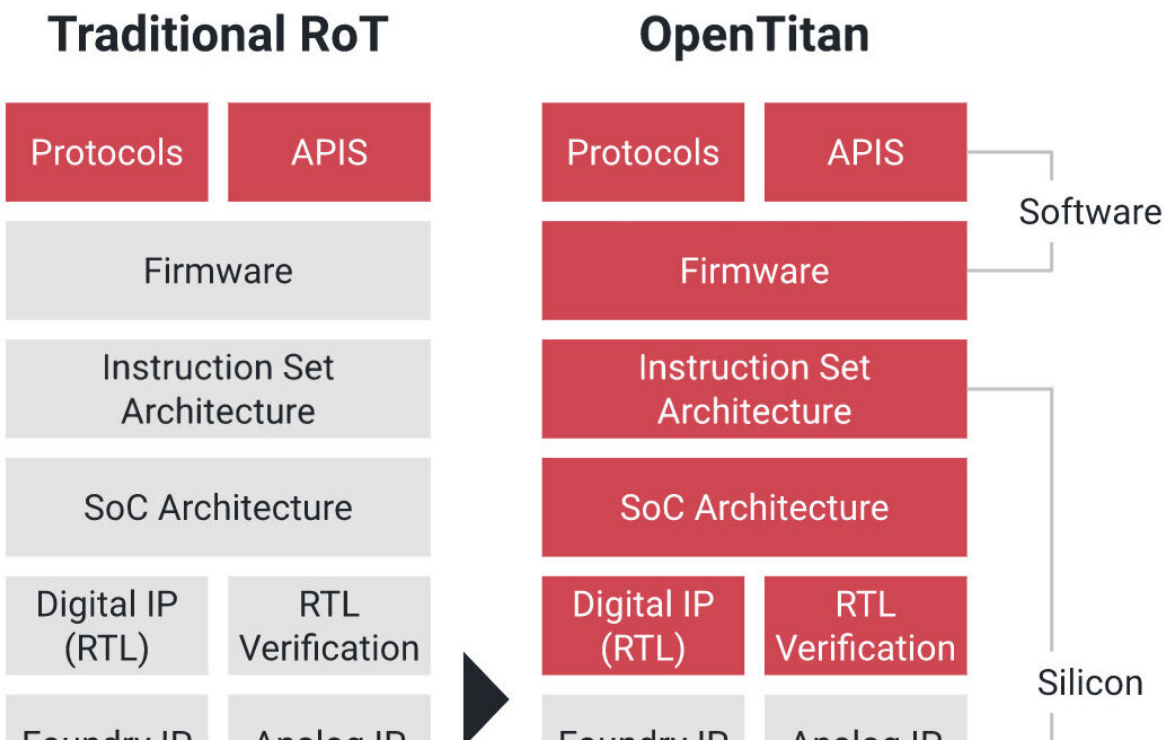
OpenTitan for data centers: Google, partners push secure silicon design

November 7 2019, by Nancy Cohen



A comparison of the major design components of a traditional RoT and an OpenTitan RoT. Credit: Google

The Google Security Blog on Tuesday announced OpenTitan as an open source chip design, where other organizations have joined Google in an effort to further rise the bar on security surrounding the original Titan chip.

Titan is Google's custom root of trust (RoT) chip. Google in the past has described Titan as "a secure, low-power microcontroller designed with Google hardware security requirements and scenarios in mind."

Titan helps ensure that machines in Google's data centers boot from a known trustworthy state with verified code.

In a 2017 post from the Google Cloud site, readers were told about Titan's role in the cloud, used as a data center layer of defense.

"In our datacenters, we protect the boot process with secure boot. Our machines boot a known firmware/software stack, cryptographically verify this stack and then gain (or fail to gain) access to resources on our network based on the status of that verification. Titan integrates with this process and offers additional layers of protection."

Now in 2019, it is going open source.

Zack Whittaker in TechCrunch: "The aim of the new coalition is to build trustworthy chip designs for use in data centers, storage and computer peripherals, which are both open and transparent, allowing anyone to inspect the hardware for security vulnerabilities and backdoors."

Google wanted the silicon design to be made more transparent, more trustworthy and ultimately secure. The Tuesday blog stated that now "we want to spread the benefits of reliable silicon RoT chips to our customers and the rest of the industry." OpenTitan as a project aims to deliver with results of a high-quality RoT design and integration guidelines. The silicon design, platform-agnostic, can be integrated into data center servers.

Anyone can contribute to OpenTitan's design and documentation as the project moves to its next phases. The blog post described what they are

building: a logically-secure silicon design, including reference firmware, verification collateral and technical documentation.

"As privileged software attacks increase and more research becomes available on rootkits, we have committed to delivering secure boot and hardware-based root of trust for machines that form our infrastructure and host our Google Cloud workloads."

Google is not in this alone; it has a number of partners haring the same pursuit of security. Zack Whttaker in *TechCrunch* said the coalition "comes at a time when tech giants and governments alike are increasingly aware that hostile nation states are trying to infiltrate and compromise supply chains in an effort to carry out long-term surveillance or espionage."

The OpenTitan project is managed by the lowRISC, a company with an engineering team based in Cambridge, UK. The announcement also came from lowRISC on Tuesday, having stated, "Today, at the mid-point of the project, we're opening up the GitHub repository containing this work, so others can get involved!"

Royal Hansen and Dominic Rizzo are the two who authored the Tuesday announcement on the Google blog. "Security begins with secure infrastructure," they said. "To have higher confidence in the security and integrity of the infrastructure, we need to anchor our trust at the foundation - in a special-purpose chip."

Hansen, quoted in *MIT Technology Review*, said that "The security guarantee the chip confers is "super critical when you're running the planet."

The article in *MIT Technology Review* clearly described what the technology does and quoted a security researcher in Amsterdam.

"Google wants to ensure from the moment you press the power button that they can verify exactly the sequence of everything that happens before the first instruction gets executed," says Kaveh Razavi, a security researcher at Vrije Universiteit Amsterdam. OpenTitan will kill the entire boot process if the code generated by the firmware doesn't match the code expected by the chip."

The lowRISC announcement quoted Dominic Rizzo, OpenTitan Lead at Google: "Customers are asked to put faith in proprietary root of trust chips for mission-critical systems without the ability to fully understand, inspect and therefore trust them...Security should never be built on opacity."

A coalition of partners include ETH Zurich, G+D Mobile Security, Nuvoton Technology (semiconductor manufacturer), and Western Digital.

Patrick Howell O'Neill at *MIT Technology Review* commented: "The cloud runs the world...For hackers, the data center is the target's brain—one of the most important points of control and one of the highest-value targets."

More information: security.googleblog.com/2019/1 … ing-transparent.html
opentitan.org/