Making an Authentication Token IC Based on the Open Titan Project

Johann Heyszl, Fraunhofer AISEC, DE

Abstract

USB security tokens are powerful and established second authentication factors. We analyzed available open source products and found severe vulnerabilities in some of the included general purpose microcontrollers. We therefore posed the question: How is a hardened microcontroller for authentication tokens made from open source designs? In this talk, we describe our efforts in modifying the OpenTitan project for this purpose. Our goals are preventing attacks as seen in the real world and simplifying ASIC fabrication. In particular, we turn the OpenTitan into a flashless design, i.e., we move the NVM off-chip, and complement it with post-quantum secure boot, rigorous isolation for cryptographic keys and authenticated debug.

Biography

Dr. Johann Heyszl received his PhD from the Technical University of Munich in the field of applied cryptography and its protection against sophisticated side-channel attacks. He is head of the Hardware Security department at the Fraunhofer Institute for Applied and Integrated Security AISEC in Garching near Munich and deputy head of the institute. His focus is on security analysis, and information security design in embedded systems from different application domains.
In networked IoT applications, the department also focuses on hardware-related attacks and corresponding hardening. The institute conducts research on other current topics, such as information security in artificial intelligence applications, security of cloud infrastructures, and has distinctive areas of focus in domains such as automotive.