



G+D Mobile Security unterstützt lowRISC und Google beim Open-Source-Projekt OpenTitan

2019-11-05

München

Giesecke+Devrient

München, 5. November, 2019 – G+D Mobile Security, ein führender Anbieter von Vernetzungs- und Sicherheitslösungen im IoT, gibt die Zusammenarbeit mit lowRISC und Google bekannt, um gemeinsam OpenTitan, ein Open-Source-Referenzdesign für eine Root-of-Trust (RoT)-Hardware, zu unterstützen. Ziel der Partnerschaft ist, Sicherheitschip-Hardware transparenter, vertrauenswürdiger und sicherer für jeden zu machen.

OpenTitan wird sicherstellen, dass eine Root-of-Trust in Hardware transparent implementiert wird und somit zum Fundament für eine Vielzahl von Geräten wie Server-Motherboards, Netzwerkkarten, Router und IoT-Endgeräten wird. Anwender des Referenzdesigns können das Design, die Firmware und die Dokumentation von OpenTitan auf Register-Transfer-Level (RTL) einsehen und mitgestalten. Durch das neue Framework können Chiphersteller und Plattform-Anbieter, qualitativ hochwertige, transparent zu implementierende RoT-Chips entwickeln und sie auf die Anforderungen von Servern und anderen Geräten anpassen.

Als führender Anbieter von sicheren Embedded-Software-Lösungen teilt G+D Mobile Security die Vision des OpenTitan-Projektes, dass Hardware-Sicherheit offen und transparent sein sollte. Die Hauptmotivation für G+D Mobile Security, dieses richtungsweisende Projekt zu unterstützen, liegt in der Möglichkeit, die eigene langjährige Erfahrung und Kompetenz in der Entwicklung und Zertifizierung von Embedded-Software-Lösungen sowie die Erfahrung in Open-Source-Projekten einzubringen. Für das sich schnell entwickelnde IoT-Ökosystem erwartet das Unternehmen zudem große Vorteile durch eine offene und transparente Root-of-Trust-Hardware.

Die Vorteile von OpenTitan für Chiphersteller und Plattformanbieter sind:

→ **Transparenz:** Anwender können das Design, die Firmware und die Dokumentation von OpenTitan einsehen, mitgestalten und so dazu beitragen, bei der Entwicklung von transparenteren und vertrauenswürdigen RoT-Chips für alle mitzuwirken.

- **Hohe Qualität:** OpenTitan hat das Ziel, ein hochwertiges und hochsicheres RTL-Design, Firmware und Dokumentation aufzubauen und zu pflegen. Die erfahrenen Ingenieure, die für das Projekt arbeiten, legen höchsten Wert auf die gründliche Validierung des Designs und die technische Dokumentation, basierend auf den Erfahrungen mit den Titan-Chips von Google.
- **Flexibilität:** Durch die Verwendung einer plattformunabhängigen RoT-Hardware können die Anwender ihren adressierbaren Markt vergrößern und Kosten reduzieren, da das gleiche Design in Rechenzentrumsservern, Peripheriegeräten und vielen anderen Hardwarekomponenten eingesetzt werden kann.

„Es ist für G+D Mobile Security ein Privileg, ein Teil dieses wegweisenden Projekts zu sein“, sagt Carsten Ahrens, CEO von G+D Mobile Security. „Wir sind fest entschlossen, OpenTitan zur ersten zertifizierten Open-Source-RoT-Hardwareplattform zu machen, die die Anforderungen aller Anwendungsfälle für Cloud- und IoT-Sicherheit erfüllt.“

„Unsere Mission bei lowRISC ist, ein dynamisches Ökosystem rund um offene Silizium-Designs aufzubauen und die Eintrittsbarrieren für die Produktion kundenspezifischer Chips zu senken“, erklärt Gavin Ferris, Board Member von lowRISC CIC. „Dabei hilft die gemeinsame Initiative gleichgesinnter Firmen, die Transparenz rund um die Chips zu verbessern und dadurch das Vertrauen in die Gesamtsicherheit der Infrastruktur, auf der Software läuft, zu stärken. Mit OpenTitan werden Unternehmen und Verbraucher gleichermaßen von Serviceangeboten profitieren, die auf einer noch sichereren Infrastruktur ausgeführt werden können, da diese auf den transparent implementierten OpenTitan-Chips basiert.“

„Von den Kunden wird erwartet, sich auf proprietäre RoT-Hardware-Chips für ihre geschäftskritischen Systeme zu verlassen, ohne die Möglichkeit zu haben, diese zu verstehen, zu untersuchen und ihnen auf dieser Basis zu vertrauen“, erläutert Dominic Rizzo, Projektleiter OpenTitan Engineering bei Google Cloud. „Durch die Entwicklung von OpenTitan in einer gemeinsamen Initiative von Hardware-, Sicherheits- und akademischen Experten können wir den Erfahrungsschatz und die Sicherheitsprinzipien von Googles eigenen Titan-Chips einbringen, um die Hardware-RoT-Designs transparenter, kontrollierbarer und zugänglich für den Rest der Industrie zu machen. Sicherheit sollte niemals auf Undurchsichtigkeit aufgebaut sein.“

OpenTitan wird geleitet von lowRISC, einem unabhängigen, gemeinnützigen Ingenieurunternehmen, das kollaborative Entwicklungsansätze verwendet, um Chipdesigns und die notwendigen Tools langfristig in Open Source zu entwickeln und zu pflegen.

Über G+D Mobile Security

G+D Mobile Security ist ein weltweit tätiger Konzern für mobile Sicherheitstechnologien mit Hauptsitz in München. Das Unternehmen ist Teil der Giesecke+Devrient-Gruppe. G+D Mobile Security hat weltweit ca. 5.300 Mitarbeiter und erwirtschaftete im Geschäftsjahr 2018 einen Umsatz von rund 868 Millionen Euro. Für internationale Kundennähe sorgen mehr als 40 Vertriebsbüros sowie über 20 zertifizierte Produktions- und Personalisierungsstandorte weltweit.

G+D Mobile Security verwaltet und sichert Milliarden von digitalen Identitäten über deren gesamten Lebenszyklus. Unsere Produkte und Lösungen werden von Banken, Netzbetreibern, Herstellern von Mobilgeräten und Automobilen, Krankenkassen, Unternehmen der Privatwirtschaft und des Öffentlichen Nahverkehrs sowie von deren Kunden täglich genutzt, um das mobile Bezahlen, die Kommunikation und die Interaktion zwischen Geräten abzusichern. G+D Mobile Security hält in diesen Märkten eine führende Wettbewerbs- und Technologieposition.