INTERSECT Newsletter

First Edition – January 2023

Index

Reporting News

Power Side Channel Attacks on IoT processors successfully carried out at VU Amsterdam

Contact Person: Herbert Bos, VU Amsterdam, e-mail: HerbertB@cs.vu.nl

Reference WPs: WP4

System-on-chips in IoT devices protect sensitive information such as cryptographic keys, by relying on trusted execution environments such as Arm's TrustZone technology. TrustZone creates two worlds: a secure world that handles all sensitive operations and information and a normal world for non-sensitive operations. In this research, Maggie Mackenzie-Cardy shows that the isolation is not complete on modern CPUs such as Cortex M33 processors and attackers can still leak sensitive information by way of side channels that measure power and they do not even require physical access to the machine. Using the on-board analog-to-digital converter (ADC) to sample as frequently as possible the power consumption while the CPU is encrypting or decrypting a message, the attacker is able to reconstruct the key. The research proposes a novel way to overcome the problem that on-board power measurements are slow compared to the CPU speed. In particular, the processor used in this study operates at 110MHz while the ADC measures power at 7.33M samples/s. By accurately rerunning the attack with minor offsets in time ("do the attack, do the attack with 1 cycle delay, do the attack with 2 cycles delay, etc."), it is possible to obtain an improved signal with only very few traces. In some cases, fewer than 5,000 traces were needed to recover the key!

Radix Security – A new startup on 5G security from Radboud University in Nijmegen

Contact Person: Erik Poll, RU, e-mail: erikpoll@cs.ru.nl

Reference WPs: WP4, WP8

Research into mobile network security by Katharina Kohls at Radboud University https://kkohls.org and David Rupprecht at Ruhr University Bochum has led to the establishment of a new start-up Radix Security (https://radix-security.com) that will focus on 5G security.

HackNijmegen event held on Cybersecurity Attacks for OT Systems

Contact Person: Erik Poll, RU, e-mail: erikpoll@cs.ru.nl

Reference WPs: WP4

In a HackNijmegen event, twenty students of the Radboud University and Fontys spent a whole day pen-testing the IT infrastructure at Nijmegen town hall on18 November 18. Also some of the OT infrastructure managed by the municipality was in scope for this. Thanks to the CISO of Nijmegen to make this possible!

Ongoing Research on Privacy-by-Design for NextGen Smart Meters at RU

Contact Person: Erik Poll, RU, e-mail: erikpoll@cs.ru.nl

Reference WPs: WP2

Researchers from Radboud University have started a collaboration with the regional grid operators Stedin and Alliander on the privacy requirements for the next-generation smart meter for which the specs are currently being developed. For more info, contact Erik Poll or Pol van Aubel.

Two papers on INTERSECT FedLab recently presented at worldwide conferences

Contact Person: Savio Sciancalepore, TU/e, e-mail: s.sciancalepore@tue.nl

Reference WPs: WP7

Throughout the last two months, two papers based on the INTERSECT Federated Lab (FedLab) have been presented at top-notch worldwide conferences.
The paper containing the main rationale and design of the FedLab, namely, “Federated Lab (FedLab): An Open-source Distributed Platform for Internet of Things (IoT) Research and Experimentation”, was presented at the IEEE World Forum on IoT, held online in Yokohama

(Japan) from the 26th to the 30th of October, 2022. The paper was authored by Max Meijer, Giacomo Tommaso Petrucci, Matthijs Schotsman, Luca Morgese, Thijs van Ede, Andrea Continella, Ganduulga Gankhuyag, Luca Allodi, and Savio Sciancalepore, and it is available here.
Another paper, based on the FedLab, was presented at the ACSAC 2022 conference in Austin, Texas, on the 7th of December, 2022. The paper, namely, “Stepping out of the MUD: Contextual threat information for IoT devices with manufacturer-provided behaviour profiles”,, was authored by Luca Morgese (TNO), Thijs van Ede (UT), Tim Booji (TNO), Savio Sciancalepore (TU/e), Luca Allodi (TU/e), and Andrea Continella (UT), and it is available here.

You can keep in touch with the managers of the FedLab for joining the platform and carrying out shared research.

Proposed Projects

Internships and Msc Projects Available at Secura for RU and TU/e students

Contact Person: Erik Poll, RU, e-mail: erikpoll@cs.ru.nl

Reference WPs: WP2, WP3, WP4

Secura regularly has possibilities for Bachelor or Master thesis or internship projects: see https://www.secura.com/careers/students.

Research Internship available at Bosch Security Systems in Breda

Contact Person: Erik Poll, RU, e-mail: erikpoll@cs.ru.nl

Reference WPs: WP2

At Bosch Security Systems in Breda there is a possibility for a research internship to look at possibilities to integrate fuzzing into their software development processes. At Bosch Security Systems they o.a. make public address systems which involve embedded Linux components and high-quality audio solutions.

Contact Erik Poll to get in touch with Stephan van Tienen at Bosch.

Master Projects available on Attack Detection and Response for Non-Public 5G networks at TNO

Contact Person: Frank Fransen, TNO, e-mail: frank.fransen@tno.nl

Reference WPs: WP3

Our digital society is becoming increasingly dependent on ICT. Moreover, the continuous introduction of large numbers of Internet-of-Things technologies make it harder to grasp the full extent of this dependency and introduce new cyber security vulnerabilities. Given the complexity and continuously evolving cyber threat landscape and the speed at which cyber-attacks occur, automation to aid human analysis and execution of response actions at machine-speed is more and more seen prerequisite. TNO is working on technology to automatically assess and respond to emerging threats and ongoing attacks.

This master thesis project takes place in the context of NWA INTERSECT project (https://intersct.nl/) on IoT Security. Within this project the focus is on development of technology and tools for securing IoT devices that are connected via 5G Non-Public Network (NPN). NPNs are private 5G networks that provide network services to devices from an organisation (e.g. factory, campus). 5G NPN are particularly interesting for factories and large industry plants to connect Industrial IoT (IIoT) devices. These 5G NPN make use of the new 5G technologies, such as Network Function Virtualisation (NFV) and network slicing. 5G network slicing enables operators to create multiple independent virtual networks on the same physical network infrastructure. Each network slice can be tailored to a specific application by fulfilling specific network requirements, such as low latency, bandwidth, reliability, and security. Since 5G NPNs are private networks, the organisation operating this network can add specific defence mechanisms for monitoring, attack detection and response.

Within this master thesis project, you will study security functions in 5G NPN and how IoT devices can be protected using 5G technologies. The IoT security slice may include novel security functions such as dynamic monitoring and attack detection, automatic containment and recovery, and automatic vulnerability discovery and mitigation. During the project you will experiment with open source 5G core network software and develop a proof-of-concept of a 5G NPN with IoT security functions in the research cloud of TNO. This may include modifying or adding functions to the open source 5G core network software.

Requirements

Required Resources: Master student on computer science (preferably on cyber security)

Required Minimum Background Knowledge: You are familiar with information security, experience with programming and IP networks technology. You are analytical and you are capable of working autonomously. In addition, you have good communication skills and you are creative and innovative.

Location: In-person at TNO, Den Haag

Estimated Duration: 6-9 months

Temptative Starting Date: 2023