NEWSLETTER #3

CONTENTS:

We have now reached halfway through the project, marking a significant milestone in achieving our first artifacts. We already have a first version of CROSSCON security stack components and they are readily accessible on our GitHub.

- Sandro Pinto

CROSSCON has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537.

WP3 Leader Notes

We have reached halfway through the project, marking a significant milestone in achieving our first artifacts. Our approach does not involve reinventing the wheel; rather, we address flaws and limitations of the existing trusted components over the entire stack across heterogeneous devices and architectures.

Dear Readers,

Welcome to the third newsletter of CROSSCON!
We have reached halfway through the project, marking a significant milestone in achieving our first artifacts. We already have the first version of CROSSCON security stack components and they are readily accessible on our GitHub[1]. This milestone represents a first step towards a cross-platform open security stack for connected IoT devices to tackle the already-known security challenges.

Despite the modern security findings and developments, several security risks and limitations persist across systems stack components of different IoT devices and architectures. Notwithstanding, due to the wide spectrum of heterogeneous devices, system stack components struggle when trying to communicate effectively with each other. Therefore, CROSSCON is focused on strengthening components from the root to the entire chain of trust and ensuring interoperability by utilizing Global Platform API standards. Our approach does not involve reinventing the wheel; rather, we address flaws and limitations of the existing trusted components over the entire stack across heterogeneous devices and architectures.
In recent months, WP3 partners have made significant progress in enhancing the security of system stack components. Key advancements include the CROSSCON Hypervisor, featuring per-VM TEE and dynamic VM creation and management, the Baremetal TEE, available in both MPU and non-MPU versions, and novel CROSSCON trusted services, such as PUF-based authentication, FPGA Trust Anchor, and Context-based Authentication. The current status and referenced links of these components are described in this newsletter edition for further information.

[1] https://github.com/crosscon

Sandro Pinto
WP3 Leader, Uni. Minho

The development of CROSSCON components has attracted significant attention from both researchers and industries, especially within the RISC-V community. In June, CROSSCON hosted a Workshop side event at the RISC-V Summit titled "CROSSCON & (Secure) Friends". Security experts from other EU projects, including ORSHIN, REWIRE, SPIRS, and SecOpera, along with Frank K. Gürkaynak from PULP Team / ETH Zürich, and Florian 'Flo' Wohlrab, the CEO of OpenHW Group, shared valuable insights on security challenges, interests, and trends. Thank you all for attending.

For a comprehensive overview of the artifacts, please refer to the subsequent pages of this newsletter. If you wish to explore these developments further, we recommend accessing the open CROSSCON GitHub project and reviewing the public deliverables of the project. Stay updated through our project's website and social media channels.

Sandro Pinto

CROSSCON Components – Hypervisor & Baremetal TEE

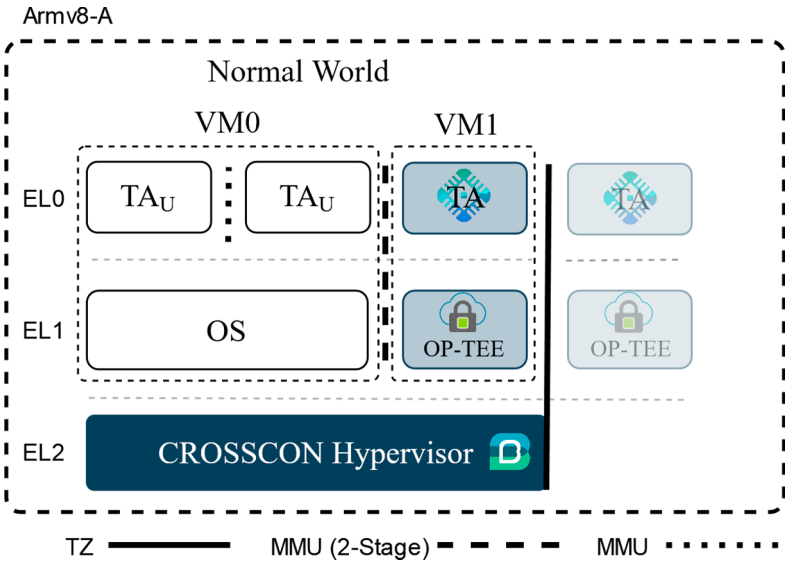
In recent months, WP3 and WP4 CROSSCON partners have released initial artifacts, including the CROSSCON Hypervisor, Baremetal TEE, CROSSCON SoC and new trusted services.

CROSSCON Hypervisor

The CROSSCON Hypervisor is a static partitioning Hypervisor that aims to provide strong isolation and real-time guarantees. It is based on the Bao hypervisor, and aims to implement novel features such as **(1) dynamic VM creation & management, (2) per-VM TEE service support, and (3) multiple VMM support.**

Current Status:
Currently, CROSSCON Hypervisor provides per-VM TEE services by isolating the TEE through one or multiple virtual machines (VMs) in the normal world. Our partners have provided demonstrations on our GitHub page to showcase its functionality, including running a Bitcoin wallet Trusted Application (TA) on top of OP-TEE within a virtual machine. It features support for QEMU (RISC-V & Armv8-A), for RPI4B and ZCU102 platforms.

Put your hands on CROSSCON Hypervisor here:
https://github.com/crosscon/CROSSCON-Hypervisor-and-TEE-Isolation-Demos



CROSSCON Baremetal TEE

To provide security for low-end systems that are not compatible with the CROSSCON Hypervisor, CROSSCON proposes a software-based bare-metal TEE. The TEE will ensure the basic security primitives such as memory isolation, privilege separation, and cross-domain communication. Two distinct versions of the bare-metal TEE are being developed, BareTEE-noMPU for baremetal devices that do not have a Memory Protection Unit (MPU), and BareTEE-MPU for devices that do.

Currrent Status:
Two prototypes of the bare-metal TEE are currently available: one where the MPU version is implemented on an ARMv7-M architecture and another where the non-MPU version is deployed on a MSP430 architecture, both illustrating the required basic security primitives.

Put your hands on CROSSCON Baremetal TEE here:
https://github.com/crosscon/baremetal-tee

PROJECT UPDATES

CROSSCON Components – SoC

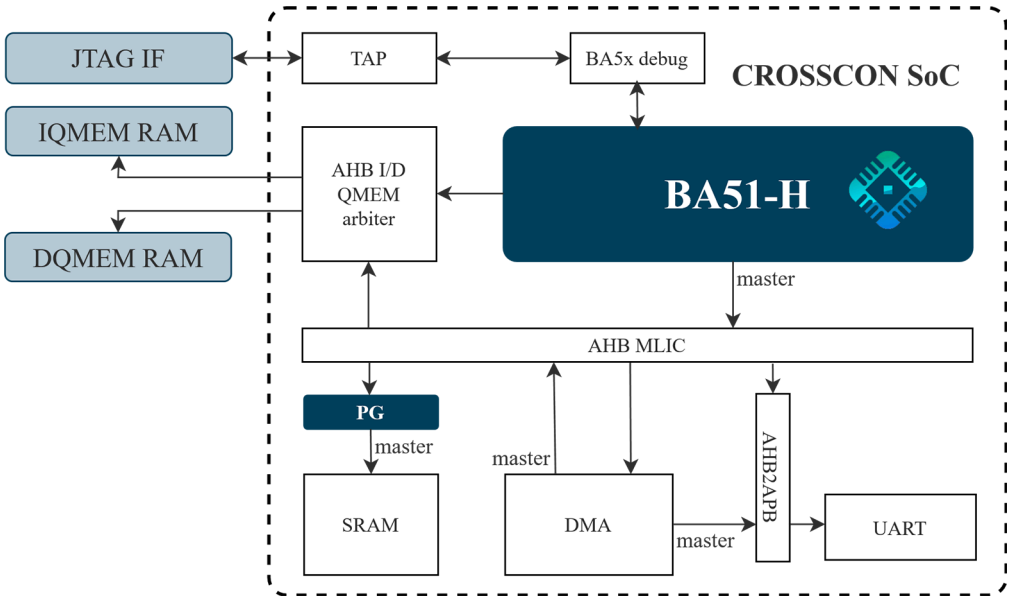
CROSSCON SoC

CROSSCON SoC is a system-on-chip (SoC) developed as part of the CROSSCON project. Its purpose is to provide a secure RISC-V execution environment for mixed-criticality IoT devices that demand robust security, adaptability, minimal code size, and low power consumption. The CROSSCON SoC aims to support strong software isolation through virtualization-based TEEs where HW modules connected to the interconnect can be shared between TEEs without compromising isolation.

Current Status:
Currently, CROSSCON SoC has successfully been integrated with Beyond Semiconductor's BA51 RISC-V2 core. BA51-H contains the first implementation of the unified (2-stage) SPMP unit, which is one of the possible SPMP candidates for standardization as part of the RISC-V SPMP standardization effort[3].

Additionally, the CROSSCON SoC introduces the Perimeter Guard (PG), a mechanism that enables hardware modules to be shared between virtual machines (VMs) while maintaining isolation. The PG module is positioned between the SoC interconnect and the shared resource, such as a cryptographic accelerator. It controls which VMs and bus masters have access and allows the resource to be "reset" before being used by a different VM or master. This reset prevents any state-related information from leaking through the shared hardware.

In the current version of the CROSSCON SoC, as shown in Figure below, we use PG to control access to SRAM so that it can be shared between different VMs without compromising their isolation.



Put your hands on CROSSCON SoC here:
https://github.com/crosscon/crosscon_soc

[2] https://www.cast-inc.com/processors/risc-v/ba51
[3] https://github.com/riscv/riscv-spmp?tab=readme-ov-file

PROJECT UPDATES

CROSSCON Components – Trusted Services

PUF-Based authentication

CROSSCON aims to innovate and integrate a secure, efficient, lightweight, and scalable PUF-based authentication scheme, facilitating resource-constraint embedded devices to authenticate themselves between each other, based on their inherent hardware variations. During the project, three main implementation methods have been identified:
ZK-PUF: PUF-based authentication via zero-knowledge proofs,
PAVOC: PUF-based authentication via one-way chains, and
PAWOS: PUF-based authentication via one-time signatures.

Current Status:
Currently, the three implementation methods of PUF-based authentication were tested on the LPC55S6x board.

Find more about CROSSCON PUF-base authentication here:
https://github.com/crosscon/crosscon_puf_authentication

Secure FPGA provisioning

The secure FPGA provisioning service of the CROSSCON Stack will allow its clients to deploy and operate remotely on shared FPGA hardware platforms, while at the same time ensuring (i) the confidentiality of the proprietary FPGA workloads and designs, and (ii) the protection against malicious workloads from other users and/or malicious logic insertions into the design itself. Two primary services are essential to realizing secure FPGA provisioning: the secure FPGA configuration service and the secure FPGA configuration/bitstream scanning service.

Current Status:
The current prototype of the secure FPGA provisioning service is able to reconfigure two virtual FPGAs at runtime with different accelerators through the internal configuration port.

Find more about CROSSCON Secure FPGA provisioning here:
https://github.com/crosscon/FPGA_TEE

Control Flow Integrity

With Control Flow Integrity (CFI), CROSSCON protects against control flow attacks, i.e., those that aim to disrupt the sequence of executed instructions in an application, especially for IoT devices that either lack or are incompatible with existing hardware-specific security solutions.
We are developing two key CFI service implementations to address these threats:

- **Flashadow:** Provides backward edge control flow protection, ensuring that each function returns to its correct point of origin within the code. This service is designed for the CROSSCON non-MPU bare metal TEE.
- **uIPS**: Offers comprehensive protection for both backward and forward edges of control flow. This ensures that not only do functions return correctly, but also that the execution only proceeds to permitted destinations. This service is designed for the CROSSCON MPU bare metal TEE.

Current Status:
The current implementation for both MPU and non-MPU devices protects the forward and backward edges of the control flow, detecting unsafe deviations from the original sequence of operations and halting the execution in such cases.

Find more about CROSSCON CFI here:
https://github.com/crosscon/crosscon_puf_authentication

DISSEMINATION UPDATES

Past Events

During M13-M21, CROSSCON organized and participated in several events. Here is the summary of what hapenned!

NECS – PhD Winter School 2024

8-12 Jan 2024 | Cortina d'Ampezzo (Italy)

http://2024.necs-winterschool.disi.unitn.it/

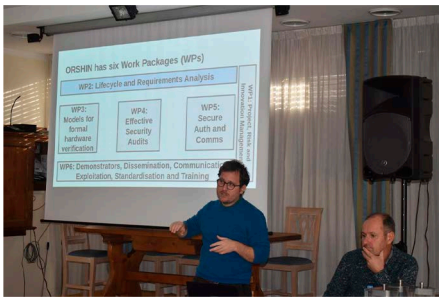
The NeCS PhD School, organized by CROSSCON and Marie Skłodowska-Curie's DUCA, trained junior researchers in cybersecurity, combining theoretical lectures with hands-on sessions. During the event, the School fostered a community for disseminating research and industry priorities. Speakers included Dr. Alexandra Dmitrienko (from UWU), Dr. Ahmad-Reza Sadeghi (from TUD), and Jurij Mihelic (from Beyond).

CROSSCON Workshop - Security Services for Connected Devices

12 Jan 2024 | Cortina d'Ampezzo, Italy

https://crosscon.eu/events/crosscon-workshop-security-services- connected-devices

The CROSSCON workshop on IoT security, held with NECS Winter School 2024, addressed security challenges across diverse devices and platforms. The workshop covered topics such as security on heterogeneous connected devices and highlighted advances from various EU projects, i.e., ORSHIN, SecOPERA, Project, ERATOSTHENES, ENTRUST, REWIRE, TRUSTaWARE, ENCRYPT Project, CyberSEAS Project, and CERTIFY. Thank you all for attending!



Workshop on Trusted Execution Environments (TEEs)

17 Jan 2024 | Online

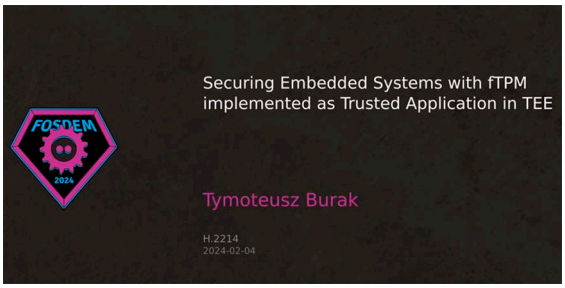
https://crosscon.eu/events/workshop-trusted-execution-environments-tees

Our partner Search-Lab, based in Budapest (Hungary), specializes in security testing and evaluation of ICT products, with a particular focus on the security of embedded systems like mobile devices. In partnership with CROSSCON, they delivered an online course about Trusted Execution Environments (TEEs), which was open to everyone.

DISSEMINATION UPDATES

Past Events

During M13-M21, CROSSCON organized and participated in several events. Here is the summary of what hapenned!



Securing Embedded Systems with fTPM implemented as Trusted Application in TEE

3-4 Feb 2024 | Brussels, Belgium

https://fosdem.org/2024/schedule/events/

At FOSDEM 2024, our partner 3mdeb participated in this event with a talk. The topic involves the benefits of fTPM as a TA in a TEE. Attendees learned about fTPM support and saw examples from GitHub for implementing it on ARM32 platforms.

CTI Workshop

6 Mar 2024 | Online

https://www.youtube.com/watch?v=69v0TILYJkw

This workshop was the inaugural event of the Cyber Threat Intelligence (CTI) cluster, which is organized by several EU-funded projects with the goal of gathering, producing, and sharing critical cyber threat information, specifically for IoT environments. CROSSCON participated in the event and contributed to a project overview presentation. Watch the video if you miss it!

CYSAT 2024

24-25 Apr 2024 | Paris, France

https://cysat.eu/

Our partner CYSEC participated in the 4th edition of CYSAT, one of the biggest European events on space cybersecurity. The event brings together academics, industrial players, and agencies to explore the latest innovations in the field.

CROSSCON & (Secure) Friends

28 Jun 2024 | Munich, Germany

https://crosscon.eu/news/crosscon-secure-friends

CROSSCON organized a side event at the RISC-V Summit. This workshop - "CROSSCON & (Secure) Friends - disseminated advances related to RISC-V with a particular focus on the topic of security among a set of EU-funded projects, i.e., CROSSCON, ORSHIN, REWIRE, SPIRS, SecOpera, and others.

KEYNOTE SPEAKER
Florian Wohlrab, CEO OpenHW Group

"Open Source RISC-V in Security and Safety"

During the workshop, "Flo", CEO of the OpenHW Group, discussed how the OpenHW Group facilitates collaboration on RISC-V for industrial use while maintaining its open-source nature and preparing it for safety and security applications.
Also, Frank from PULP Team, reveal its experience with open-source hardware since 2013, covering achievements and challenges in security and safety.
Don't miss out on the chance to view all the presentations from the workshop at the link above!

KEYNOTE SPEAKER
Frank K. Gürkaynak, PULP Team / ETH Zürich

"Security and Safety using Open Source Hardware, The Story So Far..."

DISSEMINATION UPDATES

Next Events

During next months CROSSCON will organize and participate in several events. Here is the summary of what events are scheduled!

The IoT Security Foundation Conference

23 Oct 2024 | IET, London

https://iotsecurityfoundation.org/conference/

This year CROSSCON project will be present at IoTSF. The conference theme is: "IoT Security: Past, Present, and Future". It will cover critical advancements in IoT security, including AI, quantum computing, and zero trust. Join us as we share insights from CROSSCON and engage with global IoT security experts.

NECS – PhD Winter School 2025

20-24 Jan 2025 | Cortina d'Ampezzo (Italy)

https://necs-winterschool.disi.unitn.it/

The NeCS PhD School will be organized by CROSSCON and Marie Skłodowska-Curie's DUCA. The main goal is to train junior researchers in cybersecurity, combining theoretical lectures with hands-on sessions.
We are expecting your participation in it!

News

4th GA Meeting

19-20 Mar 2024 Darmstadt, Germany

https://crosscon.eu/news/crosscon-4th-ga-meeting

The CROSSCON consortium recently assembled at the University of Darmstadt in Germany for a productive meeting filled with insightful discussions and valuable outcomes.

2nd Press Release

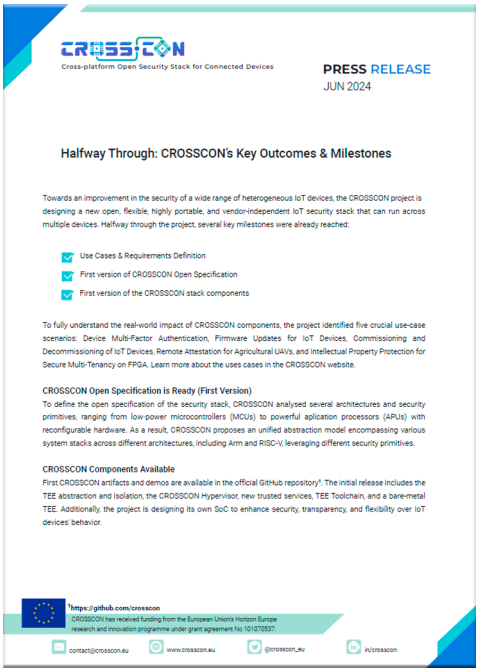
Jun 2024 Online

https://crosscon.eu/dissemination-material/second-press-release-june-2024

Towards an improvement in the security of a wide range of heterogeneous IoT devices, the CROSSCON project is designing a new open, flexible, highly portable, and vendor-independent IoT security stack that can run across multiple devices. Halfway through the project, several key milestones were already reached.

- CROSSCON Use Cases & Requirements Definition
- First version of CROSSCON Open Specification
- First version of the CROSSCON stack components

Check our second press release to know more.


CROSSCON
Cross-platform Open Security Stack for Connected Devices

PRESS RELEASE
JUN 2024

Halfway Through: CROSSCON's Key Outcomes & Milestones

Towards an improvement in the security of a wide range of heterogeneous IoT devices, the CROSSCON project is designing a new open, flexible, highly portable, and vendor-independent IoT security stack that can run across multiple devices. Halfway through the project, several key milestones were already reached:

- Use Cases & Requirements Definition
- First version of CROSSCON Open Specification
- First version of the CROSSCON stack components

To fully understand the real-world impact of CROSSCON components, the project identified five crucial use-case scenarios: Device Multi-Factor Authentication, Firmware Updates for IoT Devices, Commissioning and Decommissioning of IoT Devices, Remote Attestation for Agricultural UAVs, and Intellectual Property Protection for Secure Multi-Tenancy on FPGA. Learn more about the uses cases in the CROSSCON website.

CROSSCON Open Specification is Ready (First Version)

To define the open specification of the security stack, CROSSCON analysed several architectures and security primitives, ranging from low-power microcontrollers (MCUs) to powerful aplication processors (APUs) with reconfigurable hardware. As a result, CROSSCON proposes an unified abstraction model encompassing various system stacks across different architectures, including Arm and RISC-V, leveraging different security primitives.

CROSSCON Components Available

First CROSSCON artifacts and demos are available in the official GitHub repository[1]. The initial release includes the TEE abstraction and isolation, the CROSSCON Hypervisor, new trusted services, TEE Toolchain, and a bare-metal TEE. Additionally, the project is designing its own SoC to enhance security, transparency, and flexibility over IoT devices' behavior.

[1]https://github.com/crosscon

CROSSCON has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101070537.

contact@crosscon.eu www.crosscon.eu @crosscon_eu in/crosscon

DISSEMINATION UPDATES

Blog Posts

Over the past few months, we have published nine new blog posts where our partners share updates and insights on the project content they are responsible for.

FPGA-based Trusted Execution Environments and Their Use Cases

Field Programmable Gate Arrays (FPGAs) with Trusted Execution Environments (TEEs) enhance security and efficiency for cloud applications like Federated Learning, offering protection against threats without compromising performance.
Read more: https://crosscon.eu/blog/fpga-based-trusted-execution-environments-and-their-use-cases

Shaza Zeitouni
Post Doc
TUD

Huimin Li
Post Doc
TUD

Ensuring the Integrity of IoT Devices: Best Practices for Secure Firmware Updates

The Internet of Things (IoT) enhances convenience but poses security risks, especially in firmware updates. CROSSCON addresses these challenges with secure methods like authentication, Secure Boot, and Over-the-Air updates. It ensures integrity through version control, rollback protection, and rigorous testing, adhering to standards like ISO/IEC 27001 and NIST guidelines for robust IoT security.
Read more:
https://crosscon.eu/blog/ensuring-integrity-iot-devices-best-practices-secure-firmware-updates

Ákos Milánkovich
Security Analyst
SEARCH-LAB

Trust as a Foundation for Secure Internet of Things Services

In the expanding IoT landscape, cybersecurity of software and hardware is vital. Trust is established through a RoT and extended via a Chain of Trust, ensuring component integrity. CROSSCON enhances trusted services like Secure Boot and remote attestation, integrating secure, modular, and interoperable solutions for IoT security.
Read more: https://crosscon.eu/blog/trust-foundation-secure-internet-things-services

Peter Ten
Research Assist.
UWU

Lukas Petzi
Research Assist.
UWU

Embracing fTPM on embedded ARM Devices: Insights and Solutions

Trusted Platform Modules (TPMs) secure cryptographic keys but are costly. Firmware-based TPMs (fTPMs), integrated within CPUs and leveraging Trusted Execution Environments (TEEs) like Arm TrustZone, offer a cost-effective alternative. CROSSCON aims to simplify and standardize fTPM deployment across diverse IoT devices, enhancing security while addressing hardware and integration challenges.
Read more: https://crosscon.eu/blog/embracing-ftpm-embedded-arm-devices-insights-and-solutions

Tymoteusz Burak
Junior Embedd. Syst. Dev.
3MDEB

Stack and Stick are in Stock

The first half of the CROSSCON project targets validating research into practical techniques for complex IoT systems. CROSSCON aims to develop a versatile secure stack, leveraging diverse hardware and security mechanisms to ensure trust across multiple layers and devices, overcoming the limitations of tightly coupled, hardware-specific security solutions.
Read more: https://crosscon.eu/blog/stack-and-stick-are-stock

Aljosa Pasic
Senior Consultant
Eviden

DISSEMINATION UPDATES

Blog Posts

Using IEC-62443 to Secure Industrial Devices

The convergence of IT and OT in Industry 4.0 brings cybersecurity challenges. Barbara uses the IEC-62443 standards and the CROSSCON Secure IoT stack, including hypervisors and TEE isolation, to enhance security for industrial devices, ensuring compliance and protecting critical infrastructure in connected environments.
Read more: https://crosscon.eu/blog/using-iec-62443-secure-industrial-devices

Ainara Garcia
Project Management PMO
BARBARA IoT

Improving the resilience of trusted applications with control flow integrity

Control Flow Integrity is a time-honoured technique to prevent a whole class of attacks from compromising the correct execution of TAs. The implementation of a CFI primitive in the CROSSCON stack will definitely have a positive impact on the security of applications running on resource-constrained devices which are typical in the IoT world.
Read more: https://crosscon.eu/blog/improving-resilience-trusted-applications-control-flow-integrity

Alberto Tacchella
Post-doctoral
UNITN

Secure-by-formal-design: Towards better softwa-re and hardware assurance

Creating secure systems is not a one-time task but an ongoing process. It involves designing systems with security in mind and regularly updating them to keep pace with emerging threats. Remember, security is a journey, not a destination. Stay safe & secure!
Read more: https://crosscon.eu/blog/secure-formal-design

Jurij Mihelič
Senior Project Manager
BEYOND

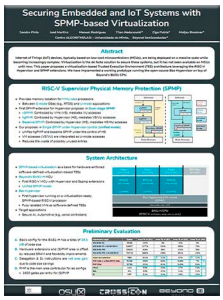
Challenges of Embedding Security in IoT Devices

The IoT revolution has brought about significant connectivity but also substantial security challenges, with vulnerabilities leading to severe consequences like data breaches and unauthorized control. Ensuring IoT security involves safeguarding devices, networks, and data through robust measures. Challenges include diverse hardware, resource constraints, scalability, and interoperability.
Read more:
https://crosscon.eu/blog/challenges-embedding-security-iot-devices

Malvina Catalano
R&D Scientist
CYSEC

DISSEMINATION UPDATES

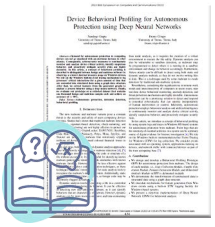
Latest Publications



Securing Embedded and IoT Systems with SPMP-based Virtualization

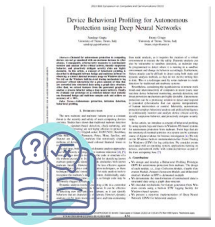
This poster presents a new TEE architecture for securing complex IoT devices using Bao Hypervisor and SPMP extensions on RISC-V architecture. It features a prototype implementation with the Bao Hypervisor on Beyond's BA51 CPU.

Sandro Pinto, José Martins, Manuel Rodrigues, Tilen Nedanovski, Ziga Putrle, Matjaz Breskvar, Securing Embedded and IoT Systems with SPMP-based Virtualization, RISC-V Summit 2024
https://riscv-europe.org/summit/2024/media/proceedings/posters/177_poster.pdf



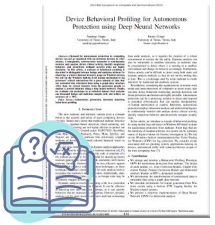
The Nonce-nce of Web Security: an Investigation of CSP Nonces Reuse

M. Golinelli, F. Bonomi & B. Crisp, The Nonce-nce of Web Security: An Investigation of CSP Nonces Reuse, In: Katsikas, S., et al. Computer Security. ESORICS 2023 International Workshops
https://link.springer.com/chapter/10.1007/978-3-031-54129-2_27



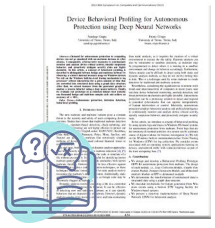
CryptojackingTrap: An Evasion Resilient Nature-Inspired Algorithm to Detect Cryptojacking Malware

A. Chahoki, H. Shahriari & M. Roveri, CryptojackingTrap: An Evasion Resilient Nature-Inspired Algorithm to Detect Cryptojacking Malware, in IEEE Transactions on Information Forensics and Security, 2024
https://ieeexplore.ieee.org/abstract/document/10400529



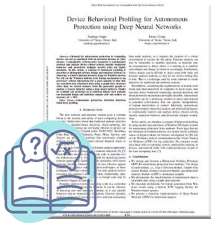
Marionette: Manipulate Your Touchscreen via A Charging Cable

Y. Jiang, X. Ji, K. Wang, C. Yan, R. Mitev, A. Sadeghi, W. Xu, Marionette: Manipulate Your Touchscreen via a Charging Cable, IEEE Transactions on Dependable and Secure Computing, 2024.
https://www.computer.org/csdl/journal/tq/5555/01/10288382/1Rp0oY44cWA



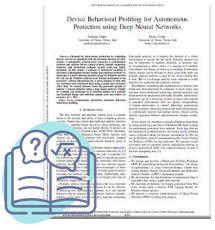
FreqFed: A Frequency Analysis-Based Approach for Mitigating Poisoning Attacks in Federated Learning

H. Fereidooni, A. Pegoraro, P. Rieger, A. Dmitrienko & A. Sadeghi, FreqFed: A Frequency Analysis-Based Approach for Mitigating Poisoning Attacks in Federated, Network and Distributed System Security (NDSS), 2024
https://arXiv preprint arXiv:2312.04432



Beyond Random Inputs: A Novel ML-Based Hardware Fuzzing

M. Rostami, M. Chilese, S. Zeitouni, R. Kande, J., Rajendran & A. Sadeghi, Beyond random inputs: A novel ml-based hardware fuzzing, Design, Automation & Test in Europe Conference & Exhibition (DATE), 2024
https://ieeexplore.ieee.org/document/10546625

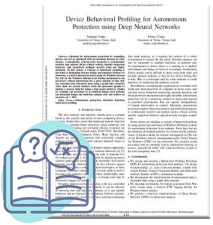


CROSSCON: Interoperable IoT Security Stack for Embedded Connected Devices

T. Gomes & S. Pinto, CROSSCON: interoperable IoT security stack for embedded connected devices, Embedded World 2024
https://ieeexplore.ieee.org/document/10218275

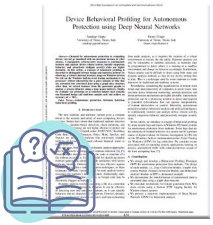
DISSEMINATION UPDATES

Latest Publications



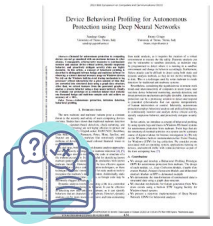
Lost and Found in Speculation: Hybrid Speculative Vulnerability Detection

M. Rostami, S. Zeitouni, R. Kande, C. Chen, P. Mahmoody, J. Rajendran & A. Sadeghi, Lost and Found in Speculation: Hybrid Speculative Vulnerability Detection, IEEE/ACM Design Automation Conference (DAC) , 2024
https://ieeexplore.ieee.org/abstract/document/10217861



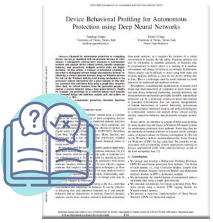
WhisperFuzz: White-Box Fuzzing for Detecting and Locating Timing Vulnerabilities in Processors

P. Borkar, C. Chen, M. Rostami, N. Singh, R. Kande, A. Sadeghi & J. Rajendran, Whisperfuzz: White-box fuzzing for detecting and locating timing vulnerabilities in processors, USENIX Security 2024
https://www.usenix.org/system/files/sec24fall-prepub-227-borkar.pdf



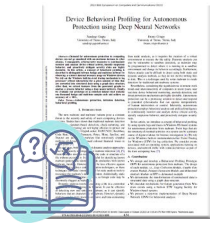
One for All and All for One: GNN-based Control-Flow Attestation for Embedded Devices

M. Chilese, R. Mitev, M. Orenbach, R. Atamli & A. Sadeghi. One for All and All for One: GNN-based Control-Flow Attestation for Embedded Devices. 2024
https://arxiv.org/abs/2403.07465



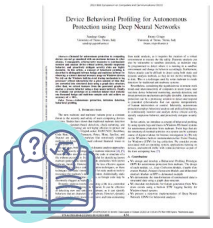
HSP-V: Hypervisor-less Static Partitioning for RISC-V COTS Platforms

J. Sousa, J. Martins, T. Gomes & S. Pinto, "HSP-V: Hypervisor-Less Static Partitioning for RISC-V COTS Platforms," in IEEE Access, 2024
https://ieeexplore.ieee.org/document/10528286



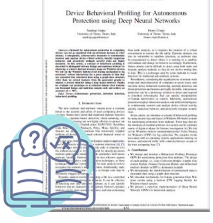
CROSSCON: Cross-platform Open Security Stack for Connected Devices

T. Gomes & S. Pinto, CROSSCON: Interoperable IoT Security Stack for Embedded Connected Devices, 2024
https://crosscon.eu/sites/crosscon/files/public/content-files/2024-04/ewC2024_13364_CROSSCON_Security_Stack_Tiago_Gomes.pdf



PUF-based Authentication in IoT against Strong Physical Adversary using Zero-Knowledge Proofs

L. Petzi, A. Dmitrienko & I.Visconti, PUF-based Authentication in IoT against Strong Physical Adversary using Zero-Knowledge Proofs. SafeThings, 2024
https://ieeexplore.ieee.org/document/10546625



Cyber-physical metropolitan area digital substations test bench for evaluating intrusion detection systems

S. Acevedo, T. Zerihun, H. Koshutanski & A. Bedoya, Cyber-physical metropolitan area digital substations test bench for evaluating intrusion detection systems, IEEE GPECOM 2024
https://www.techrxiv.org/doi/pdf/10.36227/techrxiv.171778519.94792591

GET IN TOUCH!

Next Release

NEWSLETTER #4

It will be released by the end of Q4 2024

Meanwhile, stay up-to-date with other important CROSSCON news by following our social media channels!

www.crosscon.eu contact@crosscon.eu @crosscon_eu in/crosscon

Subscribe the newsletter:
https://crosscon.eu/