Vertrauenswürdige Kanäle und Vertrauensanker in Verteilten Eingebetteten Systemen

Steffen Schulz

April 14, 2014

Eingebette Systeme werden zunehmend zur Automatisierung sicherheitskritischer Infrastrukturen eingesetzt. Typische Beispiele sind die Steuerung von Industrieanlagen, Heimautomatisierung, aber auch medizinische Implantate und Bordelektronik moderner Autos. Mit zunehmender Interdependenz, Kritikalität und Komplexität sind eingebetteten Systeme aber auch zunehmend attraktive und wertvolle Ziele für Angreifer.

In diesem Zusammenhang kann die Fähigkeit, den Sicherheitszustand von Geräten automatisch über das Netzwerk zu verifizieren und Datenverfügbarkeit an bestimmte, vertraute Systemzustände zu binden, fundamental zur Sicherheit von aus vielen Geräten zusammengesetzten Infrastrukturen beitragen. Existierende Ansätze in diesem Bereich zielen jedoch vor allem auf leistungsstarke Plattformen wie PCs und Server ab, und sind nicht ohne Weiteres auf Geräte übertragbar, die zu sehr geringen Kosten produziert werden und oft starken Ressourcenbeschränkungen unterliegen.

In dieser Dissertation untersuchen wir daher Lösungen für Trusted Computing-Funktionalitäten in verteilten eingebetteten Systemen. Speziell untersuchen wir effiziente Mechanismen zur Etablierung von Vertrauen und vertrauenswürdigen Kommunikationskanälen für Systeme mit geringer Rechen- und Speicherkapazität, bei denen sich traditionelle Sicherheitshardware aus Kostengründen und aufgrund des erhöhten Energieverbrauchs verbietet.

Als ersten Beitrag untersuchen wir die Erweiterung von Sicheren Kanälen. Hierzu erweitern wir das etablierte IPsec Schlüsselaustauschprotokoll (Internet Key Exchange, IKE) zur Übertragung von Zustandsreports und entwickeln eine prototypische virtualisierte IT-Infrastruktur, die ihre Sicherheitszonen in vertrauenswürdigen virtuellen Netzen voneinander isoliert.

Als nächstes untersuchen wir verdeckte Kanäle in IPsec-basierten VPNs und entwickeln ein IPsec Protokoll welches unerwünschte Informationsflüsse aus dem VPN heraus eliminiert. Wir zeigen weiterhin, dass auch stärkere eingebettete Systeme wie ein Mobiltelefon in der Lage sind, unerwünschte Übertragungsmuster zu verschleiern oder zu entfernen, und dass eine gezielte Verschleierung auch effizienter sein kann als ein generischer VPN-Ansatz.

Im zweiten Teil der Arbeit befassen wir uns zunächst mit einer Analyse von Software-basierter Attestierung, einem aktuellen Ansatz zur Erzeugung von Zustandsbeweisen der keinerlei vertrauenswürdiger Hardware bedarf. Dabei unternehmen wir einen ersten Schritt zur Formalisierung fundamentaler Anforderungen von Software-basierter Attestierung, präsentieren eine systematische Instantiierung und identifizieren mehrere offene Probleme. Darauffolgend präsentieren wir eine Erweiterung von Software-basierte Attestierung mit Physikalisch Unklonbaren Funktionen (PUFs). Der daraus resultierende Vertrauensanker ist nicht nur kostengünstig herstellbar ist sondern bietet auch einen gewissen Schutz gegen Hardwareangriffe.

Im nächsten Schritt untersuchen das Potential von Vertrauenswürdigen Ausführungsumgebungen mit Hilfe einer selbst entwickelten virtuellen Smartcard. Unser neuartiges Sicherheitstoken bindet sich nahtlos in existierende Anwendungen ein und bietet vereinfachte Verwaltung und Migration gegenüber echten Smartcards. Aufbauend auf diesen Erfahrungen entwickeln wir TrustLite, eine neuartige Architektur für Trusted Computing und Vertrauenswürdige Ausführungsumgebungen in stark Ressourcen- und kostenbeschränkten Geräten. TrustLite verallgemeinert traditionelle Speicherschutzmechanismen und ermöglicht so neue Formen von Softwareisolation und Attestierung zu geringen Kosten.

Zusammenfassend bieten die in dieser Arbeit vorgestellten und analysierten Konzepte neue Einsichten und Ansätze zur Konstruktion und Interaktion sicherer eingebetteter Systeme, und liefert so einen fundamentalen Beitrag zur Absicherung zukünftiger IT-Infrastrukturen.