LASIGE

driven by excellence

resilient distributed and networked systems   **cyber-physical systems**

Tue

30

Apr

2024

FORSTBYTE: TOWARDS A BETTER UNDERSTANDING OF CURRENT CYBER SECURITY THREATS

Speaker
Hans P. Reiser

Affiliation
Department of Computer Science, Reykjavík University, Iceland

When
April 30th, 14h00

Where
C6.3.27

Abstract

Cyber security threats are increasing worldwide, with an ongoing trend towards escalating complexity and severity of attacks. Robust cyber security measures have never been more important. A prerequisite for such measures is an accurate understanding of the actual threat landscape. In the first part of this talk, we look into the specific challenges confronting Iceland's cybersecurity landscape. At Forstbyte, Iceland's national cyber security laboratory, our focus is on addressing current gaps in cyber security through interdisciplinary collaboration, encompassing social sciences, legal frameworks, organizational aspects, and technical expertise. In the second part of this talk, we narrow our focus to one technical aspect: gaining deeper insights into the tactics and strategies used by cyber adversaries. Understanding their motivations, origins, and methods will serve as a valuable basis for developing efficient cyber defense. For that purpose, we take a deeper look into high-interaction honeypots based on virtual machine introsection (VMI). While VMI technology has existed for over two decades, its practical application in real-world scenarios is still limited. Our research refines existing VMI tools and enables the efficient use of VMI in diverse server environments and cloud infrastructures. On that basis, we enable the operation of VMI-based honeypots as robust platforms for capturing the evolving threat landscape. Looking ahead towards future work, we plan to leverage artificial intelligence (AI) to enhance honeypots. Through the generation of synthetic data and emulation of common network environments, such as Small and Medium Enterprises (SMEs) and household networks, we aim to enhance realism and contribute to strengthening Iceland's cybersecurity resilience and global cyber defense.

Short bio:

Hans P. Reiser is an Associate Professor in the Department of Computer Science at Reykjavík University, Iceland. He graduated in computer science from University of Erlangen, Germany, and received his PhD degree from Ulm University, Germany, in 2007. Before moving to Iceland, he worked as an assistant professor at the University of Lisbon, Portugal (2007-2011) and the University of Passau, Germany (2011-2021). He was also a visiting professor at Carnegie Mellon University, USA (2010), and Karlsruhe Institute for Technology (KIT). Hans P. Reiser's research focuses on building secure and reliable distributed systems, exploring novel methods for detecting, masking, and analyzing malicious faults.

Ciências ULisboa   FCT Fundação para a Ciência e a Tecnologia