INTERSCT.

INTERSECT Newsletter

Issue no. 4 – July 2023

Index

1. Reporting News 2
1a. New Publications on IoT Security by Researchers at TU/e 2
1b. ISP 2023 Summer School approaching 2
1c. AlgoSoc Open Positions 3
1d. Blog Post about IoT Security on Nemokennislink 3
1e. Short Brief on the Commission's Proposal for a Cyber Resilience Act 3

2. Proposed Projects 5
2a. Research Internships and Msc Projects on Fuzzing Available at TNO 5
2b. Research Internships available at RDI 5
2c. Master Thesis Project on Network Traffic Monitoring in 5G Network Slices 6
2d. Research Internship available at Bosch Security Systems in Breda 7
2e. Internships and Msc Projects Available at Secura for RU and TU/e students 7

Reporting News

1a. New Publications on IoT Security by Researchers at TU/e

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

Reference WPs: WP3, WP56

The researchers at TU/e working in WP3 and WP56 recently got the following scientific works accepted for conference presentation:

- Stash Kempinski, Shuaib Ichaarine, Savio Sciancalepore, Emmanuele Zambon, “ICSvertase: A Framework for Purpose-based Designing and Classification of ICS Honeypots”, accepted for presentation at the 2nd Workshop on Cybersecurity in Industry 4.0 (SecIndustry), held in conjunction with the 18th International Conference on Availability, Reliability and Security (ARES) 2023, Benevento (Italy), Aug. 2023.

- Michele Campobasso, Radu Radulescu, Sylvan Brons, Luca Allodi, “You Can Tell a Cybercriminal by the Company they Keep: A Framework to Infer the Relevance of Underground Communities to the Threat Landscape”, accepted for presentation at the 22nd Workshop on the Economics of Information Security (WEIS), Geneva (Switerzland), July 5—8, 2023.

The online version of the papers will be made available soon through the INTERSECT website.

1b. ISP 2023 Summer School approaching

Contact Person: Lorenzo Dalla Corte, Tilburg University, e-mail: L.DallaCorte@tilburguniversity.edu

Reference WPs: WP5

ISP 2023 is an intensive one week academic post-graduate programme that provides students with a background in privacy from a technical, legal, and social perspective and helps them to establish a first international network with peers and senior academics across disciplines. The Fifth Interdisciplinary Summerschool on Privacy (ISP 2023) is themed "Assessing and mitigating privacy risks in the Internet of Things". See https://isp.cs.ru.nl/2023/

1c. AlgoSoc Open Positions

Contact Person: Eleni Kosta, Tilburg University, e-mail: E.Kosta@tilburguniversity.edu

Reference WPs: WP5

The OCW-funded Gravitation Program Public Values in the Algorithmic Society (AlgoSoc) is a response to the urgent need for an informed societal perspective on automation and automated decision-making. Grounded in a deep understanding of the systemic changes that ADS entail for core public institutions, for society, and for how public values are realized, AlgoSoc develops solutions for the design of governance frameworks needed to complement technology-driven initiatives in the algorithmic society.

There are open positions in the context of the AlgoSoc program. Interested readers can contact Prof. Eleni Kosta, or check the website of AlgoSoc, at https://algosoc.org.

1d. Blog Post about IoT Security on Nemokennislink

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

Reference WPs: WP2

There are more and more smart devices in the house that are connected via WiFi. This internet of things makes life a lot easier for the residents, but also poses a potential danger, as the security of all those devices differs enormously.

Mattis van 't Schip, a PhD student at Radboud University Nijmegen involved in INTERSECT who mainly focuses on the legal side of cybersecurity, talks about it in a recent blog post on the website Nemokennislink.

The complete blog post and interview is available at:
https://www.nemokennislink.nl/publicaties/help-de-slimme-apparaten-vallen-aan/

1e. Short Brief on the Commission's Proposal for a Cyber Resilience Act

Contact Person: Lorenzo Dalla Corte, Tilburg University, e-mail: L.DallaCorte@tilburguniversity.edu

Reference WPs: WP5

The PhD students at Tilburg University working within the WP5, namely Suzanne Nusselder and Pratham Ajmera, prepared a short brief on the Commission's proposal for a Cyber Resilience Act.

The CRA is intended to address two major problems affecting IoT products on the internal market: a generally low level of existing cybersecurity for connected devices, and a lack of information among users, preventing them from choosing among available products accurately.

The complete document is available at:
https://surfdrive.surf.nl/files/index.php/s/sajPfARlV8ln4EX

Proposed Projects

2a. Research Internships and Msc Projects available at OMRON

Contact Person: Armanda Ruiz Dominguez, OMRON, e-mail: amanda.ruiz.dominguez@omron.com

Reference WPs: WP2, WP3

At OMRON in Den Bosch, an international manufacturer of industrial controls systems, there are several possibilities for student interships:

- *Fieldbus Monitoring.* Fieldbus is a communication standard used in industrial control systems. Goal of this project is investigate techniques to identify and detect threats on the Fieldbus network. This would include analysis of the Fieldbus protocols and developing a monitoring solution for Fieldbus communications.
- *Industrial Security Standards.* Industrial PCs (IPCs) are a key component used in industrial control systems. Goal of this project is to assess the security of OMRON's NY5 IPC using the security standard IEC 62443-4-2. This would involve analysing the security requirements of IEC62443-4-2, creating a framework to assess these security requirements, and applying it to the OMRON IPC.
- *Secure Fieldbus Communications with 5G/TSN.* Fieldbus networks pose a risk for cyber attacks: sensor data is purposely altered this can cause plant malfunction or harm personnel. Goal of the project is to look into solutions to secure these communications with 5G/TSN, investigating the choice in algorithms, and implementing the chosen solution.

2b. Research Internships available at RDI

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

Reference WPs: WP3, WP7

Agentschap Telecom is the Dutch government agency responsible for ensuring secure radio communications for the whole Netherlands. The activities of the agency span across several enabling technologies, such as Radio, Television, Telephony and also the Internet, including the safe usage and availability of new communication technologies and paradigms, such as the Internet of Things (IoT) [1].

In the IoT context, Agentschap Telecom continuously evaluates for robustness and security consumer IoT products available on the Dutch market. In particular, through customized state-of-the-art procedures, the Agency autonomously evaluate if the level of security achieved by commercially-available IoT products actually adheres to the claimed security levels, e.g., assured through well-known certification and compliance labels. When major security issues are found, the Agency can trigger follow-up actions and sanctions, possibly leading to the withdrawal of the

IoT product from the Dutch market. Daily activities are carried out at a dedicated “IoT Testlab”, just opened in Amersfoort, where experts of the Agency use dedicated advanced equipment and tools to ensure digital security of Internet-connected consumer environments.

However, at this time, most of the procedures deployed by the Agency to evaluate the security of consumer IoT devices are manual, leading to potential inefficiencies. In this context, automatizing (part of) the procedures for specific classes of IoT devices could allow for more efficient operations, as well as additional insights into the robustness of such IoT devices.

The scope of this Master’s Project, carried out by TU/e (Eindhoven) and Agentschap Telecom, is to develop automated procedures for the security evaluation of Consumer IoT Devices. Based on the specific use of IoT devices and applicable security standards, the aim of the project is to come up with routines for a set of automatic tests, requiring minimal interaction from the personnel of the Agency and the final user, and providing a report of the behavior of such IoT device to specific threats. Such an output could then be used by the Agency to draw conclusions about the effective security guarantees provided by the IoT device under test.

[1] Agentschap Telecom Website, “About Us”. Online: https://www.agentschaptelecom.nl/over-agentschap-telecom

2c. Master Thesis Project on Network Traffic Monitoring in 5G Network Slices

Contact Person(s): Frank Fransen, TNO, e-mail: frank.fransen@tno.nl, Andrea Continella, UT, a.continella@utwente.nl

Reference WPs: WP3

5G adoption is rapidly increasing, and many new use cases are envisioned for connecting IoT devices over 5G. As such, it is relevant to investigate security solutions for these new use cases. This includes security solutions for protecting the IoT Devices from cyber-attacks, and for protecting other systems from compromised IoT devices that are connected to the Internet over a 5G network.

For the master thesis project a testing infrastructure was set up using open source 5G components that conform to the 3GPP specifications. On top of this infrastructure a network traffic monitoring solution was implemented by adding a separate monitoring host. Traffic is mirrored to this separate host, as opposed to running an intrusion prevention system (IPS) on the host that routes the traffic. This specific architecture is tested using several simulated attacks. In addition, the project suggests various response actions available in 5G networks based on functions present in the 3GPP specifications, e.g. filtering traffic using Packet Detection Rules (PDR) and Forwarding Action Rules at the User Plane Function (UPF), and isolation using the 5G network slice technology. One of these response actions is implemented to be applied in an automatic fashion when malicious traffic is detected. This automated response action is also tested with a simulated attack.

2d. 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..

2e. 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.