Securing Cryptographic Systems against Quantum Adversaries and Hardware Exploits

Aydin Aysu
The University of Texas at Austin

Thursday, March 29, 2018
11:00 am – 12:00 pm
Showcase Room

Abstract:

Cryptography is essential for building trust into electronic world. Securing cryptographic systems of the future require using new theoretical and physical defenses. On the one hand, developments in quantum computing technologies are threatening hard mathematical problems that existing cryptographic systems rely on. On the other hand, deployment of embedded systems into the Internet-of-Things enables physical access to hardware, opening a new attack surface for exploits. In this talk, I will present a series of systems that can mitigate such powerful attacks. In the first part of the talk, I will analyze implementations of future cryptographic systems that can withstand theoretical quantum cryptanalysis. I will first demonstrate new techniques to break into these post-quantum encryption systems purely by observing the power consumption of the hardware and then propose low-overhead defenses to mitigate such vulnerabilities. In the second part of the talk, I will describe systems to secure the hardware root of trust against physical readout and side-channel attacks. I will describe methods for engraving unique digital keys deep into the hardware through physical unclonable functions – a hardware security primitive to construct digital fingerprints from process manufacturing variations – and demonstrate a novel method for secure key generation in hardware.

Short Bio:

Aydin Aysu is currently a Post-Doctoral Research Fellow in the Electrical and Computer Engineering Department of the University of Texas at Austin. He received his Ph.D. degree in Computer Engineering from Virginia Tech in 2016 and his M.S. degree in Electronics Engineering from Sabanci University, Istanbul, Turkey, in 2010. His research focuses on the development of secure systems that prevent cyberattacks targeting hardware vulnerabilities.