An infestation of dragons: Exploring vulnerabilities in the ARM TrustZone architecture | Program | Android Security Symposium 2015

Josh Thomas

Atredis Partners, Houston, TX, USA

Josh Thomas is a founding member of Atredis Partners, a niche consulting shop performing reverse engineering and security assessments of hardware and software products for vendors and end customers. Previously, he was a Senior Research Scientist with Accuvant's Applied Research team, and has worked as a Senior Research Engineer at The MITRE Corporation. Josh specializes in mobile, embedded systems, protocol and architecture analysis and has a deep history with malware and advanced root-kit research. Josh has written for multiple journals and industry publications over the past years and he has open sourced the entirety of his work for the DARPA Cyber Fast Track program.

Charles Holmes

Atredis Partners, Boston, MA, USA

Charles Holmes has spent nearly the last decade working on sensitive projects for various US government and research organizations. Charles specializes in mobile security, malware and rootkit development, and advanced software engineering.
Prior to joining Atredis, Charles was a Senior Research Lead with The MITRE Corporation. In that role, Charles

led research into a variety of mobile platforms including Apple, Android, Telematics, and Blackberry.
Before shifting focus to mobile security, Charles worked on a variety of projects for the Department of Defense. These projects included the next generation software for the dismounted soldier, tactical radio networking, RFID card readers, nuclear threat modeling, and mission planning systems.

ARM TrustZone is being heavily marketed as a be all solution for mobile security. Through extensive marketing promising BYOD, secure PIN entry, and protection against APT (http://www.arm.com/products/processors/technologies/trustzone/index.php) and the prevalence of ARM devices on mobile platforms, millions of devices now contain an implementation of TrustZone. However, the current drivers for TrustZone adoption primarily relate to vendor lock and Digital Rights Management (DRM), rather than increasing the difficulty in compromising user data. Further, due to TZ architecture, the inclusion of DRM protections provide a net reduction in real world security provided to the device owner.

In this talk, we provide an overview of the ARM TrustZone architecture as utilized by modern Android, Blackberry, and Windows phones. We discuss its potential, its current use cases, its shortcomings, and its impact on the security of modern phones. At this point, we dive into the details of the Qualcomm implementation, which is utilized on the flagship mobile devices from each major vendor, excluding Apple. Specifically, we cover vulnerabilities in codebases from Qualcomm, OEM Vendors, and 3rd Parties, as well as attack surface, exploitation pathways, difficulties, and successes.

Get the slides here.