Universität Rostock

Traditio et Innovatio

Modellbasierte, sichere Service- und Netzwerkkonfiguration in der Gebäudeautomation

Der Fakultät für Elektrotechnik und Informatik
der Universität Rostock zur Erlangung des
akademischen Grades eines

Dr.-Ing.

vorgelegte Dissertation von
Arne Wall
Matrikel-Nr.: 209 204 209

Rostock, 24. April 2023

Dissertation
Fakultät für Informatik und Elektrotechnik

Arne Wall
Institut für Angewandte Mikroelektronik und Datentechnik

Zusammenfassung

Die moderne Maschine-zu-Maschine-Kommunikation (M2M) wird zunehmend durch offene Standards und Webtechnologien geprägt. Dadurch ist es möglich, Geräte verschiedener Hersteller miteinander IP-basiert zu vernetzen und an das Internet anzubinden. Dabei verschmelzen das Web und die lokalen Netzwerke der Gebäudeautomation (GA).

Dieselben Angriffstechniken auf Server und Clients lassen sich auf eingebettete Systeme übertragen. Während Webserver und Endgeräte durch regelmäßige Sicherheitsupdates gegen Angriffe gehärtet werden, bleiben eingebettete Systeme oftmals auf der Strecke. Falls ein Endgerät kompromittiert sein sollte, um weitergehende Angriffe innerhalb eines Netzwerks auszuführen, lassen sich die Folgen durch eine Abschottung der Geräte voneinander drastisch reduzieren. So kommunizieren z.B. in Unternehmensnetzwerken die einzelnen Teilnehmer gemäß einer firmeninternen Sicherheitsrichtlinie miteinander.

Solche Mechanismen zur Absicherung der Gerätekommunikation existieren auf Systemebene einer GA bislang nicht. Daher wurde in dieser Arbeit eine Sicherheitsarchitektur entwickelt, die speziell an die Anforderungen einer modernen M2M-Kommunikation in einem GA-System zugeschnitten ist. Es wird ein Konzept vorgestellt, wie die einzelnen Endgeräte einer GA über ein sicheres Verfahren mit Zugangs- und Konfigurationsdaten versorgt werden und über abgeschottete Domänen miteinander kommunizieren. Dabei wird die Implementierung der Endgeräte zur Designzeit beschrieben. Des Weiteren wird ein Protokollstack vorgeschlagen und experimentell untersucht, um verschiedene Anwendungsanforderungen innerhalb der GA zu erfüllen. Sämtliche Implementierungsvorschläge für Gerätehersteller werden auf Basis von offenen Standards und Protokollen gemacht. Offene Standards sind essentiell, damit eine herstellerübergreifende Gerätekommunikation gelingen kann. Angewandte Security-Verfahren und Protokolle, die offengelegt sind, bieten den besten Schutz gegenüber Angriffen, da ihre Sicherheitseigenschaften stetig durch die Forschungsgemeinschaft untersucht werden. Der gesamte Lebenszyklus eines Gerätes, von seiner Entwicklung bis hin zur Demontage, wird durch offene Gebäudeinformationsmodelle begleitet. Ein Digital-Twin, der die gesamte GA von der Kommissionierung bis hin zu Umbaumaßnahmen modelliert, dient als Grundlage für eine automatisierte Berechnung von Konfigurationsdaten. Es gilt, den Einfluss-

faktor ”Mensch” als potentielle Security-Schwachstelle durch automatisierte Abläufe zu unterstützen, jedoch zu jeder Zeit einen manuellen Eingriff zuzulassen.

Abstract

Modern machine-to-machine communication is increasingly characterized by open standards and web technologies. This makes it possible to network devices from different manufacturers with each other on an IP basis and to connect them to the Internet. In the process, the web and local networks as used in building automation (BA) are merging. The same attack techniques on servers and clients can be applied to embedded systems. While web servers and endpoints running client applications are hardened against attacks through regular security updates, embedded systems often are not provided with urgent software fixes. If an end device is compromised to carry out more extensive attacks within a network, the consequences can be drastically reduced by separation of the devices from one another. In corporate networks, for example, the participants communicate with each other in accordance with a company-internal security guideline. Such mechanisms for securing device communication do not yet exist at the system level of a BA. Therefore, a security architecture has been developed that is specifically tailored to the requirements of modern machine-to-machine communication in a BA system. A concept is presented how each individual end device of a BA is supplied with access and configuration data via a secure procedure and communicates with other EDs within partitioned domains. The implementation of the end devices at design time is described. Furthermore, implementation proposals based on open standards and protocols are made for device manufacturers. Open standards are essential for cross-vendor device communication to succeed. Applied security procedures and protocols, that are open, offer the best protection against attacks, as their security properties are constantly being investigated by the research community. The entire life cycle of a device up to disassembly is accompanied by building information modeling. A digital twin, which models the entire BA from commissioning phase until building conversions, serves as the basis for an automated calculation of configuration data. The aim is to support the human factor as a potential security vulnerability through automated processes, but to allow manual intervention at any time.