Keynotes

Tuesday

Speaker: Dr. Anand Rajan


Abstract: This talk will explore security for 3 very important emerging paradigms (IoT, 5G, Blockchain).

1. **IoT Security:** In the past couple of years, there has been an increasing trend of security issues in the IoT context. With the projected exponential growth of connected devices, an IoT attack has significant security implications for device-owner as well as enterprise targets. Due to cost and energy constraints, security is often left out or becomes an afterthought, creating serious vulnerabilities in IoT systems. The consequences of IoT system compromise can be catastrophic, since life and physical property is usually at stake. Thus it is important to establish a foundation for Trustworthy, Safe, and Reliable IoT systems. We will present an overview of the research challenges and opportunities in building such a secure IoT foundation.

2. **5G Security:** While previous generations of cellular technology (including LTE) were designed to connect every human being with ever faster connectivity, 5G has the additional ambition to connect not just all the people but also all Things on this planet. Operators are looking for cheaper and quicker ways to deploy new IoT services on the same physical network, which would require network optimizations and innovations for these new applications. 5G must meet aggressive performance targets without compromising security and privacy requirements. A set of concepts are being embraced by the operators including SW Defined Networking (SDN), Network Function Virtualization (NFV), Network Slicing, Cloud-Radio Access Network (CRAN), Mobile Edge Computing (MEC). These concepts are likely to introduce new threat surfaces and deserve careful consideration and co-design with security.

3. **Blockchain Security:** We often talk about a blockchain as the replacement for a trusted third party for interactions within a community; i.e. the community ascribes the ultimate authority about “truth” to the blockchain. However, for applications built around a network of Things, the blockchain must be situated within a much larger context that incorporates institutional relationships, legal requirements, and regulatory control. There is a real danger for those deploying blockchain-based IoT solutions to believe that the tamperproof nature of the blockchain provides assurances about integrity and trustworthiness of information (and about actions driven by that information). A more realistic view is that the role of the blockchain transitions from a source of “shared truth” about the state of a system to a log of “decisions and actions” that might need to be adjusted in the future.
Biography: Anand Rajan is the Senior Director of the Emerging Security Lab at Intel Labs. He leads a team of researchers whose mission is to investigate novel security features that raise the assurance of platforms across the compute continuum (Cloud to Wearables). The topics covered by his team span Trustworthy Execution Environments (TEE), IoT & Mobile Security, Cryptography, and Security for Emerging Paradigms (e.g. Autonomous Systems, 5G). Anand is a Principal Investigator for Intel’s research collaboration with academia, government, and commercial labs on Trustworthy Platforms. He is the mentor for the Security Research Sector of Intel’s Corporate Research Council. Anand was an active member of the IEEE WG that crafted the P1363 (public-key crypto) standard. Anand and team developed the Common Data Security Architecture specification that was adopted as a worldwide standard by The Open Group. His team was also instrumental on several security standardization efforts (e.g. PKCS#11, BioAPI, UPnP-Security, & EPID). Prior to joining Intel in 1994, Anand was technical lead for the Trusted-UNIX team at Sequent Computer Systems and worked on development and certification of a TCSEC B1-level Operating System.
**Wednesday**

**Speaker:** Prof. Dr. Herbert Bos

**Dependability, Security and Performance walk into a bar...**

**Abstract:** Dependability problems have a nasty habit of turning into security problems. Sometimes, even dependability solutions have a habit of turning into security problems. Oh, and performance optimizations also habitually turn into security problems. In this talk, I will look into this phenomenon by way of illustrative examples that span the history of computer security. From the humble buffer overflow to today’s sophisticated microarchitectural attacks, they all have their roots in dependability and performance issues. Why is this?

While examining this question, I will talk about some of the attacks and defenses that we developed within VUSec at Vrije Universiteit Amsterdam. I will argue that attackers increasingly target the hardware rather than the software. As a result, even the most secure, bugfree, formally verified, and reliable software is, once again, at the mercy of attackers.

Finally, I will discuss the lessons we can learn from this trend. I will argue that dependability, security and performance are strongly related in often unexpected ways, and that handling one without the other is a recipe for disaster at a later stage.

**Biography:** Herbert Bos is full professor at Vrije Universiteit Amsterdam in the Netherlands where he heads the VUSec research group. He obtained his Ph.D. from Cambridge University Computer Laboratory (UK). Coming from a systems background, he drifted into security a few years ago and never left. He is very proud of his (former) students, three of whom have won the Roger Needham Ph.D. Award for best Ph.D. thesis in systems in Europe. In addition, VUSec has won three of the four Pwnie Awards awarded to researchers in the Netherlands. He claims that his life would be happier if he found a very good systems postdoc to hire (so if this is you, do apply!).

![Image of Herbert Bos]