1400 - Trojan-tolerant Hardware & Supply Chain Security in Practice

Saturday at 14:00 in Track 2
45 minutes | Art of Defense, Demo, Tool
Vasilios Mavroudis*Doctoral Researcher, University College London*

Dan Cvrcek*Co-founder, Enigma Bridge Ltd*

The current consensus within the security industry is that high-assurance systems cannot tolerate the presence of compromised hardware components. In this talk, we challenge this perception and demonstrate how trusted, high-assurance hardware can be built from untrusted and potentially malicious components.

The majority of IC vendors outsource the fabrication of their designs to facilities overseas, and rely on post-fabrication tests to weed out deficient chips. However, such tests are not effective against: 1) subtle unintentional errors (e.g., malfunctioning RNGs) and 2) malicious circuitry (e.g., stealthy Hardware Trojans). Such errors are very hard to detect and require constant upgrades of expensive forensics equipment, which contradicts the motives of fabrication outsourcing.

In this session, we introduce a high-level architecture that can tolerate multiple, malicious hardware components, and outline a new approach in hardware compromises risk management. We first demo our backdoor-tolerant Hardware Security Module built from low-cost commercial off-the-shelf components, benchmark its performance, and delve into its internals. We then explain the importance of "component diversification" and "non-overlapping supply chains", and finally discuss how "mutual distrust" can be exploited to further reduce the capabilities of the adversaries.
Vasilios Mavroudis
Vasilios Mavroudis is a doctoral researcher in the Information Security Group at University College London. He studies security and privacy aspects of digital ecosystems, with a focus on emerging technologies and previously unknown attack vectors.

He is currently working on a high-assurance cryptographic hardware. In cooperation with industrial partners, he has recently prototyped a high-assurance hardware architecture, that maintains its security properties even in the presence of malicious hardware components.

Past works include his recent publication on the ultrasound tracking ecosystem which

received wide-spread attention and is considered the seminal work on that ecosystem, and auditing tools for the Public Key Infrastructure of Deutsche Bank. Moreover, he has participated in an international consortium studying large-scale security threats in telecommunication networks, and cooperated with UC Santa Barbara in several projects, including a detection system for evasive web-malware.

Vasilios holds an Information Security MSc from UCL, and a BSc on Computer Science from University of Macedonia, Greece.

Dan Cvrcek

Dan Cvrcek is a security architect and engineer learning how to run his start-up Enigma Bridge. He has extensive experience with large banking systems from operational procedures to system architectures: Swift, card payment processing, UK Faster Payments, large key management systems. His hardware encounters include smart cards, custom and embedded systems, and hardware security modules, from design, testing, defences to attacks. He reverse-engineered a hidden API of Chrysalis-ITS crypto modules (now SafeNet) with Mike Bond, Steven Murdoch and others. Dan got his uni degrees (PhD and Associate Prof.) from Brno University of Technology, and had fun as a post-doc at the University of Cambridge (2003-2004, 2007-2008), Deloitte London (2008-2009), start-ups, freelance security consultant (2010-2016) - clients include Barclays and Deutsche Bank, co-founded Enigma Bridge in 2015.

@dancvrcek

Contributor Acknowledgement:
The Speakers would like to acknowledge the following for their contribution to the presentation.

George Danezis, Professor (University College London)
Petr Svenda, Security Researcher (Masaryk University)

#defcon25/by_track/track2/saturday #defcon25/By_Day/_saturday