Secure Cloud-based Smart Building and Infrastructure Technology

Motivation

Das „Internet der Dinge“ gilt als ein integraler Teil des zukünftigen Internets und kann definiert werden als eine Art dynamische, globale Netzwerkinfrastruktur. Diese besteht aus eingebetteten Systemen mit selbstkonfigurierbaren Eigenschaften, basierend auf standardisierten und untereinander vollständig kompatiblen Kommunikationsprotokollen. Materielle und virtuelle „ Dinge“ besitzen Identitäten, physikalische Attribute, sowie virtuelle Persönlichkeiten und nutzen ausgeklügelte und nahtlos in das Informationsnetz eingebundene Schnittstellen. Dabei wird angenommen, dass die „Dinge“ zu aktiven Teilnehmern der Informationsverarbeitung in Geschäftsbetrieben werden und damit eine automatisierte Kommunikation durch den Austausch von Daten und gewonnenen Umgebungsinformationen ermöglichen. Durch die automatisierte Reaktion zu Geschehnissen der realen Welt beeinflussen sie laufende Prozesse, welche Aktionen auslösen oder Dienste, unabhängig vom menschlichen Eingriff, bereitstellen können. Spezielle Schnittstellen ermöglichen die Interaktion mit diesen „intelligenten Dingen“ über das Internet durch das Abfragen und die aktive Beeinflussung ihres Zustands bzw. jeglicher assoziierten Informationen unter Beachtung von Problemstellungen aus Sicherheit (intern und extern) und Datenschutz.

Bedingt durch die Tatsache, dass die Anzahl eingebetteter Systeme einen rapiden Anstieg zu verzeichnen hat und die betreffenden Geräte üblicherweise rund um die Uhr im Betrieb sind, entsteht die Notwendigkeit, die einzelnen Knoten so minimal wie möglich zu halten, um dieses Konzept auch in Zukunft weiterhin nutzen zu können.

Im Hinblick auf Security müssen insbesondere auch sehr ressourcenarme Geräte mit Speicher von maximal ein bis zwei Megabytes und einer sehr geringen Energieaufnahme sicher in das globale Netzwerk eingebracht werden können. Bekannte Sicherheitsmechanismen der IT können jedoch aufgrund der sehr eingeschränkten Ressourcen nicht ohne weiteres adaptiert werden. Neuartige und ausgeklügelte Mechanismen (Stichwort: „Security by Design“) müssen eingesetzt werden, um eine effiziente Lösung für Systeme mit minimalistischen Ressourcen zu ermöglichen. Dem kommt speziell im Bereich „Smart Building / Smart Grid“ eine sehr große Bedeutung zu, da Investitionen im Bereich Smart Grid nur dann als sinnvoll erachtet werden können, wenn kosteneffiziente, ressourcenarme und im Energieverbrauch steuerbare Smart Building Technology-Komponenten zum Einsatz kommen können.

Vorgehen

Bedingt durch die steigende Komplexität im Anwendungsbereich Gebäudeautomation entstehen immer höhere Anforderungen an Verfügbarkeit, Integrität der Steuergeräte an sich, als auch der ablaufenden Kommunikation und der Vertraulichkeit. Im geplanten Projekt sollen gezielt Applikationen von eingebetteten Systemen mit minimalistischen Ressourcen untersucht werden. Bis vor einigen Jahren waren solche Systeme weitestgehend isoliert, wodurch der Fokus vor allem auf der funktionalen Sicherheit lag. Im Gegensatz dazu werden solche Geräte mit der Etablierung des Internets der Dinge immer stärker vernetzt. Diese Vernetzung ist beispielsweise für das Auslesen von Messwerten oder das Übertragen von Steuerinformationen erforderlich. Dadurch ergibt sich, im Vergleich zu ehemaligen Insellösungen, ein wesentlich größeres Feld an potentiellen Angriffszielen. Für Geräte mit minimalistischen Ressourcen gibt es zudem noch keine ausgereiften und probaten Sicherheitsmechanismen, die diese Schutzziele umfassend gewährleisten könnten. Bekannte ressourcenlastige Sicherheitslösungen, wie SSL/TLS lassen sich aufgrund ihres Implementierungsumfangs nicht ohne weiteres adaptieren. Die sich aus diesen aufgeführten Gründen ergebenden Möglichkeiten zur Sabotage und Spionage führen die Brisanz der Lage vor Augen und verdeutlichen den akuten Handlungsbedarf dieses speziellen Anwendungsbereiches.

Innerhalb dieses Projekts sollen vor allem für die Projektpartner, die die jeweiligen Anforderungen ihres Bereiches definieren, folgende übergeordnete Ziele erreicht werden:

- Verbesserung der IT-Sicherheit von Gebäudeautomationssystemen ohne negative Auswirkungen auf Verfügbarkeit und Betriebssicherheit
- Kosteneffizienz durch systemische Lösungen

- Ressourceneffizienz durch niedrigeren Materialaufwand/Leistungsverbrauch
- Einsatz von bewährten Standardtechnologien und teils adaptierten Sicherheitstechnologien
- Ausfallsicherheit durch kooperative Systeme
- Interoperabilität und hoher Grad an Benutzerfreundlichkeit
- Transparente Einbindung der Programmier- und Wartungssoftware für die Kleinsteuerungen in der Cloud
- Gewährleistung des Datenschutzes

Die Arbeitsziele, die innerhalb dieses Projekts von den verschiedenen Teilnehmern bearbeitet werden, ergeben sich somit basierend auf den übergeordneten Zielen:

- Initiales Setup der Geräte so einfach und dennoch so vertrauenswürdig wie möglich
- Sichere Kommunikation zwischen Cloud Servern und individuellen Knoten
- Sichere Kommunikation zwischen lokalen Knoten
- Eindeutige Identifikation der Teilnehmer untereinander
- Sicherstellung der Integrität von Systemen und der Kommunikation
- Erkennung von Manipulation an Software und der Kommunikation
- Möglichkeit der Wartung/Softwareupdate und Konfiguration

Finale Ziele dieses Vorhabens sind das Eindämmen von möglichen Angriffen, die Gewährleistung des Betriebes im Angriffsfall sowie die Limitierung der Reichweite bzw. der schädigenden Wirkung des Angreifers.

Eckdaten

Kurztitel

Sec-BIT

Forschungsschwerpunkt

Digitale Wirtschaft und Gesellschaft - Digital Economy and Society

Laufzeit

01.04.2015 - 31.03.2018

Fördergeber

Bayerisches Staatsministerium für Wirtschaft und Medien, Energie und Technologie

Projektleitung

Prof. Dr.-Ing. Andreas Grzemba

Ziele

Ziele des Projektes „Secure Cloud-based Smart Building and Infrastructure Technology“ sind das Eindämmen von möglichen Angriffen, die Gewährleistung des Betriebes im Angriffsfall sowie die Limitierung der Reichweite bzw. der schädigenden Wirkung des Angreifers bei ressourcenarmen Geräte mit geringer Speicherkapazität.