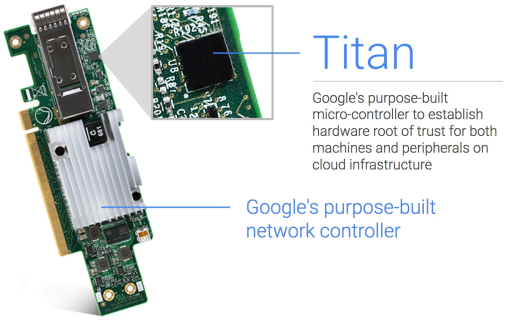
How does Google take care of security in its cloud servers? A company blog post reveals the details-- Titan, a "secure, low-power microcontroller designed with Google hardware security requirements and scenarios in mind."



As the blog post explains, the Titan chip integrates with the secure boot process. This involves the server boot a known firmware/software stack, cryptographically verify the stack and then gain (or fail to gain) access to network resources according to the verification. Titan also adds further layers of security, namely remediation (reestablishes trust in the event of firmware bugs) and first-instruction integrity (identifies the earliest code running on each machine's startup cycle).

For the curious about the hardware, Titan consists of a secure application processor, a cryptographic co-processor, a hardware random number generator, a sophisticated key hierarchy, embedded static RAM (SRAM), embedded flash and a read-only memory block. It communicates with the main CPU via Serial Peripheral Interface (SPI) bus, and interposes between the boot firmware flash of the first privileged component (such as BMC or PCH) to observe every byte of boot firmware.

A further security step involves a Titan-based end-to-end cryptographic identity system acting as the root of trust for various cryptographic operations. Making a Titan chip generates unique keying material for each chip, which is stored into a registry database. In turn, the database is cryptographically protected using keys held in an offlne quorum-based Titan Certification Authority (CA). Thus, authentication of a Titan chip requires going through the CA and the quorum of Titan identity administrators.

Does such security give Google the edge over the current cloud industry leaders, Microsoft and Amazon? Google insists this is the case, even if analysts are somewhat skeptical. As Gartner

tells Reuters, "security is a hallmark for both AWS and Microsoft. Google has a lot more work to do."

On the other hand security consultant Denim Group is more enthused, stating "those level of adversaries certainly have an incentive to hack or to have influence over the security of hardware. It's interesting of Google to say, 'Here's one part of the hardware that we're going to control.'"

Go Titan in Depth: Security in Plaintext

Go Google Touts Titan Security Chip to Market Cloud Cervices (Reuters)