

Sicherheitslösungen mit integrierten Krypto-Modulen für Embedded Geräte

Research & Development

Der Sicherheit von Embedded Geräten wird häufig weniger Beachtung beigemessen als jener von PCs. PCs sind in der Regel von der Umwelt durch Firewalls und Antivirensoftware gut abgeschottet und geschützt. Wie sieht es mit Embedded Geräten aus? Embedded Geräte wännen sich durch das Vorhandensein proprietärer Software und nicht-öffentlicher Kommunikationsnetze oft in einer vermeintlichen Sicherheit.

Typische Gefahren für Embedded Geräte zeigen sich in den folgenden Bereichen:

- Über das Internet auf die Hardware geladene fremde Software belastet die Funktionstüchtigkeit des Gerätes
- Ungeschützter Fernzugriff ermöglicht Hackern, das Ausführen von Schaltbefehlen sowie das Verfälschen von Messdaten
- Software-Updates sowie Patch-Management von nicht autorisierten Stellen
- Sicherheitsfunktionen in der Software werden umgangen oder imitiert

Embedded Geräte befinden sich häufig in sicherheitskritischen Infrastrukturnetzwerken für Strom, Wasser, Gas, Strasse und Schiene sowie in Produktionsanlagen. Die Geräte werden vermehrt mit anderen Netzwerken (Office-Netz, Internet) verbunden. Für einen sicheren und reibungslosen Betrieb sind deshalb Vorkehrungen zu treffen, um die hohe Zuverlässigkeit, Verfügbarkeit und Integrität der Geräte auch unter diesen Umständen zu gewährleisten.

Echte Sicherheit kann nur mit Hardware realisiert werden. Atmel bietet eine Reihe von kryptographischen Microcontrollern an, die für Embedded Geräte und Smartcard-Lösungen verwendet werden können. Albis Technologies hat zusammen mit Atmel Lösungen realisiert, die vor den erwähnten Gefahren schützen, indem das dafür notwendige kryptographische Schlüsselmaterial sicher vor Zugriffen und Veränderungen in einem kryptographischen Microcontroller auf dem Embedded Gerät gespeichert wird.

Typische Anwendungsbeispiele sind:

- Sicherer Firmware-/Software-Update: Nur signierte Software kann ins Gerät geladen werden
- Trusted Boot: Nur signierte Software-Komponenten werden gestartet
- Sicherer Fernzugriff für Wartung, z.B. via SSL
- Kopierschutz durch geräte-individuelle Lizenzfiles, Software-Dongles
- Realisierung von Public-Key-Infrastrukturen (PKI) für Embedded Geräte.

Planen oder realisieren Sie Sicherheitslösungen für Embedded Geräte? Ist für Sie die hohe Verfügbarkeit Ihrer Geräte trotz der notwendigen Software-Updates von grosser Bedeutung? Sind Sie an Sicherheit interessiert, die im Embedded Gerät selber integriert wird?

Albis Technologies kann Sie entlang des gesamten Entwicklungsprozesses unterstützen: Von der Risikoanalyse, der Erstellung des Sicherheitskonzeptes, der Technologieauswahl, über die Definition der System-Architektur bis hin zur Implementierung, dem Systemtest, der Produktion sowie auch bei der Wartung des Systems.

Auf der Rückseite finden Sie zwei Projektbeispiele zu Embedded Geräten und Smartcards, welche die Kompetenzen unserer Spezialisten in der Entwicklung von Sicherheitslösungen zeigen.

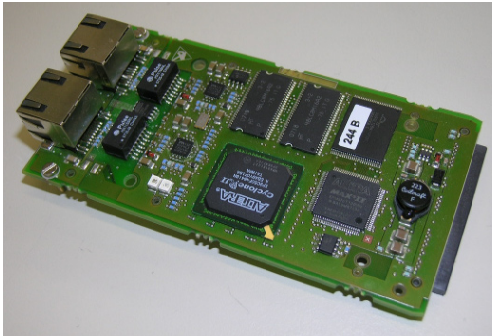
Weitere Informationen

Für weitere Informationen kontaktieren Sie:
Telefon +41 58 252 47 77

development@albistechnologies.com

Sicherer Software-Update und Kopierschutz für Embedded Gerät von Siemens AG

In diesem Projekt wurde der Kopierschutz sowie ein sicherer Software-Update für eine Gerätefamilie entwickelt, welche in schützenswerten Infrastrukturen (Wasser, Gas, Strom) zum Einsatz kommt. Eingesetzt wurde der kryptographische Microcontroller AT98SC.



Es wurden folgende Arbeiten realisiert:

- Erarbeitung des Sicherheitskonzeptes zusammen mit dem Kunden
- Hostseitige Entwicklung der benötigten Treiber und Interfaces für die projektspezifische Krypto-Library
- Entwurf und Realisierung des geschützten File-Systems
- Einbindung des kryptographischen Microcontrollers in das Real-time Betriebssystem und den Boot-Prozess
- Entwicklung einer kundenspezifischen Krypto-Library und der dazugehörigen Schnittstelle für die Applikations-Software
- Spezifikation, Projektierung und Realisation eines Trust-Centers für die Erzeugung des Schlüsselmaterials und die Integration des Initialisierungsvorgangs in den Fertigungsablauf des Kunden

Diese Projektbeispiele zeigen die Kompetenzen unserer Spezialisten in der Realisierung von Sicherheitslösungen. Gemeinsam mit unserem Partner Atmel freuen wir uns, dieses Know-how auch Ihnen zur Verfügung zu stellen.

In den beiden Projektbeispielen haben wir folgendes Technologie-Know-how verwendet:

- System-Architektur gemäss Guidelines der Trusted Computing Group
www.trustedcomputing.org
- Secure Coding (zertifiziert durch Siemens CERT)
- Testen gemäss OSSTMM
- Asymmetrische Verschlüsselungstechnologien:
PKI mit RSA 1024/2048 bit; OAEP; EMSA-PSS; ECC
- Symmetrische Verschlüsselungstechnologien:
3DES

Sicherheitslösung für ein elektronisches Türsystem mit LEGIC Smart Cards

In diesem Projekt wurde das Konzept sowohl für die Smartcard als auch für das Hostsystem für ein elektronisches Türsystem realisiert. Zum Einsatz kam der kryptographische Microcontroller AT90SC für embedded Systeme und Smartcards.



Es wurden folgende Arbeiten realisiert:

- Erarbeitung des Sicherheitskonzeptes in enger Zusammenarbeit mit dem Kunden
- Entwicklung einer projektspezifischen Firmware für den kryptographischen Microcontroller
- Definition der Krypto-Library mit Anbindung an den Hardware-Beschleuniger
- Realisierung einer Speicherverwaltung für sichere Daten mit einem kundenspezifischen Filesystem auf der Smartcard
- Implementation von Treibern und Interfaces auf Hostrechner und kryptographischem Microcontroller