INTERSECT Newsletter

Issue no. 2 – March 2023

Index

Reporting News

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

Contact Person: Luca Allodi, TU/e Eindhoven, e-mail: l.allodi@tue.nl

Reference WPs: WP2, WP4

The researchers at TU/e working in WP4 recently finalized the publication of the following scientific works:

- P. Burda, L. Allodi. and N. Zannone, A decision-support tool for experimentation on zero-hour phishing detection, Proceedings of 15th International Symposium on Foundations & Practice of Security (FPS 2022), LNCS Springer, Ottawa, Canada 2022, In press.

- I.A. Marin, P. Burda, L. Allodi. and N. Zannone, The Influence of Human Factors on the Intention to Report Phishing Emails, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems 2023, ACM, Hamburg, Germany, 2023, To appear.

- Campobasso, Michele and Allodi, Luca, THREAT/crawl: a Trainable, Highly-Reusable, and Extensible Automated Method and Tool to Crawl Criminal Underground Forums, 5 Nov 2022, (Accepted/In press) 17th Symposium on Electronic Crime Research (APWG eCrime 2022) - https://michelecampobasso.github.io/publication/2022-11-24-threatcrawl

Also, the following presentations were given (numbering does not match papers)

- Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale, 19 May 2022, WP4 “Attack”, INTERSCT ’22, Enschede

- THREAT/crawl: a Trainable, Highly-Reusable, and Extensible Automated Method and Tool to Crawl Criminal Underground Forums, 5 Nov 2022, 17th Symposium on Electronic Crime Research (APWG eCrime 2022)

- Mathematics and Computer Science poster session: Impersonation-as-a-Service: Characterizing the Emerging Criminal Infrastructure for User Impersonation at Scale, 30 Nov 2022, Eindhoven University of Technology

- P.Burda, A decision-support tool for experimentation on zero-hour phishing detection, at 15th International Symposium on Foundations & Practice of Security 2022, Ottawa, 12/12/2022

1b. New Survey and Classification on Fuzzing Tools by Researchers at RU

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

Reference WPs: WP2, WP4

A comprehensive survey and classification of fuzzing tools for stateful systems is available as pre-print: Fuzzers for stateful systems: Survey and Research Directions by Cristian Daniele, Seyed Behnam Andarzian, Erik Poll. The pre-print is available here: https://arxiv.org/abs/2301.02490

1c. Highlights from Completed Internships and Msc Projects from RU Students at Secura

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

Reference WPs: WP2, WP4

A master student from Radboud University, Thijs Fransen, completed his master thesis at Secura on the use of symbolic execution to analyse binaries with the aim to detect vulnerabilities.
Another RU student, Ankit Gautam, completed an intership at Secura looking into the security of signalling using EMRTS (European Rail Traffic Management System) as used by ProRail.

1d. ISP 2023 Summer School to be held this Summer

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/

Proposed Projects

2a. Research Internships and Msc Projects on Fuzzing Available at TNO

Contact Person: Stefan van den Berg, TNO, e-mail: stefan.vandenberg@tno.nl

Reference WPs: WP2, WP4

At TNO there are possibilities to do a research internship or master thesis on fuzzing or, more broadly, on vulnerability research and software security testing. This could take place at TNO Eindhoven, Den Haag or Groningen. Interested students can contact the reference person Stefan van den Berg at Stefan.vandenberg@tno.nl.

2b. 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.

2c. 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.

More details can be found at the following link:
https://www.tno.nl/en/careers/vacancies/2023/02/internship-iot-security-5g-npn/

Requirements

Student Requirements: 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, as early as possible