design Flows in your next design.

**Presentation: 3rd December - 12.55pm – 1:20pm**

Following our presentation join our experts to discuss how we can help with your designs.

**Meet our experts session: 3rd December - 1:20pm – 2:20pm**



[microchip.com](http://microchip.com)



The Microchip name and logo and the Microchip logo are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries. All other trademarks are the property of their registered owners.  
© 2020 Microchip Technology Inc. All rights reserved. 11/20  
MEC2349-ENG-11-20

December 2  
14:20 - 15:10

# Applied Security



“Secure Management of Things in AWS IoT”

**Dave Walker**

*Principal Specialist Solution Architect for Security and Compliance, Amazon Web Services*

“IoT security from Risk of Inaction to Return on Investment”

**Ovidiu Ursachi**

*VP & Chief Product Security Officer, Masernet*

BREAK - 15:10 - 15:20

15:20 - 16:35

“Building the Optimal Level of IoT Device Security into a Connected Product – an OEMs Guide”

**Clive Watts**

*Director, Product Management, Secure Thingz*

“ETSI EN 303 645 – the Ultimate IoT Testing Baseline. Lessons Learned and Way Forward”

**Razvan Venter**

*Team Lead Security Compliance and Certifications, Secura B.V.*

“Anatomy of Real-World IoT/OT Attacks and How to Defend Against Them”

**Lesley Kipling**, Chief Cybersecurity Advisor, Microsoft

&

**Phil Neray**, VP of IoT & Industrial Cybersecurity

BREAK - 16:35 - 16:45

16:45 - 17:50

“AI-driven Cyber Defense for Endpoint Energy Assets”

**Keynote Speaker - Leo Simonovich**

*VP and Global Head, Industrial Cyber, Siemens Energy*

**Panel Discussion**

**Leo Simonovich** - Siemens Energy, **Lesley Kipling** - Microsoft

**Phil Neray** - Microsoft, **Jen Ellis** - Rapid7

Conference Day 2 Closing Remarks

**Richard Marshall**

*Chair of IoT Security Foundation*

*Plenary Group*

DAY 2 CONFERENCE CLOSE



**Ken Munro**  
Partner, Pen Test Partners

*“The IoT is littered with security disasters. As the distinction from OT blurs how do we avoid repeating them?”*



## **Biography**

Ken has been working in IT security for over 15 years. He writes for various newspapers and industry magazines and is a regular source of comment and sanity on IoT issues to various news agencies and the BBC.

Ken has grown a reputation as someone who cuts through the noise, spin and scaremongering put about by many security vendors.

Ken takes a very active role in the IoT space. When not presenting findings, facilitating workshops, or briefing organisations Ken also provides advice to device manufacturers and is a huge advocate of responsible disclosure.

## **Abstract**

This session will explain, with hacking examples, what happens when a historically isolated tech environment meets an always connected and messy ecosystem. OT is falling in line with IoT at pace, and many OT installers simply don't understand security so we'll explore the potential for chaos which that brings.

There's advice too, the best being "Don't believe the marketing hype. There'll also be tactical help; test for security before you adopt or change systems, don't rush to the cloud, and much more.



# IoT Nation™ maps the Global IoT Ecosystem

Find Customers. Partners. Investments.  
Use Cases. Events. Competitions. Contacts.  
and more...

Find it all at [www.iotnation.com](http://www.iotnation.com)

Free 30-day access, use signup code: **IoT5F100**



## IoT Nation™

Copyright © 2020 IoT Nation LLC. All Rights Reserved.

For more information:  
[info@iotnation.com](mailto:info@iotnation.com)  
[www.iotnation.com](http://www.iotnation.com)

December 3  
09:00 - 10:30

# Resilience



## Introduction

**John Moor**

*Managing Director, IoT Security Foundation*

## Keynote Speaker - Kaja Ciglic

*Senior Director, Digital Diplomacy Cyber Tech Accord /Microsoft*

## “The Geopolitics of Industrial IoT”

*Madeline Carr, Professor of Global Politics and Cybersecurity, UCL &  
Saheli Datta Burton, Research Fellow*

## “Coming Security & Privacy Challenges, a Practice for Securing Smart Home Devices”

**Kevin Song**

*Head of Cyber Security Compliance, Xiaomi*

**BREAK - 10:30 - 10:40**

**10:40 - 11:55**

## EXPLIoT: A Journey to Secure IoT

**Aseem Jakhar**

*Co-Founder/Director R&D, Payatu*

## “The IoT is littered with security disasters. As the distinction from OT blurs how do we avoid repeating them?”

**Ken Munro**

*Partner, Pen Test Partners*

## “IIoT the platform for Sustainability”

**Victor Lough**

*Cyber Security & Advanced Digital Services Business Lead, Schneider Electric*

**BREAK - 11:55 - 12:05**

**12:05 - 13:20**

## “Meeting the Industry 4.0 Security Challenges of IEC 62443”

**Haydn Povey**

*CEO, Secure Thingz Ltd*

## “Securing the Internet of Medical Things”

**Andy Bridden**

*IoT Security Consultant, PA Consulting*

## “Is Consumer Radically Different to High-Reliability? Leveraging Hi-Reliability Product Design Flows”

**Ian Pearson**

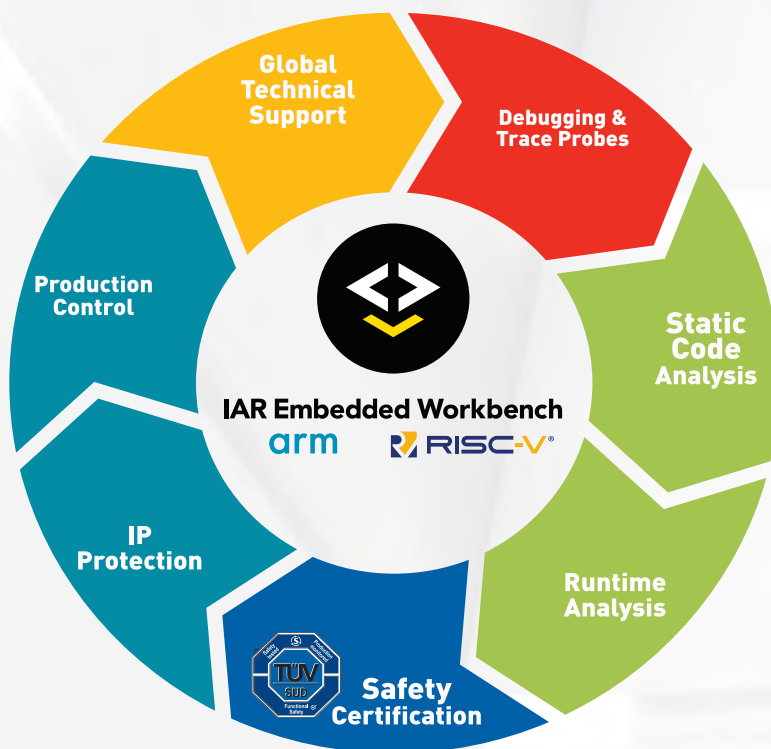
*Principal Embedded Solutions Engineer, Microchip*

**MEET THE EXPERTS- 13:20 - 14:20**

# More than an ordinary toolbox

IAR Embedded Workbench is the number one development toolchain – a robust, flexible and complete platform for all aspects of embedded development with powerful functionality just a tick box away. It supports you through the entire development process, letting you create an out-of-the-ordinary application. For now and for any projects in the future. In addition, our dedicated team of experts is just a phone call or email away. So much more than just a toolbox.

Unleash the power of IAR Embedded Workbench!



*23+ architectures, one environment.*



## IAR EMBEDDED WORKBENCH

IAR Embedded Workbench gives you a complete IDE with everything you need to ensure quality, reliability and efficiency in your embedded application. All in one single view, enabling one uninterrupted workflow.



## IP PROTECTION

Security in embedded applications is now just a tick box away. We provide integrated solutions to help you make the security of your product more straightforward, scalable and sustainable. Protect your application and deliver secure, encrypted code! If you need help, we're here to train you.



## SAFETY CERTIFICATION

Compliance with functional safety standards such as IEC 61508 and ISO 26262 is important, but often cumbersome. Our pre-certified development tools help you in making your application safe and compliant with industry standards. Safety guides and prioritized technical support is included.



## DEBUGGING AND TRACE PROBES

Integrated tools simplify your development workflow. Our feature-rich in-circuit debugging probes enable powerful features in IAR Embedded Workbench.



## GLOBAL TECHNICAL SUPPORT

You are never alone when using our technology. Our dedicated support team is there to guide you wherever and whenever you need it. And if you want to boost your skills even further, our technical training program offers a flexible learning journey.



## PRODUCTION CONTROL

Through simplified Production control, we empower developers to pre-define how many end products can be provisioned during production, preventing damaging cloning and counterfeiting.



## CODE ANALYSIS

How can you get in control of every single line of code? Let our smart analysis tools take care of it for you! Completely integrated, to make your day easier.





**Haydn Povey**  
CEO, Secure Thingz

*“Meeting the Industry 4.0 Security Challenges of IEC 62443”*



## **Biography**

Haydn is the Founder & CEO of Secure Thingz Limited, a company focused on developing and delivering next generation security technology into the Internet of Things (IoT) and other connected systems. The company specializes in supporting device creation and has a broad consultancy base encompassing AsiaPac, North America and EMEA.

Haydn has been in senior management at leading global technology companies for over 20 years, with the last 10 years in senior marketing and business development roles at ARM Holdings, the leading Microprocessor IP (Intellectual Property) company. Haydn most recently headed ARM's strategy and product roadmaps for Security within IoT and M2M marketplaces where he worked with critical groups within the US and UK government responsible for the development and deployment of security frameworks, alongside many leading silicon vendors, OEMs and system integrators and software solutions.

Prior to owning security at ARM Haydn led the development and introduction of the Cortex-M microprocessor family which has led to the rapid adoption of 32-bit microcontroller technology around the globe and underpins the majority of Internet of Things devices.

Earlier in his career Haydn held positions as Global Head of Sales and Marketing with various early stage technology companies as well as senior sales and marketing roles with National Instruments in both the UK and the US.

## **Abstract**

IEC62443 is the emerging cybersecurity standard for Industry 4.0, covering threats ranging from accidental insider enablement through to Nation State level attacks. As a major new requirement on both vendors and customers this session will highlight the core security and development requirements and demonstrate how Arm based systems can meet the evolving challenges.

# Security development tools

*Protect your application throughout the entire product lifecycle!*

The rapidly growing market of connected devices is facing major security challenges, with attacks ranging across IP theft, counterfeiting and overproduction, as well as data theft and potentially life-threatening sabotage. In addition, security legislations are being enacted around the world and will keep coming.

We are here to ease your security transition and help you implement security in a straight-forward way.



Secure Thingz is the global domain expert in device security, embedded systems, and lifecycle management. Since 2018, the company is part of IAR Systems, the future-proof supplier of software tools for embedded development.

Secure Thingz is focused on delivering advanced security solutions into the emerging industrial Internet of Things market, alongside critical infrastructure, automotive and other markets.

---

Want to know more?  
visit [iar.com](http://iar.com)

December 3  
14:20 - 15:35

# Resilience



**"Challenges of Vulnerability Management and Disclosure Processes in a big organisation – The Bosch PSIRT"**

**Carolina Adaros**  
*Product Security Incident Handler, Bosch PSIRT*

**"IoT on the frontline - when a 3rd party 0day becomes your problem.."**

**Adam Laurie**  
*Global Associate Partner and Lead Hardware Hacker, IBM*

**"Shining the Light of Truth: a journey into vulnerability disclosure practices at consumer IoT product companies"**

**David Rogers, CEO, Copper Horse &  
Rohan Panesar, Undergraduate Student, University of the West of England**

**BREAK - 15:35 - 15:45**

**15:45 - 17:30**

**"Open security challenges and opportunities in Industrial IoT & Industry 4.0 systems"**

**Kubilay Ahmet Küçük**  
*Post-Doctoral Research Associate, Cyber Security Centre*

**"Lessons on Industrial IoT Security from Finland"**

**Vikram Sharma**  
*Senior Manager Engineering, Cisco*

**"Sensory Overload – Cybersecurity Threats for Next Generation Vehicles"**

**Keynote Speaker - Steve Povolny**  
*Head of Advanced Threat Research, McAfee*

**Conference Day 3 Closing Remarks**

**John Moor**  
*Managing Director, IoT Security Foundation*

**DAY 3 CONFERENCE CLOSE**



**Kevin Song**  
**Head of Cyber Security Compliance, Xiaomi**

CISSP/CISA/ISO 27001 LA/CCNP

*“Coming security and privacy challenges, a practice for securing smart home devices”*



## **Biography**

Kevin created the security baseline of corporate smart devices to meet the compliance requirements, and navigate the function teams and supply chain vendors to research and promote the technology to secure IoT device. The methodology has applied in hundreds of device categories, which are red hot in market. Before joining Xiaomi, Kevin worked as senior manager of Global Security Operation Center (GSOC) in Lenovo, with extensive experience of cyber incident and product security bugs response. He successfully implemented several compliance projects, including PCI DSS, UK cyber essential, ISO 27001, etc.

Kevin devotes substantial resources in data security and privacy protection, mitigating the privacy concern in AI and IoT era. He also works as the co-chair of IAPP China Knowledgenet, promoting the privacy by design (PbD) principle.

## **Abstract**

Modern IoT ecosystems are complex. Various devices can be connected and configured to send data over cellular or local network to cloud applications and backends. The security and privacy risk is present at every step along the IoT journey, which expand the whole supply chain.

Xiaomi, a Chinese electronics company, is a leader in smart home devices, whose security team has developed a comprehensive solution to mitigate the above risk. No one size fits all, but how to navigate through hundreds of smart devices? The topic will introduce the practical solution of IoT device manufactures.



# Security Plus, Smarter life



















## About Xiaomi

Xiaomi Corporation is a Chinese multinational electronics company founded in April 2010 and headquartered in Beijing. Xiaomi makes and invests in smartphones, mobile apps, laptops, home appliances, consumer electronics, and many other products. Xiaomi has the world leading consumer IoT platform – Mi home. Mi home has connected more than 271 million smart devices and the MIUI system have more than 330 million MAU.

## Our IoT Products

Xiaomi IoT has a vast variety of products, including Security and Safety category devices, wearable devices, entertainment devices, transportations, smart home devices etc.. Click [here](#) for more information.

 10000 mAh Mi Wireless Power Bank	 Mi Portable Bluetooth Speaker	 Mi True Wireless Earbuds Basic 2	 Mi Air Purifier 3C
 Mi Smart Band 4C	 Mi AIoT Router AC2350	 Mi AIoT Router AX3600	 Mi Smart LED Bulb (Warm White)
 Mi Electric Scooter Essential	 Mi Curved Gaming Monitor 34	 Mi Electric Scooter Pro 2	 Mi True Wireless Earphones 2 Basic
 Mi Electric Scooter 1S	 Mi Smart Band 5	 Mi LED Smart Bulb Essential (White and Color)	 Mi Router 4A



## How we secure our products

Xiaomi established an IoT security team in November 2015 and upgraded it to an AIoT security lab in 2017. Xiaomi has established a complete cyber security and privacy management system, and always adheres to “security by design and privacy by design”. Our Lab formulated the “Xiaomi AIoT Security Baseline” and opened it to the Xiaomi ecosystem. All Xiaomi’s smart products need to pass the security and privacy test of the Lab before launch. Sold products will also be monitored for 7\*24 hours on the AIoT Security Platform.



AIoT Security Platform

- Intelligentization monitoring 7\*24
- Vulnerability scanning
- Multi-protocol analysis
- Intelligent Fuzz
- APK & firmware analysis
- Data cross-domain evaluation
- Privacy data analysis
- Network simulation

## Security Vulnerability Management and Disclosure

Xiaomi product security vulnerability management handle the receipt, investigation, internal coordination and disclosure of security vulnerability information related to Xiaomi offerings and it’s an important window to disclose the vulnerability of Xiaomi products. Security researchers, industry organizations, government agencies and vendors can proactively contact our SRC or open program on Hackerone to report potential product security vulnerabilities. Click [here](#) for more details.



## Xiaomi Trust Center

To increase transparency, xiaomi published the Trust Center portal to list the security certification, whitepaper and update the security advisory. Click [here](#) for more details.

For the smartphone, with MIUI 12 release, we also published the dedicated MIUI privacy portal to show the security and privacy features in MIUI. Click [here](#) for more details.

December 4  
09:00 - 11:05

# Training & Awareness



Introduction

**John Moor**

*Managing Director, IoT Security Foundation*

“Manage Vulnerability Reports”

**David Rogers**

*CEO, Copper Horse*

“Responding to the IOT Attack Surface Threats: an Overview of Current Initiatives to Secure IoT”

**Nick Allott**

*CEO, NquiringMinds*

BREAK - 11:05 - 11:15

11:15 - 13:00

“Using Free Tools to Test the Security of a Small Embedded System”

**David Long**

*Principal Member of Technical Staff, Doulos*

“AWS IoT Defender ML Detect”

**Andrew Delalmare**

*Senior IoT Specialist Solutions Architect, Amazon Web Services*

MEET THE EXPERTS - 13:00 - 13:30

13:30 - 14:30

“Eliminate Universal Default Passwords”

**Michael Richardson**

*Open Source and Standards Consultant, Sandelman Software Works*

“Breaking practical White-Box Cryptography”

**Guillaume Vinet**

*Security Analyst, eShard*

BREAK - 15:30 - 15:40

15:40 - 16:50

“Security Software Updates”

**Michael Richardson**

*Open source and Standards Consultant, Sandelman Software Works*

Conference Wrap up

**John Moor**

*Managing Director, IoT Security Foundation*

CONFERENCE CLOSE



**Dr. David Long**  
Principal Technical Staff, Doulos

*“Using Free Tools to Test the Security of a Small Embedded System”*



## **Biography**

Dr David Long is the Principal Member of Technical Staff at Doulos, where he has worked since 2001, developing and presenting training courses for professional engineers. During that time, he has trained several thousand engineers in more than 20 different countries, in subjects ranging from HDL-based design and verification of digital and mixed-signal hardware through to virtual prototypes, embedded software and security. He is also the co-author of the IEEE 1666 SystemC Language Reference Manual.

Prior to joining Doulos, David worked for over 15 years in both industry and academia. He has an MSc in VLSI Design and a PhD in Mixed-Signal Simulation.

## **Abstract**

Security is an increasing concern for developers of many small embedded applications such as IoT Edge devices. Unfortunately the choice of tools suitable for testing security on such systems is limited. This is quite different to web-based, desktop and even embedded Linux application developers who are able to select security tools from a wide range of commercial and open-source providers, such as those included in the popular Kali Linux distribution.

This tutorial provides an overview of open-source and free tools that are suitable to use for security testing of IoT edge devices based on a Cortex-M processor. It considers how and where these tools may be used within the security testing process. Examples include the use of the NSA's Ghidra software reverse engineering tools and tools based on the open-source Unicorn emulator. We will also discuss the steps required to perform fuzz testing on some example code for a Cortex-M processor using AFL-Unicorn, GDB, GEF and python scripts, together with hints and tips that will be useful for anyone in the audience who wishes to try this for themselves.





Delivering KnowHow

# EMBEDDED SECURITY TRAINING FOR THE CONNECTED WORLD



**SECURE  
EMBEDDED  
TRAINING**



Comprehensive Embedded  
Linux Security



Embedded System Security  
for C/C++ Developers



Arm Microcontroller Security  
with TrustZone-M

## KnowHow WEBINARS

Free to attend interactive  
webinars with Doulos experts

**NEXT SECURITY WEBINAR: FRI DEC 18**  
Embedded Linux Security: A Practical Overview

**REGISTER  
HERE NOW**

**WIN \$100 Amazon  
Voucher**

**CLICK TO  
ENTER DRAW**

[www.doulos.com](http://www.doulos.com)

## ManySecured Collaborative Intelligent Gateway Project

ManySecured's aim is to secure the Internet of Things (IoT) through security innovation at the gateway. To better protect consumers and enterprise from the security risks posed by IoT devices. The ManySecured Gateway project partners will develop publicly available specifications and developer resources aimed at hub/gateway vendors, in a bid to deliver AI-IoT-secured deployments which are resilient to attack throughout their lifecycle. The specifications with supporting resources will allow gateway vendors to take advantage of the security schema in their own products. The ManySecured partners will define collaborative information sharing protocols, IoT fingerprinting techniques and technical integration layers to make wide scale deployment and impact possible.

Founding partners in the project include Cisco, IoT Security Foundation, NquiringMinds and the University of Oxford.

The ManySecured Gateway Project is a collaborative project co-funded by Innovate UK, the UK's innovation agency.

<https://manysecured.net>

### 1-FOUNDATIONS



How do you implement the internals of a secure gateway? Secure storage, secure boot, software verification methods. Defines the underlying foundation security.

### 2-SECURE COMMS



How do IOT devices communicate securely on an internal network? Key distribution, user interface, secure local connections.

### 3-UPDATE



How do you know an IOT device needs updating? How can you manage the process easily. Remote device type identify. Simplified update user interface

### 4-MONITORING



How can you monitor IOT activity across IP and NonIP networks? Low level device activity summaries. Creation of behavioural fingerprints.

### 5-NETWORK ISOLATION



How can you restrict the IOT attack surface, incoming and outgoing? Define practical methods of segmenting and isolation network activity

### 6-THREAT DETECTION



How can you identify threat before or soon after compromise? Defining flexible methods of intelligent detection and subsequent control

### 7-SMART CONTROL



How can you locally and dynamically control the internal network? Defining simile interoperable standards for network control to increase security.

### 8-COLLABORATION



How do we share information? Smart threat detection needs high quality data in volume. This will only come through industry collaboration on activity and threats.