Wir sind heller

WSH ZigBee PRO Building

Sicherheitsstandard für Lichtsteuerungen im Industriebereich Rev. 0.1

Folgende Informationen beschreiben den genutzten Sicherheitsstandard, welcher grundlegend von der ZigBee Alliance definiert wurde und im WSH ZigBee PRO Building Steuerungssystem genutzt wird.

Die WSH PRO Building Zigbee Lösung baut auf dem Zigbee-PRO-Mesh-Netzwerkprotokoll der ZigBee Allianz auf. Es verfügt – anders als die herkömmlichen ZigBee Home Automation Lösungen – über wichtige Sicherheitsfunktionen für den angriffssicheren und stabilen Einsatz im industriellen Bereich.

Besonders zu erwähnen sind hier:

- Geräte benötigen eine eindeutige Authentifizierung beim Beitritt in das Netzwerk
- Laufzeitschlüssel Updates während des Betriebs
- Sicherung der OTA-Firmware Updates
- Logische linkbasierte Verschlüsselung

Sicherheitsmodell

Für höhere Sicherheit verfügen die zentralen Systeme über ein Trust Center (TC), welches typischerweise auch der Netzwerk Koordinator ist. Der TC bildet ein zentralisiertes, in sich abgeschlossenes Netzwerk und ermöglicht es Routern und Endgeräten nur sich dem Netzwerk anzuschließen, wenn diese über ordnungsgemäße Anmeldeinformationen verfügen. In diesem geschlossenen, zentralisierten Netzwerk kann nur der TC Verschlüsselungsschlüssel ausgeben. Das TC stellt einen eindeutigen TC Link Key für jedes Gerät im Netzwerk zur Verfügung, sobald sich diese dem Netzwerk anschließen.

Schicht Sicherheit

Die Schicht Sicherheit nutzt einen überlagerten Ansatz, beginnend mit physischer Sicherheit, welcher sich bis hin zur Anwendungsschicht fortsetzt. Aus einer Protokoll- / Standardperspektive bieten sowohl die Netzwerk- als auch die Anwendungsschichten Sicherheitsfunktionen (zusätzlich zu den Prozeduren, die mit dem Beitritt zu einem Netzwerk verbunden sind). Auf Netzwerkebene befinden sich alle Geräte im geschlossenen Netzwerk unter der gleichen Sicherheitsumgebung.

Installations-Codes

Der TC verlangt, dass jedes neue Gerät einen eindeutigen Installationscode verwendet, um dem zentralisierten Sicherheitsnetzwerk beizutreten. Der Installationscode muss mit einem Code übereinstimmen, der zuvor in den TC ohne Funkverbindung implementiert wurde (d.h. nicht mit einer Zigbee-Nachricht). Der Installationscode ist als Nummer und Datamatrix-Code auf der Verpackung des Gerätes aufgedruckt. Der Benutzer oder Installateur kann den Code in den Projektdaten des Netzwerkmanagers eintragen oder einscannen. Dieser überträgt dann die Daten an das TC. Alle Zigbee-Geräte müssen einen eindeutigen Installationscode enthalten. Den Code bildet eine zufällige 128-Bit-Nummer, welche durch einen 16-Bit-CRC geschützt ist. Das beitretende Gerät und das TC ermitteln mit der Matyas-Meyer-Oseas (MMO) Hash-Funktion einen einzigartigen 128-Bit Trust Center Link Key aus dem Installationscode.

Rollende Schlüssel

In dem zentralisierten Sicherheitsnetz erschafft, verteilt und wechselt das Trust Center regelmäßig einen neuen Netzwerkschlüssel. Sollte also ein Angreifer einen Netzschlüssel erhalten, hat dieser nur eine begrenzte Lebensdauer, bevor er abläuft. Aktualisierte Schlüssel werden verschlüsselt mit dem TC-generierten TC Link Key verschickt.

Application-Layer-Verschlüsselung

Ein weiteres, wichtiges Sicherheits-Tool ist die Fähigkeit, eine in der Anwendungsebene gesicherte Verbindung zwischen einem Gerätepaar im Netzwerk zu erstellen. Dies wird durch die Einrichtung eines einzigartigen Satzes von AES-128 Verschlüsselungsschlüsseln zwischen einem Gerätepaar verwaltet. Dies ermöglicht logische, gesicherte Verbindungen zwischen zwei beliebigen Geräten im Netzwerk. Damit wird eine "virtuelle private Verbindung" zwischen diesen Geräten in einem Netzwerk mit vielen anderen ermöglicht.

OTA-Updates

Over-the-Air (OTA) Updates ermöglichen es, neue Funktionen zu den Geräten im Netzwerk hinzuzufügen, Fehler in einem Produkt zu beheben und Sicherheits-Patches anzuwenden. Normalerweise stellen OTA-Updates eine mögliche Sicherheitsanfälligkeit dar, wenn das Protokoll keine ausreichenden Schutzmaßnahmen bereitstellt oder nicht alle verfügbaren Schutzmaßnahmen verwendet werden. Zigbee-Geräte bieten hier mehrschichtige Sicherheit, um Geräte im Feld zu aktualisieren und sicherzustellen, dass aktualisierte Software Codes nicht böswillig geändert werden. Zuerst stellt der Zigbee-Standard eine Methode zur Verschlüsselung aller Dateiübertragungen über das Netzwerk mit einem einzigartigen Schlüssel zur Verfügung. Zweitens stellt der Standard eine Methode zur Unterzeichnung der OTA-Datei mit einem anderen eindeutigen Schlüssel zur Verfügung. Drittens kann die Datei während der Fertigung verschlüsselt werden, so dass nur das Endprodukt den Schlüssel enthält, um ihn zu entschlüsseln. Schließlich kann die Datei im On-Chip-Speicher gespeichert werden, in der die Debug-Read-Back-Funktion deaktiviert wurde. Dies verhindert die Nutzung von Reverse Engineering mit Debug-Tools. Sobald ein Gerät eine verschlüsselte Datei empfängt, entschlüsselt sein sicherer Bootloader die Datei, bestätigt die Signatur und aktualisiert dann erst das Gerät.

Zusätzliche Sicherheits-Techniken

Um Replay-Attacken zu stoppen, in denen ein Angreifer eine Befehlsnachricht aufnehmen und wiedergeben kann (zum Beispiel die Leuchten ein- oder ausschalten), enthält jeder Zigbee-Befehl einen Systemzähler. Das Empfangsgerät prüft den Systemzähler und ignoriert doppelte Meldungen. Zigbee unterstützt Frequenzbeweglichkeit. Das Netz kann auf einem anderen Kanal (Frequenz) verlagert werden, wenn der aktuelle Kanal beeinträchtigt wird, zum Beispiel durch einen Störungsangriff.

Zigbee Sicherheitsalgorithmen

Um Produktionsumgebungen und Industriebetriebe bestmöglich zu schützen greifen wir auf hochsichere Algorithmen zu. Unter anderem:

- 128-Bit-AES-CCM * für Nachrichtenverschlüsselung, Authentifizierung und Integrität (NIST FIPS Publikation 197)
- Hash Message Authentication Code (NIST FIPS Publikation 198)
- Matyas-Meyer-Oseas Hash-Funktion, um vorkonfiguriert Linkschlüssel aus Installationscodes abzuleiten (Handbuch der angewandten Kryptographie)

Schlussfolgerung

Das WSH ZigBee PRO Building Steuerungssystem nutzt vielschichtige Sicherheitslösungen und Technologien, um so die Sicherheitsanforderungen modernster Industriebetriebe zu erfüllen.