Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Sicherheit in der Heimautomatisierung

von

Bastian van Venrooy

Erstprüfer:	Prof. Dr. Karl Jonas
Zweitprüfer:	Prof. Dr. Lemke-Rust
Eingereicht am:	18. Februar 2016

Persönliche Erklärung

Erklärung

Hiermit erkläre ich an Eides Statt, dass ich die vorliegende Arbeit selbst angefertigt habe; die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher keiner Prüfungsbehörde vorgelegt und auch noch nicht veröffentlicht.

Bonn, (18. Februar 2016) _____

(Bastian van Venrooy)

Inhaltsverzeichnis

Tabellenverzeichnis IV

Abkürzungsverzeichnis V

1 Einleitung 1
- 1.1 Motivation . . . 1
- 1.2 Ziel der Arbeit . . . 2
- 1.3 Aufbau . . . 2

2 Grundlagen 3
- 2.1 Sicherheitsziele . . . 3
- 2.2 Angriffsszenarien . . . 4
- 2.3 Kryptographie . . . 4

3 ZigBee 7
- 3.1 Herstellerangaben laut Dokumentation . . . 7
- 3.2 Aufbau . . . 8
- 3.3 Gerät anlernen . . . 8
- 3.4 Protokoll . . . 9
- 3.5 Kommunikation mithören . . . 9
- 3.6 Sichere Kommunikation . . . 10
- 3.7 Schlüsselproblem . . . 11
- 3.8 Bekannte Sicherheitsprobleme bei ZigBee . . . 12
  - 3.8.1 Auslesen des Keys . . . 12
  - 3.8.2 Replay-Angriff . . . 12
  - 3.8.3 ZigBee Light Link Master Schlüssel . . . 13
  - 3.8.4 Kompatibilität . . . 13
- 3.9 Sicherheitsziele . . . 14
- 3.10 Ergebnis . . . 15

4 EnOcean 16
- 4.1 Herstellerangaben laut Dokumentation . . . 16
- 4.2 Enocean Kommunikation . . . 16
- 4.3 Sichere Kommunikation . . . 18
- 4.4 Sichere Kommunikation aktivieren . . . 20
- 4.5 Sicherheitsziele . . . 21
- 4.6 Ergebnis . . . 22

5 ZWave 23
- 5.1 Herstellerangaben laut Dokumentation . . . 23

5.2 Aufbau . . . 24
5.3 Protokoll . . . 25
5.4 Sichere Kommunikation . . . 26
5.5 Schlüssel Reset Problem . . . 28
5.6 Sicherheitsziele . . . 29
5.7 Ergebnis . . . 29

6 KNX 30
6.1 Aufbau . . . 30
6.2 Gerät anlernen . . . 31
6.3 Herstellerangaben laut Dokumentation . . . 31
6.4 Konfigurationsmodus . . . 32
6.5 Kommunikation mithören . . . 32
6.6 Befehle senden . . . 33
6.7 KNX Data Security . . . 34
6.8 Sicherheitsziele . . . 35
6.9 Ergebnis . . . 36

7 FS20 37
7.1 Herstellerangaben laut Dokumentation . . . 37
7.2 Aufbau . . . 38
7.3 Gerät anlernen . . . 38
7.4 Kommunikation mithören . . . 39
7.5 Befehle senden . . . 39
7.6 Adressschema und Protokoll . . . 40
7.7 Sicherheitsziele . . . 41
7.8 Ergebnis . . . 42

8 HomeMatic 43
8.1 Herstellerangaben laut Dokumentation . . . 43
8.2 Aufbau . . . 44
8.3 Gerät anlernen . . . 44
8.4 Protokoll . . . 45
8.5 Kommunikation mithören . . . 45
8.6 Befehle senden . . . 46
8.7 HomeMatic ID . . . 47
8.8 Gesicherte Kommunikation . . . 47
8.9 Gesicherte Befehle . . . 48
8.10 Problem mit dem Default-Sicherheitsschlüssel . . . 49
8.11 System-Sicherheitsschlüssel ersetzen . . . 50
8.12 Sicherheitsziele . . . 50
8.13 Ergebnis . . . 51

9 DECT **52**
9.1 Herstellerangaben laut Dokumentation 52
9.2 FRITZ Smart Home 52
9.3 Sicherheitsprobleme mit DECT 53
9.4 DECT Security 54
9.5 Sicherheitsziele 54
9.6 Ergebnis 55

10 Zusammenfassung **56**

11 Ergebnis **58**

Tabellenverzeichnis

1 ZigBee Komponenten 8
2 EnOcean Komponenten 17
3 Interpretation EnOcean Nachricht 17
4 Z-Wave Komponenten 24
5 KNX Komponenten 30
6 Interpretation KNX Nachricht 33
7 FS20 Komponenten 38
8 Interpretation FS20 Nachricht 39
9 Umrechnung FS20 Adresse [fhe] 40
10 HomeMatic Komponenten 44
11 Interpretation HomeMatic Nachricht 45
12 Interpretation HomeMatic Nutzdaten Statusmeldung Steckdose 45
13 Interpretation HomeMatic Befehl senden 46
14 DECT Komponenten 52
15 Zusammenfassung 57

ACK Acknowledgement
AES Advanced Encryption Standard
APCI Application Layer Protocol Control Information
BidCoS Bidirectional Communication Standard
CBC Cipher Block Chaining
CBC-MAC Cipher Block Chaining Message Authentication Code
CCM Counter with CBC-MAC
CFB Cipher Feedback
CMAC Cipher-based Message Authentication Code
CTR Counter
CUL CC1101 USB Lite
DSAA DECT Standard Authentication Algorithm
DSC DECT Standard Cipher
ECB Electronic Codebook
ETS Engineering Tool Software
FHEM Freundliche Hausautomatisierung und Energie-Messung

IV Initialisierungsvektor
L/NPCI Link/Network Protocol Control Information
MD5 Message-Digest Algorithm 5
MIC Message Integrity Code
OFB Output Feedback
PAN Personal Area Network
REST Representational State Transfer
RSSI Received Signal Strength Indication
RSSI Received Signal Strength Information
TPCI Layer Protocol Control Information
WPAN Wireless Personal Area Network
XOR Exclusive or

1 Einleitung

1.1 Motivation

Heimautomatisierung stellt den Oberbegriff für das sogenannte Smart Home, bei dem verschiedene Teile des Wohnbereiches durch steuerbare Aktoren und Sensoren ausgestattet sind, dar. Dies eröffnet eine Vielzahl an Einsatzmöglichkeiten. Beginnend bei der Steuerung der Rollladen, sobald die Sonne aufgeht [knxb], über die automatische Regelung der Raumtemperatur, sobald der Bewohner auf dem Weg nach Hause ist [sma16], bis zum automatischen Verriegeln der Haustür, sobald der Bewohner das Haus verlässt [rwe15]. Diese Komponenten können Daten über Anwesenheit und Verbrauch verarbeiten beziehungsweise können sie die Zugangskontrolle wie beispielsweise das Schloss der Haustür kontrollieren.
Heimautomatisierung soll das Leben der Bewohner bequemer und sorgenfreier gestalten. Mithilfe von Smartphones lässt sich unterwegs überprüfen, ob man die Heizung im Bad abgestellt hat und falls man dies vergessen hat, kann man dies bequem von unterwegs aus erledigen. Intelligente Steckdosen teilen mit, wie ihr aktueller Verbrauch ist. Diese Daten kann ein Besitzer von einem Smart Home benutzen, um aufzudecken, ob irgendwo ein Gerät mit besonders hohem Verbrauch ist. Die intelligente Haustür lässt sich über das Internet oder mit dem Smartphone steuern, so kann vor der Tür stehender Besuch schon eingelassen werden, auch wenn noch niemand zu Hause ist.
All diese Fähigkeiten des Smart Homes sind möglich, da die einzelnen Komponenten miteinander kommunizieren. Diese Kommunikation sollte geschützt sein. Unbefugte sollten nicht in der Lage sein, die Daten der Sensoren zu interpretieren beziehungsweise Aktoren zu steuern.

1.2 Ziel der Arbeit

Diese Bachelorarbeit befasst sich mit dem Thema Sicherheit in der Heimautomatisierung. Es gelangt zur Betrachtung, welche Angaben die Hersteller zum Thema Sicherheit in ihren Komponenten machen. Die einzelnen Kapitel über die verschiedenen Techniken der Heimautomatisierung beginnen mit einer Vorstellung der Firma, welche die Technik entwickelt hat. Danach wird beschrieben, welche Informationen über eingesetzte Sicherheitsmechanismen erhältlich sind. Es erfolgt ein Aufbau mit verschiedenen Komponenten der Technik und es wird untersucht, ob sich Sicherheitsmechanismen konfigurieren lassen. Die eingesetzten Sicherheitsmechanismen werden analysiert und beschrieben. Falls es zu den Sicherheitsmechanismen bekannte Schwächen gibt, werden diese ebenfalls beschrieben. Im Anschluss findet eine Zusammenfassung, ob die in den Grundlagen definierten Sicherheitsziele erfüllt werden. Die Kapitel enden mit einem Ergebnis, indem die Erkenntnisse zusammengefasst werden.

1.3 Aufbau

Diese Arbeit ist neben einer Einleitung, Grundlagen und einem Ergebnis in sieben Kapitel unterteilt. Zu Beginn werden die Grundlagen beschrieben, die verwendet werden können, um Systeme abzusichern beziehungsweise welche Sicherheitsziele dabei verfolgt werden. Für die zu betrachtenden Hersteller gibt es je ein Kapitel, in dem die Sicherheit der Heimautomatisierung zur Betrachtung gelangt. Am Ende der Arbeit werden die Resultate der Kapitel zusammengefasst.

2 Grundlagen

In diesem Kapitel werden Grundlagen erörtert, welche für das Verständnis dieser Arbeit erforderlich sind.

2.1 Sicherheitsziele

Sicherheit lässt sich anhand von sechs Parametern beschreiben.

Vertraulichkeit: Gelingt es einem Angreifer, Kommunikation abzuhören, muss diese in einer Art geschützt sein, dass der Angreifer daraus keine Informationen beziehen kann. Mit Kryptografie ist es möglich, zu kommunizieren und die Informationen der Kommunikation vor Unbefugten zu schützen.

Integrität: Jene Daten, die übertragen werden, müssen gegen Veränderung geschützt sein. Um zu überprüfen, ob eine Nachricht verändert wurde, ist es möglich, eine Prüfsumme der Nachricht mit zu übertragen. Nach dem Erhalt der Nachricht errechnet der Empfänger eine eigene Prüfsumme der Nachricht und überprüft, ob diese identisch zur mitgeschickten Prüfsumme ist. Eine identische Prüfsumme bestätigt, dass die Nachricht nicht verändert wurde.

Authentifizierung: Authentifizierung wird genutzt, um Vertrauenswürdigkeit eines Senders sicherzustellen. Der Sender hat ein Authentifizierungsmerkmal, um sich als dieser Sender zu identifizieren. Ein Merkmal kann ein Passwort sein, welches nur der Sender kennt.

Verfügbarkeit und Zugang: Informationen sind nur dort und dann zugänglich, wo und wann sie von Berechtigten gebraucht werden. Unberechtigte haben keinen Zugang und sind auch nicht in der Lage, die Verfügbarkeit zu stören.

[Sik03]

2.2 Angriffsszenarien

In diesem Abschnitt werden mögliche Angriffsszenarien in der Heimautomatisierung beschrieben.

Mithören: Komponenten der Heimautomatisierung, die per Funk kommunizieren, sind der Gefahr ausgesetzt, dass jeder in Reichweite des Senders die gesendeten Nachrichten empfangen kann. Als Gegenmaßnahme können gesendete Nachrichten mit kryptographischen Algorithmen verschlüsselt werden.

Unberechtigtes Senden: Ein Angreifer in Funkreichweite eines Heimnetzes kann versuchen, unberechtigt Nachrichten zu senden. Er kann selbst Nachrichten erstellen und diese senden beziehungsweise kann er versuchen, zuvor mitgehörte Nachrichten erneut abzuspielen. Wird etwa die Funkübertragung beim Öffnen eines Garagentores aufgezeichnet, könnte ein Angreifer versuchen, diese Funkübertragung erneut zu senden. Diese Art des Angriffes wird als Replay Angriff bezeichnet. Diese Art von Angriff lässt sich entdecken, indem in den Paketen Informationen enthalten sind, die lediglich für diesen Moment oder nur einmal gültig sind. Dies wird mithilfe von Rolling Codes oder auch Nonce Werten erreicht. Ein Rolling Code ist ein Zähler, den zwei Kommunikationspartner kennen. Nonce steht für `used only once`. Dies bezeichnet einen Wert, der nur ein einziges Mal Verwendung findet. Wird so eine nur einmal aktuell gültige Information mit in einer Nachricht verarbeitet, kann ein Empfänger erkennen, wenn sie zu einem späteren Zeitpunkt erneut gesendet wird. Der Angreifer kann auch versuchen, Werte einer mitgehörten Nachricht zu verändern und diese erneut senden. Um sich vor so einem Angriff zu schützen, gibt es Methoden, um die Integrität einer Nachricht zu überprüfen.

Physikalischer Zugriff: Erlangt ein Angreifer physikalischen Zugriff zu einer Komponente, kann er versuchen, sich Zugriff zum Speicher beziehungsweise zur Konfiguration des Gerätes zu verschaffen. Gelingt es ihm, das Gerät unter seine Kontrolle zu bekommen, wäre es beispielsweise möglich, unberechtigt Nachrichten an das Heimautomatisierungsnetzwerk zu senden.

2.3 Kryptographie

Kryptographie setzt sich aus den griechischen Wörter *kryptós* und *gráphein* zusammen, was übersetzt bedeutet *verborgen* und *schreiben* [Kan12, 3]. Es handelt sich um mathematische Verfahren zum Ver- und Entschlüsseln von Daten. Die moderne Kryptographie lässt sich in zwei Klassen unterteilen. Es gibt die symmetrische und asymmetrische

Verschlüsselung [Kan12, 9]. Bei der symmetrischen Verschlüsselung benötigen beide Kommunikationspartner den gleichen geheimen Schlüssel, um eine Nachricht zu verbeziehungsweise entschlüsseln. Bei der asymmetrischen Verschlüsselung existiert ein öffentlicher Schlüssel, mit dem die Daten ausschließlich verschlüsselt werden können. Zudem gibt es einen privaten Schlüssel, mit dem die Daten entschlüsselt werden können [Kan12, 17]
Die symmetrische Verschlüsselung unterteilt sich in Strom- und Blockverschlüsselungen. Bei der Blockverschlüsselung werden die Daten einer Nachricht in Blöcke mit einer bestimmten Länge zerlegt. Bei der Stromverschlüsselung gelangen die Daten Bit für Bit zur Verarbeitung [Kan12, 10]. Es gibt verschiedene Algorithmen der symmetrischen Verschlüsselung, der am meisten verbreitete ist Advanced Encryption Standard (AES). Wird bei einer Blockverschlüsselung derselbe Klartext mit dem gleichen geheimen Schlüssel verschlüsselt, entsteht der identisch verschlüsselte Text. Dies könnte es einem Angreifer ermöglichen, Rückschlüsse aus dem verschlüsselten Text zu ziehen, ohne dass dieser den Text entschlüsselt [Kan12, 15]. Es gibt bei AES verschiedene Methoden, wie der Algorithmus verwendet wird, um diese Schwäche zu umgehen beziehungsweise den Algorithmus für verschiedene Zwecke, wie etwa Integritätssicherung, zu verwenden.

Electronic Codebook: Der Electronic Codebook (ECB) Modus ist der einfachste und effizienteste, allerdings auch der unsicherste Modus [Kan12, 15]. In diesem Modus wird dem AES Algorithmus ein Block mit fester Länger zum Ver- bzw. Entschlüsseln übergeben.

Cipher Block Chaining: Damit bei Cipher Block Chaining (CBC) der verschlüsselte Text auch beim zweiten Verschlüsseln mit dem identischen geheimen Schlüssel unterschiedlich ist, gibt es einen Initialisierungsvektor (IV). Der IV muss nicht geheim sein, es sollte allerdings für jede Übertragung ein anderer zufällig gewählter IV eingesetzt werden [Kan12, 15]. Zudem wird bei CBC der zweite und jeder nachfolgende Block beim Verschlüsseln mit dem verschlüsselten Text des vorherigen Blocks mit Exclusive or (XOR) verknüpft.

CBC-Message Authentication Code: Dieser Modus findet zum Signieren von Daten Verwendung. Beim Cipher Block Chaining Message Authentication Code (CBC-MAC) wird der CBC Modus angewendet, jedoch wird nur der letzte Block nach der Verschlüsselung zurückgegeben [cbc13].

Counter: In diesem Modus werden ein Nonce und ein Zähler mit dem geheimen Schlüssel verschlüsselt. Die verschlüsselte Zeichenkette wird mit dem zu verschlüsselnden Text mit XOR verknüpft [Kak16, 26].

Counter with CBC-MAC: Der Modus Counter with CBC-MAC (CCM) Mode stellt eine Mischung aus Counter (CTR) und CBC-MAC Mode dar. Er gelangt zum Einsatz, um Daten zu verschlüsseln sowie ihre Integrität sicherzustellen. [ccm02]

Cipher Feedback: Der Modus Cipher Feedback (CFB) ermöglicht es, AES als Stromchiffre zu verwenden. Bei CFB kann die Verschlüsselung auch beginnen, wenn der Datenblock kleiner als die eigentliche Blockgröße ist [Kan12, 16]. Wie bei CBC wird der verschlüsselte Block zur Verschlüsselung des zweiten und folgendes Blocks verwendet.

Output Feedback Der Output Feedback (OFB) Modus arbeitet ähnlich wie der CFB. Es handelt sich um eine Stromchiffre. Der Unterschied zwischen CFB zu OFB besteht darin, welcher Block beim Verschlüsseln zum XOR Verschlüsseln des nächsten Blocks verwendet wird [Kan12, 16].

3 ZigBee

Die erste Version der ZigBee Spezifizierung stammte aus dem Jahr 2004 und trägt den Namen ZigBee. Später wurde sie als ZigBee 2004 bezeichnet. Diese Version ist veraltet und wird von neuen ZigBee Geräten nicht mehr unterstützt. Die zweite Version der ZigBee Spezifizierung stammte aus dem Jahr 2006 und wurde ebenfalls mit ZigBee bezeichnet. Später wurde diese als ZigBee 2006 bezeichnet. Die aktuelle Version der ZigBee Spezifizierung kommt aus dem Jahr 2007 und wird als ZigBee 2007 beziehungsweise ZigBee Pro bezeichnet [VHPA+13, 5132].
ZigBee Pro unterstützt zwei unterschiedliche Sicherheitsstufen: `High Security` (auch bekannt als Commercial Security) und `Standard Security` (ebenso bekannt als Residential Security). Der größte Unterschied zwischen diesen beiden Stufen besteht darin, wie das Schlüssel-Management und die Verteilung der Schlüssel geregelt sind [VHPA+13, 5133]. Geräte, welche die Sicherheitsstufe High Security unterstützen, benötigen mehr Arbeitsspeicher, da sie mehrere Schlüssel für die sichere Kommunikation speichern müssen. Diese Sicherheitsstufe ist für Geräte im industriellen Sektor bestimmt. Die Sicherheitsstufe Standard Security ist für Geräte konzipiert, bei denen kein besonderer Wert auf erhöhte Sicherheit gelegt wird. Ob dies Nachteile für die Sicherheit bei ZigBee bedeutet, wird in diesem Kapitel untersucht.
Diese Bachelorarbeit befasst sich mit der Sicherheit in der Heimautomatisierung und betrachtet in diesem Kapitel ZigBee Pro in der Sicherheitsstufe Standard Security, welche für Heimautomatisierung vorgesehen ist.

3.1 Herstellerangaben laut Dokumentation

Die Angaben des Herstellers zum Thema Sicherheit beziehen sich auf die Möglichkeit, Anwesenheit zu simulieren, indem zum Beispiel Licht mit ZigBee ein- und ausgeschaltete werden kann [ZBha]. Der Hersteller weist darauf hin, dass die Philips Hue Produkte auf ZigBee Light Link basieren. Es wird beschrieben, dass ZigBee Light Link eine sichere, stromsparende und zuverlässige Technik zur Steuerung von Beleuchtung darstellt [ZBhb]. Wie die sichere Technik bei ZigBee funktioniert, wird nicht erörtert.

Auf der Website der ZigBee Allianz gibt es einen Überblick über Sicherheit bei ZigBee Light Link. Dort wird vermerkt, dass ZigBee auf Netzwerkebene Sicherheit benutzt und beide Seiten einen Netzwerkschlüssel austauschen müssen. Damit dieser Schlüssel nicht im Klartext übertragen wird, gibt es einen ZigBee Light Link Master Schlüssel, mit welchem der Netzwerkschlüssel verschlüsselt wird. Dieser ZigBee Light Link Master

Schlüssel wird nur an Hersteller weitergegeben, wenn dessen Gerät ZigBee zertifiziert ist [ZBz12].

3.2 Aufbau

Zur Überprüfung der Angaben des Herstellers und der ZigBee Allianz wird eine Umgebung aufgebaut und die Kommunikation der ZigBee Komponenten untersucht. Bei diesem Aufbau gelangt das Bloom Starter Pack von Philips zum Einsatz. Dieses wird von Philips als ZigBee zertifiziertes Produkt beworben. Das Starter Kit enthält zwei Lampen sowie eine Zentrale. Das Modell und die Produktbezeichnung, ebenso die eingesetzte Firmware-Version findet sich in Tabelle 1.

	Bezeichnung	Modell	Firmware-Version	Betriebssystem
Zentrale	Philips Hue bridge	BSB001	01028090	FreeRTOS v6.0.5
Lampe	Philips Hue bloom	7299761PH		

Tabelle 1: ZigBee Komponenten

Gemäß der Bedienungsanleitung wird die Lampe an den Strom und einen Netzwerkanschluss angeschlossen. Verfügt dieses Netzwerk über einen Zugang zum Internet, erleuchtet zudem die dritte LED. Bei einem Netzwerk ohne Internetanschluss lässt sich die Zentrale nur über eine Representational State Transfer (REST) Schnittstelle steuern. Um die Zentrale über eine existierende Heimautomatisierung-Zentrale, wie beispielsweise Freundliche Hausautomatisierung und Energie-Messung (FHEM), zu kontrollieren, ist kein Internetanschluss nötig. Zum Steuern der Zentrale über die meethue Website (`https://my.meethue.com`) oder mit der Hue Smartphone Anwendung ist ein Internet Zugang notwendig.

3.3 Gerät anlernen

Zuerst wird die Zentrale mit der Smartphone Anwendung und der meethue Webseite verknüpft. Um dies zu vollziehen, muss die App oder die Webseite geöffnet werden. Damit die App oder die Website sich mit der Zentrale verbinden kann, muss der Knopf auf der Zentrale gedrückt werden.
Die Zentrale und die Lampe werden vorkonfiguriert ausgeliefert und sind bereits miteinander verknüpft. Sollte die Zentrale die Lampe nicht erkennen, muss die Lampe manuell zur Zentrale zugewiesen werden. Um die Lampe mit der Zentrale manuell zu verbinden, muss die Zentrale die Seriennummer der Lampe kennen. Die Seriennummer der Lampe befindet sich auf einem Aufkleber, auf dem Netzteil der Lampe. In den Einstellungen

der Hue Smartphone Anwendung muss My Lights und dann Connect New Lights ausgewählt werden, um zur manuellen Suche zu gelangen. Dort wird die Seriennummer der Lampe eingegeben. Sobald die Zentrale mit der Lampe verbunden ist, erscheint sie in der App und kann gesteuert werden.

3.4 Protokoll

Die Kommunikation zwischen der Lampe und der Zentrale erfolgt mit dem ZigBee Light Link Protokoll. Bei diesem Standard handelt es sich um eine vereinfachte Version des ZigBee Standard, bei dem es lediglich Kontrollkomponenten und Licht-Komponenten gibt [ZBf, 16]. Produkte, die ZigBee Light Link zertifiziert sind, gelten als vollständig kompatibel zu ZigBee.
ZigBee basiert auf IEEE 802.15.4, was ein Standard für Datenübertragung in Wireless Personal Area Network (WPAN) ist, welcher darauf ausgelegt ist, wenig Energie zu verbrauchen. Dieser Standard beschreibt die Bitübertragungsschicht (engl. Physical Layer, Abk. PHY) und die Sicherungsschicht (engl. Medium Access Control Layer, Abk. MAC). ZigBee beschreibt die Kommunikation auf der Netzwerkschicht (engl. Network Layer, Abk. NWK) sowie der Anwendungsschicht (engl. Application Support Layer, Abk. ASL) [KS07, 21]. Die Spezifikationen für ZigBee und ZigBee Light Link sind öffentlich und kostenfrei zugänglich und können auf der Website der ZigBee Allianz bezogen werden.

3.5 Kommunikation mithören

Um die Kommunikation zwischen der Zentrale und der Lampe mitzuhören, wird ein USB-Stick mit einem Texas Instrumens CC2531 Chip benutzt. Zum Interpretieren der Nachrichten findet die Software Ubiqua Protocol Analyzer (Version 1.4, Build 2256) Einsatz. Mit dem Ubiqua Protocol Analyzer wird die Kommunikation beim Einschalten einer Lampe mitgehört. Das Einschalten findet über die meethue Website statt.

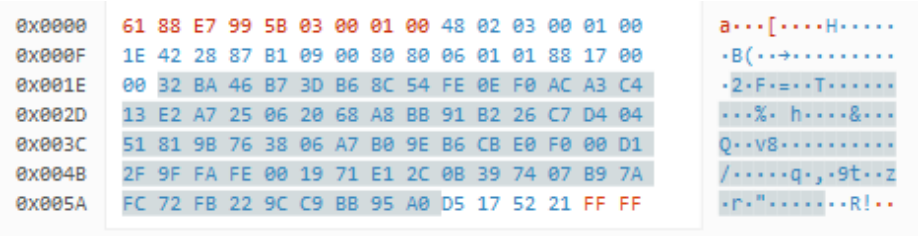

Abbildung 1: ZigBee Paket Bytes aus Ubiqua Protocol Analyzer

Das in Abb. 1 dargestellte Paket ist das mitgelesene Paket zwischen der Lampe und der Zentrale, welches nach dem Einschalten gesendet wurde.

Das Paket besteht aus MAC Kontrolldaten, MAC Nutzdaten und MAC Footer. Die ersten neun Bytes sind die MAC Kontrolldaten und enthalten die Quell- und Ziel-Adresse, Ziel Personal Area Network (PAN) Nummer, eine MAC Sequenz Nummer und MAC Kontrollbytes. Die MAC Nutzdaten des Pakets sind 94 Bytes lang und bestehen aus NWK Kontrolldaten, NWK Kontrollhilfsdaten, NWK Nutzdaten sowie einem Message Integrity Code (MIC). Die NWK Kontroll- und NWK Kontrollhilfsdaten enthalten die Quell- und Ziel-Adresse, Quell-MAC Adresse, eine NWK Sequenz Nummer, eine NWK Frame Nummer und NWK Kontrollbytes. Der Ubiqua Protocol Analyzer zeigt an, dass die NWK Nutzdaten verschlüsselt sind. Die Bytes werden angezeigt, aber nicht mehr von der Software interpretiert. Um dies zu überprüfen, wurden die Nutzdaten mehrerer Pakete mitgehört und verglichen. Die Daten dieser Nutzdaten waren sehr unterschiedlich und es konnte kein Muster erkannt werden.

```
▷ Frame Information: (105 bytes)
◢ MAC Header: (9 bytes)
  ▷ Frame Control: 0x8861
    Sequence Number: 231
    Destination PAN ID: 0x5B99
    Destination Address: 0x0003
    Source Address: 0x0001
◢ MAC Payload: (94 bytes)
  ◢ NWK Header: 0x421E000100030248
    ▷ Frame Control: 0x0248
      Destination Address: 0x0003
      Source Address: 0x0001
      Radius: 0x1E
      Sequence Number: 66
  ◢ NWK Aux Header: (14 bytes)
    ▷ Network Security Control: 0x28
      NWK Frame Counter: 635271
      Source Address: 00:17:88:01:01:06:80:80
      NWK Key Sequence Number: 0
  ◢ NWK Payload: (68 bytes)
      Encrypted Payload: (68 bytes)
    NWK MIC: 0xD5175221
◢ MAC Footer: 0xFFFF
    Frame Check Sequence: 0xFFFF
```

3.6 Sichere Kommunikation

Die Kommunikation auf der Netzwerkschicht ist durch Verschlüsselung der NWK Nutzdaten sowie durch das Anhängen von Prüfsummen an die Datenpakete gesichert. Bei den hier betrachteten Komponenten ist dies bereits vom Hersteller voreingestellt und kann nicht verändert werden. Zum Sichern der Daten gelangt der Algorithmus AES-128 im Modus CCM zum Einsatz. Dies setzt voraus, dass die Kommunikationspartner vorher einen geheimen Schlüssel getauscht haben.
Vor dem Senden eines Pakets wird eine Prüfsumme des Pakets erstellt. Die Nutzdaten und die Prüfsumme werden mit AES-128 im Modus CTR verschlüsselt. Nur wenn ein

Empfänger den geheimen Schlüssel kennt, kann er die Daten und Prüfsumme entschlüsseln. Siehe Abb.2. Dies gewährleistet, dass unbefugte Empfänger, die den Schlüssel nicht kennen, die Daten nicht entschlüsseln können [Cry].

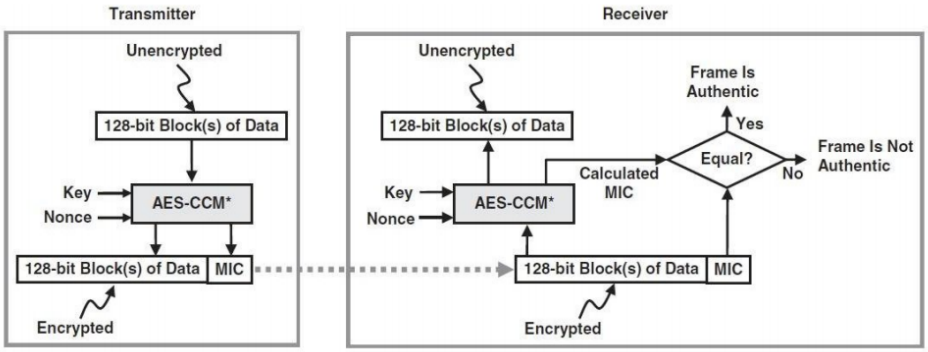

Abbildung 2: Sicherstellen, dass die Datenintegrität nicht verletzt wurde [Far08]

.

3.7 Schlüsselproblem

Es existieren drei Arten von Schlüsseln bei ZigBee.

Master Schlüssel: Der Master Schlüssel wird lediglich für das Ver- und Entschlüsseln von Link und Netzwerk Schlüsseln benutzt. Falls eine der Komponenten den aktuellen Netzwerk Schlüssel nicht kennt, da sie gerade erst dem Netzwerk beigetreten ist, fragt sie diesen bei der Zentrale an. Die Zentrale verschlüsselt den aktuellen Netzwerk Schlüssel mit dem Master Schlüssel und sendet diesen an die Komponente. Ist die Komponenten im Besitz des Master Schlüssels, kann sie den Netzwerk Schlüssel entschlüsseln sowie dem Netzwerk beitreten. In der Spezifikation wird beschrieben, dass der Master Schlüssel vom Hersteller voreingestellt wird.

Link Schlüssel: Link Schlüssel dienen der sicheren Kommunikation zwischen zwei Komponenten. Jede Komponente weist für jede andere Komponenten, mit der sie kommuniziert, einen eigenen Link Schlüssel auf. Wenn Komponente A mit Komponente B kommuniziert, benötigen beide den Schlüssel AB. Erhält ein Angreifer Zugang zu diesem Schlüssel, hat er die Möglichkeit, die Kommunikation zwischen Komponente A und B zu entschlüsseln. Die Kommunikation zwischen den anderen Komponenten kann mit dem Schlüssel AB allerdings nicht entschlüsselt werden.

Link Schlüssel kommen in einem ZigBee Netzwerk mit Standard Security nicht zum Einsatz.

Netzwerk Schlüssel: Alle Komponenten in einem ZigBee Netzwerk benutzen denselben Netzwerk Schlüssel. Dieser wird von der Zentrale generiert und verteilt. Mit diesem Schlüssel werden die NWK Nutzdaten verschlüsselt.

Alle Teilnehmer des PAN müssen denselben NWK Schlüssel für sichere Kommunikation nutzen. Die Verteilung des Schlüssels ist so geregelt, dass ein neuer Teilnehmer sich bei der Zentrale eines ZigBee Netzes anmeldet. Die Zentrale erzeugt einen zufälligen Schlüssel, falls noch kein Schlüssel für dieses Netz erzeugt wurde. Dieser Schlüssel wird mit dem ZigBee Light Link Master Schlüssel verschlüsselt. Ist der neue Teilnehmer ein ZigBee Light Link zertifiziertes Gerät, so sollte der Master Schlüssel in dem Gerät hinterlegt sein. Mit diesem Master Schlüssel entschlüsselt der neue Teilnehmer den NWK Schlüssel für diese ZigBee Netz und nutzt ab sofort diesen für sichere Kommunikation.

3.8 Bekannte Sicherheitsprobleme bei ZigBee

3.8.1 Auslesen des Keys

Die Komponenten sind nicht gegen Auslesen geschützt. Ein Angreifer, welcher Zugang zu einem Gerät hat, welches an einem gesicherten ZigBee Netz teilnimmt, kann versuchen, den Arbeitsspeicher des Gerätes auszulesen. Der Schlüssel für die sichere Kommunikation ist unverschlüsselt im Arbeitsspeicher des Chips abgelegt und kann ausgelesen werden [DF14, 347].
Eine Lösung könnte darin bestehen, dass die Komponente ihren Speicher löscht, sobald sie Anzeichen erkennt, dass versucht wird, den Speicher auszulesen. Sobald erkannt wird, dass ein Teilnehmer aus dem ZigBee Netzwerk verschwunden ist, sollte die Zentrale einen neuen Schlüssel generieren und diesen an sämtliche Geräte verteilen. Die nachfolgende Kommunikation sollte nur noch mit dem neuen Schlüssel stattfinden.

3.8.2 Replay-Angriff

Die ZigBee Pakete enthalten eine Frame und Sequenz Nummer, um zu verhindern, dass ein Paket von einem Angreifer erneut gesendet werden kann. Im Modus Standard Security wird die Frame Nummer allerdings nicht überprüft [ZBs10b, 496]. Die Sequenz Nummer ist nur ein Byte lang und kann folglich nur 256 Zustände annehmen. Ein mitgehörtes Paket mit einer hohen Sequenz Nummer kann erneut gesendet werden, wenn die Sequenz Nummern der Pakete größer als 256 werden. Nachfolgende Pakete beginnen dann wieder bei einer niedrigeren Sequenz Nummer. Wird das aufgezeichnete Paket nun gesendet, wird es akzeptiert. Dies wurde in einem Versuch von Jan Durech und Mario

Franekova beschrieben und durchgeführt [DF14, 348].
Eine Lösung gegen Replay-Angriffe könnte sein, dass die Pakete einen aktuellen Zeitstempel enthalten. Sollte die Sequenz Nummer zurückgesetzt werden und ein Angreifer sendet ein Paket mit einer höheren Sequenz Nummer, hätte die Komponente die Möglichkeit, dies zu erkennen. Dies würde jedoch erfordern, dass die Komponenten die aktuelle Zeit kennen müssen.

3.8.3 ZigBee Light Link Master Schlüssel

Der ZigBee Light Link Master Schlüssel wurde im März 2015 im Internet veröffentlicht und ist online frei zugänglich. Einer der ersten Posts kam von dem Twitter Benutzer `MayaZigBee`. Der Post ist nicht mehr verfügbar, an dieser Stelle ist der Text `"This Tweet from @MayaZigBee has been withheld in response to a report from the copyright holder."` zu lesen. Dies deutet darauf hin, dass Twitter sehr schnell aufgefordert wurde, diesen Post zu entfernen, da `MayaZigBee` sich bereits nach sieben Tag nach seiner Veröffentlichung darüber beschwert, dass sein Post entfernt wurde [May15]. Der Versuch, die Veröffentlichung des Schlüssels zu unterbinden, war nicht erfolgreich. Die Twitter Nachricht wurde zwar gelöscht, allerdings gibt es weiterhin mehrere Stellen im Internet, auf denen der Schlüssel veröffentlicht ist. Mit einer Suchmaschine ist der Schlüssel weiterhin im Internet zu finden.
Da der Master Schlüssel nun für jeden zugänglich ist, bedeutet dies eine Gefahr für den verschlüsselten Schlüsseltausch (siehe 3.7).

3.8.4 Kompatibilität

Damit ZigBee zertifizierte Komponenten untereinander kommunizieren können, müssen sie sich an die Standard ZigBee Schnittstellen halten. Eine dieser Schnittstellen sieht vor, dass ein Gerät, welches noch nicht an einem ZigBee Netz teilnimmt, den aktuell eingesetzten Netzwerkschlüssel abfragen kann, um dem Netzwerk beizutreten. Diesen Prozess bezeichnet man als unsicheres Beitreten [ZBs10a, 31]. Der aktuelle NWK Schlüssel wird dann mit dem Standard TrustCenter Link Schlüssel verschlüsselt. Der Standard TrustCenter Link Schlüssel ist öffentlich in der ZigBee Spezifizierung dokumentiert sowie für jeden zugänglich. Der Schlüssel besteht aus dem Wort `ZigBeeAlliance09` umgewandelt zu Hexadezimal.
Gelingt es einem Angreifer, die Kommunikation dieses Schlüsseltausches mitzuhören, kann er diese mit dem TrustCenter Schlüssel entschlüsseln und hat somit den aktuell eingesetzten Netzwerkschlüssel [Zil15]. Ein Angreifer hat ebenfalls die Möglichkeit, den Schlüsseltausch selber zu initiieren, indem er eine ZigBee Komponente simuliert, die

dem Netzwerk beitreten möchte.
Dies ist jedoch nur möglich, wenn die Komponenten im Modus Standard Security laufen. Das unsichere Beitreten eines Netzwerks ist bei einem Netzwerk im Modus High Securtiy nicht gestattet [Gis08, 338].

3.9 Sicherheitsziele

Hier wird beschrieben, ob die in 2.1 definierten Sicherheitsziele erfüllt werden.

Bei ZigBee werden die NWK Nutzdaten mit AES-128 verschlüsselt. Die Verschlüsselung gilt als sicher und nur wer den Schlüssel besitzt, kann die Daten entschlüsseln. Um Vertraulichkeit zu gewährleisten, muss sichergestellt sein, dass ausschließlich Befugte Zugang zu den Schlüsseln haben. In der aktuellen Implementierung des ZigBee Standards ist die Verteilung nicht sicher. Ein Benutzer hat keine Möglichkeit, darauf Einfluss zu nehmen.

Bei jedem Paket wird eine Prüfsumme des Pakets erstellt und mitübertragen. Dies stellt sicher, dass die Pakete vollständig übertragen und nicht verändert werden. Sollte die Prüfsumme nicht zu dem empfangenen Paket passen, ist die Integrität des Pakets verletzt. Ein Empfänger hat die Möglichkeit, dies zu überprüfen, indem es selbst eine Prüfsumme erstellt.

Im Modus Standard Security verwenden die Komponenten in einem ZigBee Netzwerk alle denselben Schlüssel für die sichere Kommunikation. Dies gewährleistet, dass nur Komponenten in dem ZigBee Netzwerk miteinander kommunizieren können. Sollte ein Angreifer den aktuellen Netzwerk-Schlüssel besitzen, kann er ein Paket senden, bei dem die Absender- beziehungsweise Empfänger-Adresse gefälscht ist. Eine verlässliche Authentifizierung der Komponenten innerhalb des Netzwerks ist nicht möglich. Im Modus High Security wird die Kommunikation zwischen den Komponenten mit einem Link-Schlüssel verschlüsselt. Für die Kommunikation zwischen den Komponenten werden unterschiedliche Schlüssel eingesetzt. Kommuniziert eine Komponente A mit Komponente B und wird die Kommunikation mit dem Link-Schlüssel AB verschlüsselt, kann Komponente B davon ausgehen, dass Komponente A authentisch ist, da sie den Schlüssel AB besitzt. Sollte ein Angreifer in den Besitz des Link-Schlüssels AB gelangen, kann er nur Kommunikation zwischen Komponente A und B abhören beziehungsweise Pakete erzeugen, die angeblich von Komponente A oder Komponente B stammen.

ZigBee kann auf verschiedenen Frequenzen kommunizieren. Für Europa steht ein Kanal auf der Frequenz 868,3 MHz zur Verfügung. Für Amerika und Australien bieten sich

auf der Frequenz 902 bis 928 MHz zehn Kanäle. Für den weltweiten Einsatz kann die Frequenz 2405 bis 2480 MHz Nutzung finden. Hier stehen 16 verschiedenen Kanäle zur Verfügung [zig14, 23]. Sollte ein Kanal gestört oder belegt sein, besteht die Möglichkeit, auf einen anderen Kanal zu wechseln, falls vorhanden beziehungsweise falls dies möglich ist. Dies ermöglicht es, die Verfügbarkeit zu erhöhen. Die hier betrachtete Lampe kann nur auf 2,4 GHz kommunizieren, ein Wechsel zu anderen Frequenzbereichen wie etwa 868,3 MHz ist nicht möglich.

3.10 Ergebnis

Bei ZigBee wird für die Verschlüsselung und Authentizität der Daten ein sicheres Verfahren benutzt. Die Sicherheit für die Verschlüsselung hängt davon ab, ob der Schlüssel geheim ist. Die Veröffentlichung des ZigBee Light Link Master Schlüssels stellt nur ein geringes Risiko da. Dieser erlaubt es einem Angreifer, den neuen NWK Schlüssel zu entschlüsseln. Hierfür muss ein Angreifer in dem Moment, in dem ein neues Geräte dem Netzwerk beitritt, den Netzwerkverkehr mithören und entschlüsseln. Nur dann hat er die Möglichkeit, mit dem ZigBee Light Link Master Schlüssel den neuen NWK Schlüssel zu erfahren.
Ein erheblich größeres Risiko bedeuten die Kompatibilität-Schnittstellen in ZigBee. Diese erlaubt es einem Angreifer, jederzeit einen unsicheren Beitritt zu einem ZigBee Netzwerk zu beantragen. In einem Netzwerk im Modus Standard Security kann dies in der aktuellen Spezifikation 1.2 auch nicht abgeschaltet werden. Die Spezifikation hat Potenzial, um damit ein sicheres Netzwerk zu betreiben, allerdings erst dann, wenn die genannten Probleme in einer neueren Version der ZigBee Spezifikation gelöst werden.

4 EnOcean

EnOcean ist ein Funkstandard für Funkanwendungen im Bereich Hausautomatisierung gemäß Standard ISO/IEC 14543-31X [enO15c, 3]. Dieser Standard beschreibt Funkanwendungen, welche einen besonders niedrigen Energieverbrauch aufweisen. Die EnOcean Komponenten gibt es für verschiedene Frequenzbereiche, damit sie in Regionen wie Asien (315 MHz), Europa und China (868 MHz), USA und Kanada (902 MHz) und Japan (928 MHz) Einsatz finden können [enO15a]. Die EnOcean Komponenten erhalten ihre Energie aus Bewegung, etwa durch das Betätigen einer Taste. Es besteht überdies die Möglichkeit, die Energie durch Solarzellen oder Temperaturunterschiede zu generieren. Durch diese Energiegewinnung ist es möglich, die EnOcean Komponenten ohne Batterie und Wartungsfrei zu betreiben. Dieses Kapitel untersucht, ob EnOcean Sicherheitsmechanismen einsetzt, um ihre Kommunikation zu schützen. Bei einem selbst durchgeführten Versuch wird die Kommunikation analysiert, um festzustellen ob Sicherheitsmechanismen zur Verwendung gelangen.

4.1 Herstellerangaben laut Dokumentation

In der Bedienungsanleitung des EnOcean Starter Kits wird angeführt, dass bei dem Taster zwischen einem normalen und sicheren Modus gewechselt werden kann [enO15b, 6]. Details zum sicheren Modus werden nicht genannt, es wird lediglich darauf hingewiesen, dass eine weitere Dokumentation unter `http://www.enocean.com/en/securit-specification/` verfügbar ist. Ob bei den anderen Komponenten aus dem Starter Kit zwischen dem normalen oder sicheren Modus gewechselt werden kann, wird nicht erörtert.
Auf der EnOcean Webseite wird beschrieben, dass EnOcean auf ein Modulares Sicherheitskonzept setzt [eno16]. Es ist möglich, je nach Anforderung an Sicherheit, Rolling Codes oder Verschlüsselung einzusetzen beziehungsweise beides zu kombinieren [enO15c, 4]. EnOcean verweist darauf, dass die Komponenten nicht genutzt werden sollen, wenn dies Wertsachen gefährden könnte [enO13a, 5].

4.2 Enocean Kommunikation

Zur Untersuchung der Kommunikation bei EnOcean wird das EnOcean Starter Kit ESK 300 (868MHz) verwendet. Daraus werden die Komponenten in Tabelle 2 eingesetzt. Der Bausatz für Industrieschalter und der Temperatursensor finden bei diesem Aufbau nicht Anwendung.

	weitere Bezeichnung	Typ
Zentrale	USB Gateway	USB 300 DB
Schalter	Taster	PTM 215

Tabelle 2: EnOcean Komponenten

Das USB Gateway wird mit dem Computer verbunden und zum Konfigurieren und Auslesen der Nachrichten wird die Software DolphinView (Advanced Version 3.6.0.0) eingesetzt. Das Programm verbindet sich mit dem USB Gateway und ist ohne weitere Konfiguration einsatzbereit. Beim Schalter handelt es sich um einen batterielosen Funkschalter. Die benötigte Energie zum Senden von Nachrichten wird durch das Betätigen des Schalters gewonnen. Der Schalter hat zwei Tasten, genannt A und B, die sich oben sowie unten betätigen lassen. Wird Taste A oben gedrückt, wird dies als A0 bezeichnet. Beim Drücken der Taste A unten, wird dies als A1 bezeichnet. Es wird die Taste A0 betätigt. Durch das USB Gateway werden diese Nachrichten empfangen:

```
55 00 07 07 01 7A F6 30 FE FE E1 E5 30 02 FF FF FF FF 37 00 89
55 00 07 07 01 7A F6 20 FE FE E1 E5 30 02 FF FF FF FF 34 00 C9
```

Die Nachricht in Zeile eins erschien, nachdem die Taste A0 heruntergedrückt wurde. Die Nachricht in der zweiten Zeile wurde nach dem Loslassen der Taste A0 empfangen. Wie die Nachricht aus Zeile zwei interpretiert werden kann, ist in Tabelle 3 ersichtlich. Die

Byte	Bezeichnung	Hex	Beschreibung
1	Sync Byte	55	
2,3	Länge Daten	00 07	7
4	Länge optionale Daten	07	7
5	Paket Typ	01	Funk Nachricht
6	Prüfsumme	7A	
7	RORG	F6	Repeated Switch Communication
8	Nutzlast	20	Taste loslassen
9,10,11,12	SenderID	FE FE E1 E5	
13	Status	30	0011 0000
14	Teilnachrichten	02	
15,16,17,18	Empfänger	FF FF FF FF	Broadcast
19	Empfangsstärke (dBm)	34	-52
20	Nutzdaten	00	
21	Prüfsumme	C9	

Tabelle 3: Interpretation EnOcean Nachricht

Nachricht ist in drei Teile geteilt. Byte eins bis fünf sind Kopf Informationen, Byte 7-13

sind Daten und Byte 14-20 sind optionale Daten. Die Prüfsumme der Kopf Informationen ist in Byte sechs gespeichert und die Prüfsumme der Daten und optionale Daten sind in Byte 21 gespeichert. Das erste Byte ist stets 0x55 und dient der Synchronisierung. Byte zwei und drei beschreiben die Länge der Daten. Byte vier beschreibt die Länge der optionalen Daten. An fünfter Stelle steht das Byte mit Informationen über den Paket Typ, in diesem Fall ist es 0x01, da es sich um eine Funk-Nachricht handelt [enO14, 13]. Der Datenblock (Byte 7 bis 13) enthält in Byte 9 bis 12 die eindeutige SenderID sowie die Nutzlast 0x20 in Byte acht. Byte sieben umfasst die Information des Nachrichten Typs, in diesem Fall 0xF6, was für Repeated Switch Communication steht [enO14, 8]. Der Status in Byte 13 beschreibt Nachrichten-Kontrollbits. Byte 14 beschreibt, in wie vielen Teilnachrichten, sogenannten Sub Nachrichten, die Nachricht gesendet wurde [Gra13, 158]. In Byte 15 bis 18 steht die Empfängeradresse, in diesem Fall handelt es sich um eine Nachricht an alle und die Empfängeradresse lautet FF FF FF FF. In Byte 19 steht die Empfangsstärke, 0x34 steht für -52dBm. Die Nutzdaten in Byte 20 sind 00. Das letzte Byte ist die Prüfsumme. [enO14, 13]
Das Herunterdrücken der Taste A0 sendet eine Nachricht mit der Nutzlast 0x30. Sobald die Taste losgelassen wird, erfolgt das Senden einer Nachricht mit der Nutzlast 0x20. Dies ermöglicht es, den Taster nicht nur für das Ein- und Ausschalten zu verwenden, er kann zudem zum Dimmen genutzt werden. Als Nächstes wird probiert, die Kommunikation mit den Sicherheitsmaßnahmen bei EnOcean abzusichern.

4.3 Sichere Kommunikation

EnOcean bietet drei verschiedene Sicherheitsmechanismen an. Diese können je nach Bedarf kombiniert werden. Um Vertraulichkeit zu gewährleisten, können die Nutzdaten verschlüsselt werden. Damit der Empfänger die Integrität und Authentizität prüfen kann, existiert ein Nachrichtenauthentizität Code. Gegen Replay Angriffe gibt es einen Rolling Code. In diesem Kapitel gelangen diese Sicherheitsmechanismen zur Erläuterung und Beschreibung.
Damit die Verschlüsselung und das Generieren der Nachrichtenauthentizität Codes möglich sind, muss zuvor ein geheimer Schlüssel getauscht werden. Dieser wird beim Anlernen der Komponenten übertragen. Sollten die Komponenten einen gleichen voreingestellten Schlüssel haben, wird der geheime Schlüssel mit dem voreingestellten Schlüssel vor dem Übertragen verschlüsselt. Ist dies nicht der Fall, wird der geheime Schlüssel unverschlüsselt übertragen. Um den Anlernvorgang zu starten, muss an dem USB-Gateway der Lern-Modus aktiviert werden. Nur wenn dies der Fall ist, kann eine neue Komponente eine Anlernnachricht an das Gateway schicken und so einen Schlüsseltausch starten [enO13a, 16]. Für manche Sicherheitsmechanismen ist ein sogenannter SubKey

notwendig. Dieser wird erzeugt, indem der geheime Schlüssel bitweise verschoben sowie mit einer Zeichenkette aus Nullen mit XOR verknüpft wird [enO13a, 16].

Es werden zwei verschiedene Verschlüsselungsalgorithmen angeboten. Als sicherere Verschlüsselung wird die variable AES Verschlüsselung beschrieben [enO13a, 23]. In der Konfigurationsoberfläche von DolhinView wird diese als VXOR AES bezeichnet. Bei dieser Verschlüsselung wird eine bekannte Zeichenkette, von EnOcean wird dies als öffentlicher Schlüssel benannt, mit dem Rolling Code durch XOR verschlüsselt [enO13a, 26]. Diese XOR Zeichenkette wird dann mit dem geheimen Schlüssel per AES verschlüsselt. Die nun AES verschlüsselte Zeichenkette wird mit den zu übertragenden Daten per XOR verschlüsselt, siehe Abb. 3. Alternativ kann der Verschlüsselungsalgorithmus AES im Modus CBC verwendet werden. EnOcean nutzt für den CBC Modus immer den gleichen IV, bei dem alle Bytes auf `0` gesetzt sind [enO13a, 22].

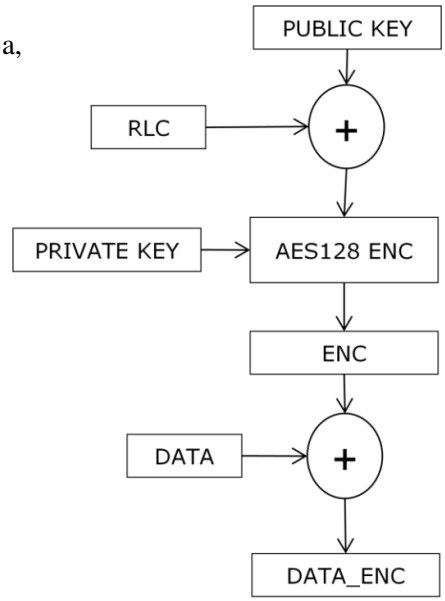

Abbildung 3: Variable AES Verschlüsselung [enO13a, 23]

Zur Erstellung eines Nachrichtenauthentizität Codes, auch Cipher-based Message Authentication Code (CMAC) genannt, werden das RORG Byte, die Daten Bytes und, falls konfiguriert, ein Rolling Code mit einem Unterschlüssel durch XOR verschlüsselt. Dieses Ergebnis wird dann mit dem 128 Bit Schlüssel mit AES-CMAC verschlüsselt. Dieser CMAC wird vor dem Senden einer Nachricht erstellt und mit übertragen. Der Empfänger hat somit die Möglichkeit, die Integrität der Nachricht zu überprüfen. Lediglich Sender, die im Besitz des geheimen Schlüssels sind, können Nachrichten mit einem korrekten CMAC erzeugen.

Der Rolling Code ist ein Zähler, der beim Anlernen der Komponenten gesetzt wird. Je nach Einstellung ist dieser Zähler 16 oder 24 Bit groß. Der Zähler wird um den Wert eins erhöht, wenn der Sender eine Nachricht sendet beziehungsweise wenn der Empfänger eine Nachricht empfängt. Der Zähler kann in den Nachrichten mitgeschickt werden, um die Berechnung des CMAC zu beschleunigen [enO13a, 27]. Wird der Zähler mitgeschickt, wird die Nachricht länger und es wird mehr Energie zum Übertragen benötigt. Außerdem schwächt dies die Sicherheit, da der Zähler beim Übertragen nicht verschlüsselt wird [enO13a, 27]. Für den Fall, dass die Zähler auf Sender- und Empfänger-Seite nicht mehr gleich sind, gibt es einen Zähler-Toleranzbereich. Falls der Sender ein paar Nachrichten gesendet hat, die nicht beim Empfänger angekommen sind, ist der Zäh-

ler beim Sender höher als beim Empfänger. Empfängt der Empfänger eine Nachricht, bei welcher der Zähler zu hoch ist, merkt der Empfänger, dass die Zähler nicht mehr stimmen. In diesem Fall erhöht der Empfänger seinen Zähler um den Wert eins und probiert erneut, ob die Zähler stimmen. Dies wird so oft wiederholt, bis der Zähler-Toleranzbereich überschritten wird oder die Zähler erneut identisch sind. Der Zähler-Toleranzbereich erlaubt eine Abweichung von 128 [enO13a, 27].

4.4 Sichere Kommunikation aktivieren

Das Programm DolhinView ermöglicht es, das USB-Gateway zu konfigurieren. Unter dem Reiter Sicherheit kann zwischen verschiedenen Optionen für die Sicherheitsmechanismen ausgewählt werden. Es kann die Größe, 24 oder 32 Bit, des Rolling Codes festgelegt werden und ob dieser in den Nachrichten mit übertragen werden soll. Für die CMAC kann ebenfalls die Größe, 16 oder 24 Bit, gewählt werden. Wenn eine Verschlüsselung Verwendung finden soll, kann zwischen AES-128 und VXOR AES-128 gewählt werden. Für diesen Test wird eingestellt, dass der Zähler für die Rolling Codes 16 Bit lang ist und nicht mit übertragen wird. Zudem soll ein 24 Bit CMAC und VXOR AES Verschlüsselung eingesetzt werden. Nach Einstellung dieser Werte wird der Anlernknopf betätigt und danach auf dem Taster die Tastenkombination fürs Anlernen gedrückt. Für das Anlernen werden B1 und B0 oder A1 und A0 gleichzeitig gedrückt. In den Nachrichten, die im DolhinView angezeigt werden, steht, dass sichere Anlernnachrichten geschickt wurden. Um dies zu überprüfen wird die Taste A1 heruntergedrückt, wodurch der Taster folgende Nachricht sendet:

```
55 00 0A 07 01 EB  \
30 02 14 6E 09 FE FE E1 E5 00 \
02 FF FF FF FF 31 00 01
```

Um die Nachricht lesbarer zu machen, wurden der Kopf, der Daten sowie der optionale Datenteil durch einen Zeilenumbruch und \ getrennt. Der Kopfteil und optionale Datenteil, siehe Zeile eins und Zeile drei, weist keine Veränderung gegenüber dem mitgehörten Paket aus Abschnitt 4.2 auf. Der Datenteil in Zeile zwei hat sich von sieben auf zehn Bytes vergrößert. Das RORG Byte hat den Wert `30`. Dies legt fest, dass diese Nachricht als sichere Nachricht interpretiert werden muss [enO13a, 10]. Die Nutzlast verfügt über den Wert `02 14 6E 09`. Zum Vergleich: Ist die Kommunikation nicht verschlüsselt, wird beim Betätigen der Taste A1 die Nutzlast `30` gesendet. Die Nutzlast der Nachricht wird nicht im Klartext übertragen, sobald Verschlüsselung eingeschaltet ist.

4.5 Sicherheitsziele

Hier wird erörtert, ob die in 2.1 definierten Sicherheitsziele erfüllt werden.

Die Komponenten bei EnOcean haben die Möglichkeit, vertraulich zu kommunizieren. Hierfür können der Verschlüsselungsalgorithmus AES im Modus CBC oder das variable XOR AES Verfahren gewählt werden. Bei aktivierter Verschlüsselung können die Nachrichten nur entschlüsselt werden, wenn der Empfänger im Besitz des geheimen Schlüssel ist. Sollte die Kommunikation unberechtigt abgehört werden, sind die Nutzdaten geschützt und liefern keine Informationen.

Die Integrität der Nachrichten wird unter anderem durch Prüfsummen in den Nachrichten gewährleistet. Die Prüfsumme bietet allerdings lediglich Schutz vor Übertragungsfehlern. Sollte ein Angreifer eine unautorisierte Nachricht schicken, könnte er die korrekte Prüfsumme selbst bestimmen und mit der Nachricht übertragen. Es besteht die Möglichkeit, die Nachrichten mit einem Nachrichtenauthentizität Code zu schützen. Im Rahmen dessen wird vor dem Senden eine Prüfsumme der Nachricht berechnet sowie mit einem geheimen Schlüssel verschlüsselt. Ist der Empfänger im Besitz des geheimen Schlüssels, kann er die Prüfsumme entschlüsseln und überprüfen, ob die Integrität der Nachricht verletzt wurde.

Zur Authentifizierung von Nachrichten bestehen mehrere Möglichkeiten. Die Komponenten bei EnOcean weisen eine eindeutige Absenderkennung auf. Es ist nicht vorgesehen, dass diese geändert werden kann. Eine Komponente, die als Zentrale Einsatz findet, hat die Möglichkeit, ihre Absenderkennung zu ändern. Dies ist jedoch nur zehnmal möglich [enO13b, 52]. Weiterhin gibt es die Möglichkeit, einen Nachrichtenauthentizität Code mit den Nachrichten zu übertragen. Somit ist gewährleistet, dass die Nachricht nur von einer Komponente gesendet werden kann, welche im Besitz des geheimen Schlüssels ist.

Die EnOcean Komponenten kommunizieren per Funk auf der Frequenz 868 MHz. Wird diese Frequenz gestört oder ist diese belegt, können die EnOcean Komponenten nicht mehr kommunizieren. Ein Wechsel der Frequenz ist nicht möglich. Sollte die Übertragung auf der Frequenz gestört sein, hat ein Anwender keine Möglichkeit, die EnOcean Komponenten zu nutzen. Die EnOcean Komponenten können von RFID-Funk gestört werden, da diese auf der gleichen Frequenz kommunizieren. In Bezug auf EnOcean wir geraten, bei der Installation von EnOcean Komponenten darauf zu achten, dass keine RFID-Sender in der unmittelbaren Nähe eingesetzt werden [enO15c, 5].

4.6 Ergebnis

Das modulare Sicherheitskonzept bei EnOcean ermöglicht es, die Komponenten, je nach Bedarf, abzusichern. Bei Sensoren genügt es unter Umständen, wenn die Daten verschlüsselt sind, jedoch keine CMAC übertragen wird. Bei einer Rollladensteuerung wäre es beispielsweise ausreichend, die Daten im Klartext zu übertragen, die Kommunikation aber mit CMAC abzusichern. Für sensiblere Daten, wie beispielsweise den Stromverbrauch, würde ein Benutzer auf die Kombination von Verschlüsselung und CMAC setzen. Die Nachrichtenlänge, Verarbeitungszeit sowie der Energieverbrauch der Komponenten steigen, je mehr Sicherheitsmechanismen aktiviert sind. Benutzer sollten abwägen, welches Maß an Sicherheit sie bei ihren Komponenten benötigen.

5 ZWave

Das Protokoll Z-Wave wurde von der Firma Sigma Designs entwickelt. Es findet bei der Funkkommunikation Einsatz, um Daten für die Heimautomatisierung zu übertragen. Das proprietäre Protokoll wird von verschiedenen Herstellern für Heimautomatisierung genutzt. Um Kompatibilität zwischen den Herstellern zu gewährleisten, müssen die Hersteller ihre Komponenten von der Z-Wave Alliance zertifizieren lassen [zwa15d]. Vorteile des Protokolls sind die Fähigkeit, ein Mesh-Netzwerk zu bilden sowie trotz geringer Leistungsaufnahme Pakete innerhalb des Netzwerks schnell zu übertragen [zwa]. Die Protokoll Spezifikation ist nicht frei verfügbar. Hersteller erhalten die Spezifikation erst, nachdem sie eine Verschwiegenheitserklärung unterzeichnet haben. Es erfolgt eine Untersuchung, wie die Z-Wave Komponenten eingesetzt werden und wie die Kommunikation abzusichern ist.

5.1 Herstellerangaben laut Dokumentation

Auf der Website des Herstellers devolo wird angegeben, dass das devolo Home Control System auf der Funktechnik Z-Wave basiert und dieses zertifizierte System die maximale Datensicherheit gewährleistet. Zudem wird erwähnt, dass die standardisierte Funktechnik eine verschlüsselte Verbindung zwischen den Z-Wave Komponenten herstellt und somit eine hohe Kommunikationssicherheit offeriert. Auf dem Datenblatt der Z-Wave Zentrale von devolo wird angeführt, dass AES-128 zur Sicherheit zum Einsatz gelangt [zwa15c]. Die Z-Wave Komponenten bilden ein Netzwerk und jede Z-Wave Komponenten bietet die Möglichkeit, Nachrichten an andere Z-Wave Komponenten weiterzuleiten. Develo gibt zudem an, dass ihre Z-Wave Komponenten mit den Z-Wave Komponenten anderer Hersteller kompatibel sind [zwa15e].
Die Website des Z-Wave Hersteller vermerkt, dass Z-Wave eine sichere Technologie sei. Als Begründung wird erwähnt, dass jede Z-Wave Komponente eine einmalige ID in einem Z-Wave Netzwerk bekommt. Dies soll sicherstellen, dass sich die IDs von benachbarten Z-Wave Komponenten differenzieren und Konflikte mit benachbarten Komponenten vermieden werden. Für Komponenten, welche ein hohes Maß an Sicherheit erfordern, bietet Z-Wave eine AES-128 Verschlüsselung an. Diese Art der Verschlüsselung werde auch von großen Banken eingesetzt, um ihre Finanzdaten zu sichern. Z-Wave mit AES Verschlüsselung wird laut der Z-Wave Website von vielen eingesetzten Z-Wave Zentralen unterstützt. Dies ist an dem Z-Wave Plus Logo auf den Geräten zu erkennen [zwa15a].

5.2 Aufbau

Für diesen Aufbau gelangt das Home Control Starter Paket (9362) von Devolo zur Verwendung. Es kommen die Komponenten aus Tabelle 4 zum Einsatz. Nach dem Auspa-

	Bezeichnung	Typnummer
Zentrale	devolo Home Control Central Unit	MT2600
Steckdose	devolo Metering Plug	MT02646

Tabelle 4: Z-Wave Komponenten

cken wird die Zentrale an den Strom angeschlossen. Zur Steuerung benötigt die Zentrale einen Internet-Zugang. Der Hersteller devolo bietet Komponenten an, um das Stromnetz zur Übertragung von Netzwerkkommunikation zu nutzen. Diese Technologie befindet sich ebenfalls in der Zentrale. Somit ist es möglich, die Zentrale ohne Netzwerkkabel zu benutzen, falls es einen Internetzugang durch das Stromnetz gibt. Für diesen Aufbau wird die Zentrale mit einem Netzwerkkabel an ein Internetgateway angeschlossen. Vom Hersteller wird eine Website unter der Adresse `https://www.mydevolo.com/` bereitgestellt. Zuerst erfolgt das Anlegen eines Benutzerkontos. Beim Erstellen des Benutzerkontos muss eine Postleitzahl eingeben werden. In der Erklärung wird angegeben, dass dies zum Ermitteln von Wetterdaten nötig sei. Nach dem ersten Anmelden mit dem Benutzerkonto muss die Zentrale mit dem Benutzerkonto verknüpft werden. Auf der Website steht bereits, dass eine Zentrale gefunden wurde. Es wird die Seriennummer der Zentrale angegeben, um sicherzustellen, dass es sich um die richtige Zentrale handelt. Nachdem dies bestätigt wurde, muss der Home-Knopf auf der Zentrale gedrückt werden. Dies gewährleistet, dass der Benutzer Zugang zur Zentrale hat. Die Zentrale ist somit erfolgreich eingerichtet und mit dem Benutzerkonto verknüpft. Um die Steckdose mit der Zentrale zu verbinden, wird im Menü der Punkt Geräte ausgewählt. Als Nächstes muss angegeben werden, um welche Art von Gerät es sich handelt. Die Website zeigt an, dass die Zentrale sich für drei Minuten im Anlern-Modus befindet. Innerhalb dieser Zeit muss eine neue Z-Wave Komponente eingeschaltet werden. Die Steckdose wird an den Strom angeschlossen und die Zentrale meldet, dass sie erfolgreich verbunden sind. Über die Website lässt sich die Steckdose steuern sowie der Verbrauch ablesen. Auf der Website gibt es keine Informationen, ob die Zentrale und die Steckdose Sicherheitsmechanismen bei der Kommunikation einsetzen. Alle bei der für Z-Wave zertifizierten Geräte werden auf der Website der Z-Wave Alliance gelistet. Dort gibt es detaillierte Informationen über die Z-Wave Komponenten. Gemäß der Z-Wave Alliance unterstützt die Steckdose `Z-Wave Network Security`, `Z-Wave AES-128 Security` und die Kommando Klasse `Security` [zwa14].

Um zu überprüfen, ob sich die Steckdose ohne Sicherheitsmechanismen betreiben lässt,

fand ein Versuch statt. Zur Steuerung wird die Open Source Software des Heimautomatisierungsprojekts FHEM eingesetzt. Zum Senden und Empfangen der Nachrichten wird ein USB Stick der Firma Z-Wave.Me benutzt. Bei der Konfiguration wurden keine Sicherheitsmechanismen konfiguriert. Um die Steckdose einzuschalten, wird die Nachricht `00 13 03 03 25 01 FF 25 03` geschickt. Die Steckdose schaltet sich direkt ein, nachdem die Nachricht gesendet wurde. Zum Ausschalten wird die Nachricht `00 13 03 03 25 01 00 25 03` geschickt. Die Steckdose schaltet sich direkt aus, nachdem die Nachricht gesendet wurde. Die Nachrichten unterscheiden sich nur durch ein Byte. Beim Einschalten wird das Byte 0xFF und beim Ausschalten das Byte 0x00 geschickt. Es ist also möglich, die Steckdose auch ohne den Einsatz von Sicherheitsmechanismen zu betreiben.

Die Zentrale von devolo bietet keine Konfiguration, um auszuwählen, ob sichere Kommunikation eingesetzt werden soll. Zudem besteht in der Zentrale keine Informationen darüber, ob die Kommunikation abgesichert ist.

5.3 Protokoll

Das Z-Wave Protokoll ist proprietär und nicht frei verfügbar. Hersteller, die Z-Wave Komponenten entwickeln, verfügen über Zugang zu den Protokoll-Spezifikationen, allerdings dürfen sie keine Information darüber veröffentlichen. Es gibt eine offene und frei verfügbare Version des Z-Wave Protokolls mit dem Name Open-Zwave [zwa15b]. Die Open-Zwave Software kommuniziert mit den Z-Wave Komponenten über ein Kontrollgerät mit einem Z-Wave Chip. In diesem Z-Wave Chip ist eine einmalige Home-ID eingestellt, welche nicht geändert werden kann [zwa13, 1]. Dies soll sicherstellen, dass mit einem Z-Wave Chip lediglich die eigenen Geräte kontrolliert werden. Durch die Arbeit des Open-Zwave Projekts und die Evaluation des Z-Wave Protokolls von Behrang Fouladi und Sahand Ghanoun wurden Details zu dem Z-Wave Protokolls öffentlich.

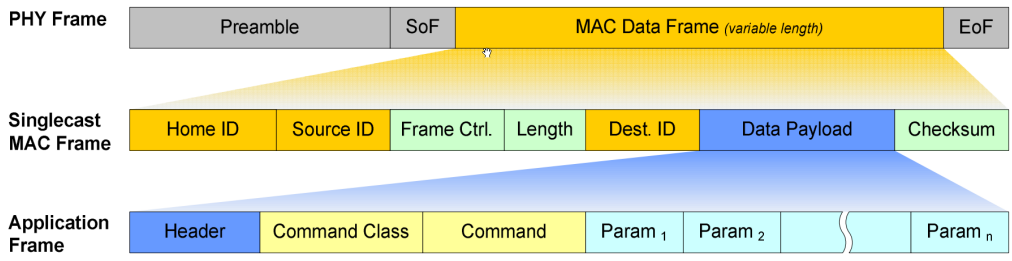

Abbildung 4: Z-Wave Paket mit verschieden Ebenen [zwa13, 3]

Das Protokoll ist in vier Ebenen unterteilt. Die physikalische Ebene wird genutzt, um per

Funk Nachrichten zu senden und empfangen. Diese Ebene basiert auf der Spezifikation ITU-T G.9959. Dort wird beschrieben, wie die Kommunikation abläuft [zwa13, 2].
Die Transport-Ebene ist für das Weiterleiten, das Senden von Empfangsbestätigungen sowie die Bestimmung der Paket Authentizität zuständig. Die Z-Wave Pakete enthalten eine 32 Bit Home-ID. Diese stellt sicher, dass es keine Konflikte gibt, falls mehrere Z-Wave Netzwerke gleichzeitig betrieben werden. Zur Identifizierung einer Z-Wave Komponente enthalten die Pakete zudem eine acht Bit Node-ID. Das Paket enthält zudem Kontrollinformationen, ob es sich an einen oder mehrere Empfänger richtet. Die Daten zur Kommunikation sind in den Nutzdaten des Pakets enthalten. Damit ein Empfänger die Möglichkeit hat, Übertragungsfehler festzustellen, inkludiert das Paket zudem eine Prüfsumme [zwa13, 2]. Ist zur Übertragung der sichere Übertragungsmodus aktiviert, wird ein acht Byte Authentisierungs-Block mit übertragen.
Die Netzwerk-Ebene ist für die Weiterleitung von Paketen zuständig. Die Komponenten in einem Z-Wave Netzwerk bilden ein Mesh Netzwerk. Dies ermöglicht es, den Teilnehmern Pakete zu schicken und empfangen, auch wenn sie keine direkte Verbindung zu einer Komponente aufweisen [zwa13, 3].
Auf der Anwendungsebene werden Informationen übertragen, die von der Z-Wave Komponente verarbeitet werden. Die Kopfdaten, auch Header genannt, am Anfang des Paketes legen fest, ob dieses Paket an eine oder mehrere Adressen geschickt wurde. Der Kommandotyp, auch als Command Class bezeichnet, enthält Informationen, welche Kommandos in dem Paket übertragen werden. Informationen über Kommando-Klassen und Kommandos finden sich auf der Seite des Open-Zwave Projekts.

5.4 Sichere Kommunikation

Durch die Arbeit von Behrang Fouladi und Sahand Ghanoun ist bekannt, wie die sichere Kommunikation bei Z-Wave abläuft. Im nachfolgenden Teil wird beschrieben, welche Erkenntnisse durch ihre Arbeit gewonnen wurden. Die Resultate sind ebenfalls in dem Dokument Security Evaluation of Z-Wave Wireless Protocol nachzulesen.
Tritt eine neue Z-Wave Komponenten einem Z-Wave Netzwerk bei, bei dem sichere Kommunikation eingeschaltet ist, bekommt diese den eingesetzten Netzwerkschlüssel übermittelt. Es können ausschließlich dann Komponenten dem Netzwerk beitreten, wenn dieser Prozess durch den Benutzer angestoßen wurde. Der Netzwerkschlüssel wird nicht im Klartext übertragen, sondern vor dem Senden verschlüsselt. Damit der Empfänger den Netzwerkschlüssel entschlüsseln kann, muss er den Schlüssel, mit dem verschlüsselt wurde, kennen. Bei der Analyse der Firmware wurde der Schlüssel zum Verschlüsseln und Entschlüsseln des Netzwerkschlüssels gefunden. Fouladi und Ghanoun vermerken, dass dies keine besondere Bedrohung darstelle. Dieser Schlüsseltausch findet nur statt, wenn eine neue Komponente dem Netzwerk beitritt.

Der Netzwerkschlüssel (K_n) wird genutzt, um mit AES im Modus ECB einen Paketschlüssel (K_c) sowie einen Authentizitätsschlüssel (K_m) zu generieren.

$$K_c = AES - ECB_{Kn}(Wort_c)$$
$$K_m = AES - ECB_{Kn}(Wort_m)$$

Die Wörter $Wort_m$ und $Wort_c$ sind in der Firmware der Z-Wave Geräte hinterlegt. Nachdem die Z-Wave Zentrale und die Z-Wave Komponente identische Paketschlüssel und Authentizitätsschlüssel erzeugt haben, können sie diese benutzen, um sicher zu kommunizieren.
Die Pakete bei Z-Wave werden im sicheren Modus mit einem Authentizitäts-Code, auch MAC genannt, verschickt. Bei diesem Verfahren wird ein Code erstellt sowie mit dem Authentizitätsschlüssel verschlüsselt. Nur wenn eine Komponente im Besitz des Authentizitätsschlüssels ist, kann sie einen gültigen Code erzeugen, der von einem Empfänger als korrekt erkannt wird. Sollte ein Angreifer ein Paket schicken, bei dem das Paket verändert wurde, kann der Empfänger dies feststellen, indem er den Code mit seinem Authentizitätsschlüssel entschlüsselt und die Parameter aus dem Code mit dem Paket vergleicht. Der Authentizitäts-Code enthält überdies einen 64 Bit langen Zufallswert. Mit diesem einmalig zu verwendenden Zufallswert, auch Nonce genannt, kann ein Empfänger einen Replay Angriff erkennen und das Paket verwerfen. Um die MAC zu erzeugen, dient folgende Formel:

$$MAC = AES - CBCMAC_{Km}(\text{IV,SK + Sid + Eid + L + C})$$

Der 16 Byte lange IV besteht aus zwei Hälften. Die ersten acht Byte sind eine zufällig generierte Zahl. Die restlichen acht Byte sind der Wert des Nonce. Den Wert SK stellen die Kopf-Informationen zu dem Paket dar. Dieser legt fest, wie das Paket zu interpretieren ist. Folgende Werte sind möglich: 0x40 Nonce Anfrage, 0x80 Nonce Antwort und 0x81 verschlüsselte Nutzlast. Die Sid und Eid sind die Node-ID der jeweiligen Sender beziehungsweise Empfänger. Der Parameter L hat den Wert der Länge der verschlüsselten Nutzdaten. Der Wer C steht für die verschlüsselten Nutzdaten. Um die Nutzdaten zu verschlüsseln, findet das Verfahren AES im Modus OFB Verwendung. Die Nutzdaten werden mit folgender Formel verschlüsselt:

$$C = AES - OFB_{Kc}(IV, Nutzdaten)$$

Zusammengefasst, läuft die sichere Kommunikation bei Z-Wave wie folgt ab. Die Zentrale möchte einen Befehl an eine Z-Wave Komponenten senden. Da sie für die sichere

Kommunikation eine Nonce benötigt, sendet sie an die Z-Wave Komponenten eine Anfrage bezüglich einer Nonce. Die Z-Wave Komponente generiert dies und merkt sich das Nonce und sendet es an die Zentrale. Das Nonce wird eingesetzt um einen IV zu erzeugen. Mit dem Paketschlüssel und dem IV wird der Befehl verschlüsselt. Der verschlüsselte Befehl wird, zusammen mit weiteren Parametern, mit dem Authentizitätsschlüssel verschlüsselt, um den MAC zu erzeugen. Die Zentrale sendet den verschlüsselten Befehl und den MAC an die Z-Wave Komponente.
Die Informationen zum Ablauf der sicheren Kommunikation stammen von Fouladi und Ghanoun und sind in ihrer Arbeit Security Evaluation of Z-Wave Wireless Protocol nachzulesen. Fouladi und Ghanoun haben ihre Erkenntnisse zur sicheren Kommunikation bei Z-Wave genutzt und die Kommunikation auf Sicherheitslücken untersucht.

5.5 Schlüssel Reset Problem

In der Arbeit Security Evaluation of Z-Wave Wireless Protocol berichten Fouladi und Ghanoun, dass sie eine Schwachstelle in der sicheren Kommunikation bei Z-Wave gefunden haben. In diesem Kapitel werden ihre Erkenntnisse erörtert.
Bei der sicheren Kommunikation mit dem Z-Wave Protokoll werden die Nachrichten mit einem geheimen Schlüssel verschlüsselt und authentifiziert. Z-Wave Komponenten, die einen Netzwerkschlüssel erhalten und diesen zum Generieren des Paketschlüssel und Authentizitätsschlüssels genutzt haben, sollten ausschließlich diese Schlüssel für sichere Kommunikation nutzen. Die Sicherheitsforscher haben bei ihrem Test ein Türschloss verwendet, welches sich mit Z-Wave Kommandos ver- und entriegeln lässt. Die Kommunikation des Schlosses war mit den Z-Wave Sicherheitsmaßnahmen abgesichert. Allerdings war die Firmware des Schlosses für einen Schlüssel Reset Angriff anfällig. Mit einer selbst geschriebenen Software gelang es, einen neuen Schlüsseltausch durchzuführen. Dafür wurde dem Schloss die Nachricht geschickt, dass es einen Netzwerkschlüssel geschickt bekommt. Das Schloss hat diesen Befehl befolgt und aus dem neuen Netzwerkschlüssel einen neuen Paketschlüssel und Authentizitätsschlüssel generiert. Dementsprechend waren sie in der Lage, das Schloss mit einem neu gesetzten Netzwerkschlüssel zu kontrollieren.
Vor der Veröffentlichung ihrer Arbeit haben sich Fouladi und Ghanoun an den Hersteller und Sigma Designs gewandt. Der Hersteller des Schlosses antwortete und gab an, eine Sicherheitsüberprüfung durchzuführen. Sigma Designs meldete, dass sie in Zukunft das Schlüssel Reset Problem bei den Sicherheitstests überprüfen, wenn ein Gerät sich zertifizieren lässt.

5.6 Sicherheitsziele

Hier wird beschrieben, ob die in 2.1 definierten Sicherheitsziele erfüllt werden.

Das Z-Wave Protokoll bietet die Möglichkeit, vertraulich zu kommunizieren. Die übertragenen Pakete enthalten Informationen wie Home-ID und Node-IDs im Klartext. Die Nutzdaten sind mit AES-128 verschlüsselt. Ein Angreifer hat zwar die Möglichkeit, Informationen über das Netzwerk zu gewinnen, allerdings sind Kommandos und Parameter, wie zum Beispiel Verbrauch einer Steckdose, in den Nutzdaten verschlüsselt.

Die Integrität der Pakete bei Z-Wave ist durch eine Prüfsumme in jedem Paket gegeben. Bei der sicheren Kommunikation werden außerdem Informationen wie Absenderadresse, Empfängeradresse und der Befehl mit einem MAC gesichert. Dies gewährleistet, dass nur sichere Kommandos geschickt werden können, wenn der Sender im Besitz der Netzwerkschlüssel ist.

Zur Authentifizierung schicken die Z-Wave Komponenten ihre Node-ID als Absenderadresse mit. Gelangt sichere Kommunikation zum Einsatz, wird mit dem MAC gewährleistet, dass die Absenderadresse nicht verändert wurde. Dies schützt allerdings nicht davor, dass eine Komponente, die den Netzwerkschlüssel kennt, eine Nachricht schickt sowie die Absenderadresse fälscht.

Das Z-Wave Protokoll kommuniziert per Funk in Deutschland auf der Frequenz 868,42 MHz. Sollte die Frequenz belegt oder gestört sein, können die Z-Wave Komponenten nicht kommunizieren.

5.7 Ergebnis

Das Z-Wave Protokoll setzt eine sichere Verschlüsselung für die Übertragung der Nutzdaten ein. Die Z-Wave Komponenten können überprüfen, ob die Integrität einer Nachricht verletzt wurde. Durch diese Vorkehrungen lässt sich ein Z-Wave Netzwerk sicher betreiben. Das Schlüssel Reset Problem wäre möglicherweise früher entdeckt und geschlossen worden, hätte sich Sigma Designs dazu entschieden, Informationen über die Protokoll Spezifizierung zu veröffentlichen. Bei den hier untersuchten Z-Wave Komponenten war nicht festzustellen, ob die Kommunikation mit den gegebenen Sicherheitsmaßnahmen gesichert ist. Ein Anwender kann sich lediglich darauf verlassen, dass die Sicherheitsmechanismen wie beschrieben auch Einsatz finden.

6 KNX

Der weltweit verbreite Standard KNX stellt einen offenen Standard für Gebäude und Heimautomatisierung dar. Durch den Zusammenschluss der drei führenden Herstellern für Gebäude und Heimautomatisierung, BatiBUS Club International, European Installation Bus Association und European Home Systems Association, entstand die KNX Association [KNX13, 4]. Der Name KNX stammt von dem ursprünglichen Namen Konnex ab [KNX07, 1]. Der Name Konnex stammt vermutlich von dem lateinischen Wort conexus, deutsch: Verknüpfung, ab. Bei KNX gibt es vier verschiedene Systeme der Kommunikation. Für KNX-TP müssen die KNX Komponenten miteinander verkabelt werden, damit sie kommunizieren können. TP ist die Abkürzung für Twisted Pair, deutsch: verdrehtes Kabel. Bei dieser Lösung erfolgt die Übertragung von Daten und Strom über die Verkabelung. Bei KNX-PL wird die existierende Stromverkabelung genutzt. Daten und Strom werden über das Stromnetz übertragen. PL steht für Power Line, deutsch: Stromleitung. KNXnet/IP verwendet für die Kommunikation ein IP-Netzwerk. Dies bietet die Möglichkeit, dass eine bereits existierende Netzwerkstruktur für die Kommunikation Verwendung finden kann. Für KNX-RF müssen die Komponenten nicht per Kabel verbunden werden. Die Kommunikation findet per Funk auf der Frequenz 868,3 MHz statt. RF steht für Radio Frequency, deutsch: Funkfrequenz. [KNX13, 7]. In diesem Kapitel wird überprüft, ob beziehungsweise welche Sicherheitsmechanismen bei KNX-RF zum Einsatz gelangen. Hierfür erfolgt ein Versuch, bei dem die Kommunikation untersucht wird.

6.1 Aufbau

Die Kommunikation der KNX Komponenten wird in einem selbst durchgeführten Versuch, mit einer KNX Steckdose und einer KNX Fernbedienung, untersucht. Für diesen Versuch wird die Fernbedienung der Firma Becker und eine Steckdose der Firma Siemens verwendet. Das Modell und die Produktbeschreibung sind in Tabelle 5 ersichtlich. Auf der Steckdose befindet sich ein Knopf, mit dem die Steckdose ein- beziehungsweise

	Bezeichnung	Modell
Steckdose	Siemens Steckdosenschalter	wave S 564
Fernbedienung	Becker B-Tronic EasyControl	EC5415B

Tabelle 5: KNX Komponenten

ausgeschaltet wird. Zudem gibt es auf der Steckdose eine LED. Diese leuchtet, sobald die Steckdose eingeschaltet wird beziehungsweise leuchtet nicht, wenn sie ausgeschaltet wird.

Die Fernbedienung kann für die Steuerung unterschiedlicher KNX Anwendungen, wie etwa Rollladen, Dimmer oder Schalter, genutzt werden. Das Display zeigt an, in welchem KNX Anwendungsmodus sie sich gerade befindet. Nach dem Einlegen der Batterien, zeigt die Fernbedienung an, dass sie sich im Modus Rollladen befindet. Durch Drücken und gedrückt Halten der Umschalt- und Einlerntaste wechselt die Fernbedienung durch die verschieden Modi. Dies wird so oft wiederholt, bis sie im Modus Schalter ist. Die Steckdose und Fernbedienung sind einsatzbereit und die Steckdose kann mit der Fernbedienung angelernt werden.

6.2 Gerät anlernen

Damit die Steckdose Befehle von der Fernbedienung verarbeitet, muss die Steckdose mit der Fernbedienung verbunden werden. Bei KNX wird dieser Prozess als binding bezeichnet. Zum Aktivieren des Anlern-Modus bei der Steckdose zu aktivieren, wird für mindestens zehn Sekunden der Knopf auf der Steckdose gedrückt. Dieser Anlern-Modus wird in der Anleitung als Easy Mode bezeichnet. Die Steckdose muss dafür nicht ausgeschaltet sein, das Anlernen kann auch aktiviert werden, wenn die Steckdose angeschaltet ist. Nach etwa zehn Sekunden beginnt die LED auf der Steckdose zu blinken, um zu signalisieren, dass sie sich im Anlern-Modus befindet. Sollten für mehr als zwei Minuten keine KNX Nachrichten[1] zum Anlernen eingehen, beendet die Steckdose den Anlern-Modus. Um eine KNX Nachricht zum Anlernen zu senden, wird auf der Fernbedienung die Anlern-Taste gedrückt. Die Status LED auf der Fernbedienung zeigt durch schnelles orangefarbenes Blinken an, dass eine Anlern-Nachricht gesendet wurde. Sobald die Steckdose diese empfängt, blinkt die LED auf der Steckdose mehrmals, um anzuzeigen, dass sie eine Anlern-Nachricht empfangen hat. Das erfolgreiche Anlernen wird mit grünem Blinken der Status LED auf der Fernbedienung abgeschlossen.

6.3 Herstellerangaben laut Dokumentation

Auf der Website des Herstellers Beckers wird zum Thema Sicherheit erwähnt, dass ein KNX System dazu beiträgt, die Sicherheit zu erhöhen. Durch Anwesenheitssimulation und beispielsweise Steuern der der Rollladen sollen Einbrecher abgeschreckt werden [KNXa]. Der Hersteller tätigt keine Angaben, ob die KNX-RF Komponenten Sicherheitsmechanismen einsetzen.
Die Website der KNX Organisation gibt Informationen über die eingesetzten Sicherheitsmechanismen bei KNX. Es wird beschrieben, dass KNX Data Security unabhängig

[1] Bei KNX werden Nachrichten als Telegramm bezeichnet.

von jedem KNX-Medium zur Nutzung gelangen kann [KNX15, 6]. Data Security bedeutet in diesem Zusammenhang, dass die Datenintegrität und Vertraulichkeit sichergestellt sein sollen.

6.4 Konfigurationsmodus

Der KNX Standard eignet sich für unterschiedlich große Installationen. Für kleine und einfache Installationen, beziehungsweise große und komplexe Installationen existieren zwei verschiedene Konfigurationsmöglichkeiten. Der E-Mode, auch Easy Mode genannt, wird verwendet, wenn für die Konfiguration kein PC mit spezieller Software Einsatz finden soll. In diesem Fall erfolgt die Konfiguration durch das manuelle Verbinden zwischen Sendern und Empfängern. Für größere und komplexere System, bei denen mehrere Komponenten zum Einsatz kommen, ist dies jedoch sehr aufwendig beziehungsweise gar nicht realisierbar. Wird das System zu einem späteren Zeitpunkt erweitert, besteht die Möglichkeit, das System im S-Mode zu betreiben. Der S-Mode, auch System Mode genannt, bietet die Möglichkeit, die KNX Komponenten mit einer Konfigurationssoftware, der sogenannten Engineering Tool Software (ETS), zu konfigurieren. Dies ermöglicht nicht nur die Konfiguration und das Verbinden der KNX-Komponenten, es bietet ebenso die Programmteile zur Diagnose, Fehlersuche und dem Einbinden von Softwareerweiterungen [KNXc, 17]. Der Preis für eine ETS Lizenz für mehr als 20 KNX-Komponenten liegt bei 1000,00 und richtet sich an die Dienstleister, die bei der Einrichtung der KNX-Komponenten unterstützen.

6.5 Kommunikation mithören

Um die Kommunikation zwischen der Steckdose und der Fernbedienung mitzuhören, findet ein USB Stick mit einem RC1180-KNX2 Chip von Radiocrafts Verwendung. Zum Interpretieren der Nachrichten wird das Programm KNX-DEMO Version 1.03 (KNX2) aus der Softwaresammlung RCTools-KNX genutzt. Die Steckdose ist bereits eingeschaltet und auf der Fernbedienung wird der Knopf zum Ausschalten der Steckdose gedrückt. Das Betätigen der Taste AUS sendet folgende Nachricht:

```
12 44 FF 0E 00 6E 80 00 02 41 00 05 FF 00 97 E4 00 80 45
```

Wie diese Nachricht zu interpretieren ist, stellt Tabelle 6 dar [KNXd].

Das erste Byte gibt die Länge der Nachricht an. Der Wert des zweiten Bytes beschreibt das C-Feld, welches bei KNX-RF stets den Wert 0x44 aufweist. Dies kommt daher, dass

Byte	Bezeichnung	Hex	Beschreibung
1	Länge	12	18
2	C-Feld	44	
3	ESC-Feld	FF	
4	Kontrollfeld	0E	
5-10	Seriennummer/Domain Adresse	00 6E 80 00 02 41	
11	Kontrollfeld	00	
12,13	Sender	05 FF	
14,15	Empfänger	00 97	
16	L/NPCI	E4	
17	TPCI	00	
18	APCI	80	Steckdose AUS
19	RSSI	45	

Tabelle 6: Interpretation KNX Nachricht

KNX-RF auf dem Standard IEC-60780-5 basiert [GR15, 168]. Der Wert für das ESC-Feld in Byte drei ist bei KNX-RF ebenfalls immer gleich, und zwar 0xFF. Dieses Feld dient dem Unterscheiden zwischen KNX-RF und Metering [KNXd]. Byte fünf bis zehn enthalten die Seriennummer beziehungsweise Domain Adresse des Senders. Der Wert des Kontrollfeld an Position 11 dient zum Bestimmen, ob es sich um eine Standard- oder eine erweiterte Nachricht handelt. In Byte 12 und 13 ist die Absenderadresse enthalten. Da die Seriennummer einmalig genug ist, hat die Absenderadresse bei KNX-RF stets den Wert `05 FF` [wir07, 20]. Die Empfängeradresse befindet sich in Byte 14 und 15. Feld 16 enthält die Link/Network Protocol Control Information (L/NPCI) sowie Informationen über die Art der Adresse und Informationen zum Routing der Nachricht [KNXe, 8]. Die Layer Protocol Control Information (TPCI) in Byte 17 ist bei KNX-RF immer 0x00. Dieses Feld wird bei KNX-TP und KNX-PL für Managementzwecke genutzt, welche nicht für KNX-RF vorgesehen sind [KNX07, 3]. Der Befehl für die Steckdose steht in Byte 18, welches die Application Layer Protocol Control Information (APCI) enthält. Den letzten Wert in Byte 19 stellt die Received Signal Strength Information (RSSI) dar. Diese beschreibt die Signalstärke beim Empfang der Nachricht.

6.6 Befehle senden

In diesem Abschnitt wird eine Nachricht erstellt und gesendet, um zu testen, ob sich die Steckdose mit einer selbst erstellten Nachricht schalten lässt. Die in Absatz 6.5 mitgehörte Nachricht enthält die Seriennummer und Empfänger-Adresse, diese werden benötigt, um eine eigene Nachricht zu erstellen. Das Programm KNX-DEMO wird gestartet und mit dem KNX Chip RC1180-KNX2 verbunden. Damit die selbst generierten Nachrichten die gleiche Seriennummer wie die Fernbedienung haben, wird in dem Programm

eingestellt, dass der KNX Chip über die Seriennummer `00 6E 80 00 02 41` verfügt. Als Absenderadresse wird `05 FF` und als Empfängeradresse `00 97` eingestellt. Für die L/NPCI wird der Wert `E4` aus der mitgehörten Nachricht eingetragen. Die Steckdose ist ausgeschaltet, um sie einzuschalten, wird der APCI auf 0x81 gesetzt. Das Paket wird gesendet und die Steckdose schaltet sich ein. Zur Überprüfung, ob sich die Steckdose wieder abschalten lässt, wird die APCI auf 0x80 gesetzt. Nach dem Senden dieser Nachricht schaltete sich die Steckdose ab. Somit ist es möglich, nachdem eine Nachricht zwischen Steckdose und Fernbedienung abgehört wurde, selbst Nachrichten zu erstellen und die Steckdose zu steuern.

6.7 KNX Data Security

Der oben beschriebene Versuch erfolgte im E-Mode. Bei diesem Konfigurationsmodus gibt es keine Möglichkeit, Sicherheitsmethoden zu konfigurieren. Anfang 2016 wird ETS in Version 5.5 veröffentlicht. Ab dieser Version wird es möglich sein, Sicherheitsmethoden, bei KNX wird dies KNX Data Security genannt, zu konfigurieren und zwar unabhängig vom dem eingesetzten KNX-Medium [KNX15, 6].
KNX Data Security kann die Kommunikation absichern, indem die Nachrichten authentifiziert oder authentifiziert und verschlüsselt werden. Hierfür findet das Verschlüsselungsverfahren AES im Modus CCM mit einem 128 Bit Schlüssel Einsatz. Wird das System so konfiguriert, dass die Nachrichten lediglich authentifiziert werden, sind sie nicht gegen Abhören geschützt. Vor dem Senden erzeugt eine KNX-Komponente eine Prüfsumme der Nachricht und verschlüsselt diese. Die verschlüsselte Prüfsumme, auch Authentifizierungscode genannt, wird mit übertragen. Nachdem der Empfänger die Nachricht erhalten hat, erstellt er eine Prüfsumme der Nachricht und entschlüsselt den Authentifizierungscode. Sind Prüfsumme und entschlüsselter Authentifizierungscode gleich, ist gewährleistet, dass die Nachricht nicht verändert wurde und vom vorgegebenen Absender stammt. Da die Nachricht eine Sequenznummer enthält, ist sichergestellt, dass die Nachricht nicht wiederholt gesendet wurde, beziehungsweise kann der Empfänger dies feststellen. Ist bei KNX Data Security eingestellt, dass die Nachrichten authentifiziert und verschlüsselt werden, wird vor dem Senden die Nutzlast der Nachricht verschlüsselt. Die Authentizität ist, wie bereits erörtert, auch sichergestellt. Dies stellt sicher, dass ein Angreifer nur sehr wenige Informationen über die gesendeten Daten erhält.
Die KNX-Komponenten werden mit einem einmaligen gerätespezifischen Schlüssel ausgeliefert. Bei der Konfiguration mit der ETS wird der gerätespezifische Schlüssel für diese KNX Komponente hinterlegt. Die ETS erzeugt einen projektspezifischen Schlüssel. Bevor dieser an die KNX-Komponente übertragen wird, verschlüsselt die ETS den

projektspezifischen Schlüssel mit dem gerätespezifischen Schlüssel. Folglich wird weder der projektspezifische noch der gerätespezifischen Schlüssel im Klartext übertragen. Der gerätespezifische Schlüssel ist bereits in der KNX-Komponente hinterlegt, somit kann sie den projektspezifischen Schlüssel entschlüsseln. Sobald eine KNX Komponente einen projektspezifischen Schlüssel erhalten hat, akzeptiert sie nur noch diesen, wenn sie mit der ETS kommuniziert. Der gerätespezifischen Schlüssel wird nicht mehr akzeptiert. Um die Kommunikation zwischen den KNX-Komponenten zu schützen, wird diese mit einem Kommunikationsschlüssel geschützt. Es werden so viele Kommunikationsschlüssel erzeugt wie nötig. Diese werden mit dem projektspezifischen Schlüssel verschlüsselt und an die KNX-Komponenten übertragen. Dies stellt sicher, dass die Kommunikationsschlüssel nicht im Klartext übertragen wird [KNX15, 7].

6.8 Sicherheitsziele

Hier wird beschrieben, ob die in 2.1 definierten Sicherheitsziele bei KNX-RF erfüllt werden.

Die Nachrichten bei KNX-RF im E-Modus werden ungeschützt übertragen, sodass jeder in Reichweite Nachrichten mithören und interpretieren kann. Der Inhalt der Nachricht ist dementsprechend nicht vertraulich. Durch das Mithören der Nachrichten können Rückschlüsse auf Anwesenheit und sogar auf Gebrauch der einzelnen Geräte gezogen werden. Zudem kann ein Angreifer, aus den nicht verschlüsselten Nachrichten, Adressen und Seriennummern der eingesetzten KNX-RF Komponenten gewinnen. Im S-Modus ist es möglich, die Nutzlast der Nachricht zu verschlüsseln. Somit ist ein Teil der Nachricht vertraulich.

Die Nachrichten bei KNX-RF werden in zwei Blöcke geteilt und jeder Block erhält eine Prüfsumme. Dies ermöglicht es einem Empfänger, festzustellen, ob die Integrität einer Nachricht verletzt wurde. Dies schützt allerdings nur vor Übertragungsfehlern. Die Prüfsumme ist nicht geschützt beziehungsweise mit keinem Merkmal versehen, dass ausschließlich Sender und Empfänger kennen. Sollte ein Angreifer eine Nachricht abgefangen und verändert haben, kann er selbst eine Prüfsumme erstellen sowie Integrität vortäuschen. Der E-Modus bietet keine Möglichkeit, die Integrität der Nachrichten sicherzustellen. Beim S-Modus ist es möglich, einen Authentifizierungscode mit zu übertragen. Dieser kann lediglich vom tatsächlichen Sender erzeugt werden. Sollte ein Angreifer die Nachricht mithören und verändern, kann er keinen neuen gültigen Authentifizierungscode erzeugen.

KNX-RF im E-Modus bietet keine Möglichkeit zur Authentifizierung. Um eine eigene Nachricht zu erstellen, benötigt ein Angreifer die Seriennummer und Empfängeradresse,

welche er aus unverschlüsselten Nachrichten gewinnen kann. Somit hat ein Empfänger keine Möglichkeit, um zu überprüfen, ob eine Nachricht von einem Sender stammt. Die Authentizität im S-Modus wird durch den Authentifizierungscode sichergestellt.

Es existieren zwei Arten von KNX-RF. Bei KNX-RF ready steht nur ein Kanal zur Verfügung. Bei KNX-RF multi stehen drei schnelle sowie zwei langsame Kanäle zur Verfügung. Beide Arten funken im Bereich der Frequenz 868 MHz. Sollte ein Kanal gestört oder belegt sein, können Nachrichten nicht übertragen werden. Bei KNX-RF multi könnte in diesem Fall der Kanal gewechselt werden.

6.9 Ergebnis

Betreibt ein Anwender sein System im E-Modus, bietet KNX keine Möglichkeit, dies zu schützen. Ein Angreifer hat die Möglichkeit, unbefugt Geräte zu kontrollieren sowie die unverschlüsselte Kommunikation auszuwerten. KNX im S-Modus ermöglicht eine authentische beziehungsweise authentische und verschlüsselte Kommunikation. Durch die Vergabe gerätespezifischer Schlüssel durch die KNX Hersteller ist sichergestellt, dass der Schlüsseltausch beim Einrichten der Geräte gegen Abhören gesichert ist. Dies setzt allerdings voraus, dass der gerätespezifische Schlüssel zufällig erzeugt wird.

Ob die Hersteller den Data Security Standard der KNX Association korrekt implementiert haben, lässt sich erst überprüfen, wenn die Hersteller KNX-RF Komponenten auf den Markt bringen, die Data Security unterstützen.

7 FS20

Der Begriff FS20 stellt den Oberbegriff für Komponenten in der Heimautomatisierung dar, welche mit dem Funkprotokoll FS20 kommunizieren. Die Produktpalette umfasst eine Vielzahl von Komponenten, die für die unterschiedlichsten Einsatzmöglichkeiten bestimmt sind. Es existieren beispielsweise Regen- und Temperatursensoren, die Daten über die Umwelt sammeln. Diese Daten können ausgewertet und aufgrund dessen Rollladen oder Licht beziehungsweise Strom gesteuert werden. Die Produkte wurden von der Firma eQ-3 entwickelt. Auf der Website des Herstellers wird angegeben, dass trotz des Erfolgs von HomeMatic nicht geplant sei, FS20 einzustellen. Die FS20 Komponenten sollen weiterhin unterstützt werden und selbst zehn Jahre alte FS20 Komponenten werden mit aktuellen FS20 Komponenten kombinierbar sein [fs2c].
Ein Onlinehändler hat auf seiner Website veröffentlicht, dass eQ-3 ab dem 01.11.2015 den Vertrieb von FS20 im Fachhandel abgekündigt. Die FS20 Komponenten können ab diesem Datum nur noch von einem Tochterunternehmen der eQ-3 bezogen werden [FS2b]. In diesem Kapitel gelangt die Kommunikation der FS20 Komponenten zur Untersuchung und es wird überprüft, welche Sicherheitsmechanismen bei FS20 Komponenten vorhanden sind.

7.1 Herstellerangaben laut Dokumentation

In der mitgelieferten Bedienungsanleitung gibt es keine Informationen über die Sicherheitsmechanismen der FS20 Komponenten. Es wird nicht beschrieben, wie die Kommunikation zwischen den Komponenten abläuft. Ein Benutzer erhält dort keine Informationen darüber, ob die Geräte sicher kommunizieren beziehungsweise ob jene Daten, welche von den FS20 Komponenten gesendet werden, gegen Abhören oder Veränderung geschützt sind.
Auf der Website des Lieferanten, bei dem es sich um ein Tochterunternehmen des Herstellers handelt, gibt es Informationen zu Einsatzmöglichkeiten von FS20 Komponenten. Dort wird auch Sicherheit genannt, jedoch beziehen sich diese Informationen auf das Schalten von Steckdosen und Licht, um Anwesenheit zu simulieren und somit potenzielle Einbrecher abzuschrecken. Es wird nicht beschrieben, welche Sicherheitsmechanismen Einsatz finden, um FS20 abzusichern [FS2d].
Ein Benutzer erhält weder in der Bedienungsanleitung noch auf der Website des Herstellers und Lieferanten Informationen darüber, wie die FS220 Komponenten geschützt sind. Im Internet finden sich mehrere Foren, die das Thema Sicherheit bei FS20 behandeln. In den Foren wird darüber gesprochen, dass bei FS20 keine Sicherheitsmechanismen eingesetzt werden [fs215].

7.2 Aufbau

Um zu überprüfen, wie die FS20 Komponenten kommunizieren, wurde eine Umgebung mit zwei FS20 Komponenten aufgebaut. Bei den Komponenten für diesen Aufbau handelt es sich um einen Handsender, im Weiteren als Fernbedienung bezeichnet, sowie eine Funkschaltdose, im Folgenden Steckdose genannt. Das Modell und die Produktbeschreibung sind in Tabelle 7 ersichtlich. Die Fernbedienung dient zum Schalten von

	Bezeichnung	Modell
Fernbedienung	FS20 Handsender	FS20 S4
Steckdose	FS20 Funkschaltdose	FS20 ST-4

Tabelle 7: FS20 Komponenten

bis zu zwei Aktoren. Nach dem Einlegen der Batterie ist die Fernbedienung einsatzbereit. Eine weitere Einrichtung der Fernbedienung ist nicht notwendig. Als Aktor dient die Steckdose. Diese wird nach dem Auspacken an einen Stromkreis angeschlossen. Damit sie Nachrichten verarbeitet, muss die Steckdose noch mit der Fernbedienung gepairt werden.
Nachdem die Steckdose sich mit der Fernbedienung schalten lässt, wird die Kommunikation untersucht. Dabei ist festzustellen, ob die Kommunikation geschützt ist beziehungsweise welche Sicherheitsmaßnahmen der Hersteller bietet, um sie zu schützen.

7.3 Gerät anlernen

Die Steckdose reagiert erst auf Kommandos, nachdem eine Adresse aus dem FS20 Adressschema programmiert wurde. Zum Programmieren einer Adresse muss die Steckdose in den Anlernmodus beziehungsweise Programmier-Modus versetzt werden. Um die Steckdose in den Programmier-Modus zu versetzen, muss die Bedientaste auf der Steckdose für mindestens fünf Sekunden lang gedrückt werden. Sobald die Kontroll-Leuchte zu blinken beginnt, befindet sich die Steckdose im Programmier-Modus. In diesem Modus verarbeitet die Steckdose jede FS20 Nachricht und speichert die Adresse aus der Nachricht. Damit die Steckdose die Nachrichten der Fernbedienung verarbeitet, muss die Adresse der Fernbedienung in der Steckdose programmiert werden. Die Fernbedienung muss in keinen Anlernmodus geschaltet werden. Durch das Betätigen einer der Bedientasten auf der Fernbedienung sendet diese eine Nachricht aus. Die Steckdose empfängt die Nachricht und speichert die Adresse aus dieser Nachricht. Das Anlernen ist abgeschlossen. Sobald ein Sender eine Nachricht mit dieser Adresse und einem Befehl sendet, wird dieser von der Steckdose verarbeitet. Wird der Knopf zum Einschalten auf der Fernbedienung gedrückt, sendet die Fernbedienung eine Einschaltnachricht mit ihrer

Adresse aus. Die Steckdose empfängt diese Nachricht. Da die Adresse der Fernbedienung beim Anlernvorgang programmiert wurde, verarbeitet die Steckdose den Befehl.

7.4 Kommunikation mithören

Um zu überprüfen, wie die Kommunikation abläuft, wurde diese aufgezeichnet und ausgewertet. Die FS20 Komponenten kommunizieren auf der Funkfrequenz 868,35 MHz. Mit einem CC1101 USB Lite (CUL) ist es möglich, den Funkverkehr der FS20 Komponenten auf diese Frequenz mitzuhören. Nach dem Pairen der Steckdose mit der Fernbedienung kann diese mit der Bedientaste AN und AUS gesteuert werden. Mit dem Betätigen der AN beziehungsweise AUS Bedientaste sendet die Fernbedienung jedes Mal eine Nachricht. Das Betätigen der Taste AUS sendet folgende Nachricht:

```
F30DA0100
```

Wie diese Nachricht zu interpretieren ist, zeigt 8.

Byte	Bezeichnung	Hex	Beschreibung
1	Kommando	F	FS20
2,3,4	Empfänger	30 DA 01	1411 4233 1112
5	Befehl	00	Steckdose AUS

Tabelle 8: Interpretation FS20 Nachricht

Diese Nachricht enthält die Hexadezimal-Empfänger Adresse sowie einen Befehl. Die Empfänger-Adresse soll sicherstellen, dass der Befehl nur von FS20 Komponenten ausgeführt wird, die diese Adresse programmiert haben. Die Empfänger Adresse setzt sich aus einem Haus- und Gerätecode zusammen (Siehe Adressschema 7.6). FS20 Komponenten geben keine Rückmeldung darüber, dass ein Befehl verarbeitet wurde. Es wird keine Bestätigung geschickt wie bei anderen Protokollen (Siehe HomeMatic 8). Ist die Übertragung gestört und der Empfänger kann die Nachricht nicht empfangen, kann dies der Sender nicht ohne Weiteres feststellen.

7.5 Befehle senden

Nach dem Mithören des FS20 Funkverkehrs (siehe Kommunikation mithören 7.4) ist die Empfängeradresse der Steckdose bekannt. Da es keine Zähler, Zeitstempel oder Absenderadressen in den Nachrichten bei FS20 gibt, genügt dies, um die Steckdose zu kontrollieren. Zur Überprüfung dieser Theorie wurde die Steckdose ausgeschaltet und mit

dem CUL die Nachricht `F30da0111` gesendet. Diese Nachricht inkludiert die Empfängeradresse `F30da01` und wird von der Steckdose verarbeitet. Die letzten beiden Ziffern `11` werden von der Steckdose als Befehl, sich einzuschalten, interpretiert. Direkt nach dem Senden dieser Nachricht schaltet sich die Steckdose ein. Wird dieselbe Nachricht `F30da0111` erneut gesendet, gibt es keine Reaktion, da die Steckdose bereits eingeschaltet ist. Erst nachdem die Nachricht `F30da0100` zum Ausschalten der Steckdose gesendet wird, schaltet sich die Steckdose ab.

7.6 Adressschema und Protokoll

Eine FS20 Komponenten Adresse besteht aus 3 Bytes und wird mit hexadezimalen Ziffern dargestellt. Bei diesem Versuch wurde die Empfänger Adresse `30 DA 01` mitgehört. Die Dokumentation des Herstellers beschreibt in ihren Unterlagen ein quaternär ähnliches Adressformat [fs2a]. Um Adressen zwischen diesen beiden Formaten umzurechnen, kann man die Tabelle 9, welche im FHEM Forum beschrieben wurde, verwenden. In dieser Tabelle steht, wie ein quaternär ähnlicher Wert zu einer hexadezimalen Ziffer umgerechnet werden kann.

11 = 0x0	12 = 0x1	13 = 0x2	14 = 0x3
21 = 0x4	22 = 0x5	23 = 0x6	24 = 0x7
31 = 0x8	32 = 0x9	33 = 0xA	34 = 0xB
41 = 0xC	42 = 0xD	43 = 0xE	44 = 0xF

Tabelle 9: Umrechnung FS20 Adresse [fhe]

.

So wird aus der Hexadezimal-Adresse eine quaternär ähnliche Adresse `1411 4233 1112`. Diese Pseudoquaternäre-Adresse ist 12 Zeichen lang und besteht aus den Ziffern 1 bis 4. Die ersten acht Stellen sind der Haus Code `1411 4233`. Gemäß Herstellerangaben ist es mit unterschiedlichen Hauscodes möglich, mehrere FS20 Komponenten getrennt voneinander zu kontrollieren. Der Geräte-Code lautet in diesem Fall `1112`. Durch das pseudoquaternäre Adress-Schema ist es möglich, bis zu 256 eindeutige Geräte-Codes beziehungsweise 4096 Haus-Codes zu vergeben. Eine Empfänger-Adresse besteht aus dem Haus- und Gerätecode.

Die FS20 Komponenten benutzen das gleichnamige proprietäre Protokoll FS20. Der Hersteller hat die Spezifizierung des Protokolls nicht veröffentlicht. Mehrere Open Source Projekte für Heimautomatisierung haben die Nachrichten bei FS20 untersucht und unterstützen das FS20 Protokoll. Wie sich die Nachrichten des Protokolls zusammensetzen, ist dem frei zugänglichen Quellcodes des FHEM Projekts zu entnehmen [fhe13a].

7.7 Sicherheitsziele

In diesem Abschnitt wird erörtert, ob die in 2.1 definierten Sicherheitsziele erfüllt werden.

Die Kommunikation bei FS20 ist nicht verschlüsselt und es ist auch nicht vorgesehen, eine Verschlüsselung zu aktivieren. In Funkreichweite der FS20 Komponenten ist es möglich, den Verkehr mitzuhören und auszuwerten. Dies ermöglicht es einem Angreifer, den Haus- und Gerätecode mitzuhören sowie selbst Nachrichten mit Befehlen an die FS20 Komponenten zu senden. Zudem hat ein Angreifer die Möglichkeit, die übertragenen Daten auszuwerten und somit Rückschlüsse auf Anwesenheit und Verhalten der Bewohner zu ziehen.

Die Nachrichten, welche übertragen werden, sind nicht gegen Veränderung geschützt. Ein Angreifer hat somit die Möglichkeit, eine Nachricht mitzuhören und einen Wert darin zu verändern und diese Nachricht erneut zu senden. FS20 bietet einem Empfänger keine Möglichkeit, zu überprüfen, ob die Integrität des Pakets verletzt wurde. Sollte ein Befehl in einer Nachricht von einem Angreifer oder durch Übertragungsfehler verändert worden sein, so wird dieser dennoch ausgeführt.

Das FS20 System biete keine Möglichkeit der Authentifizierung. Die FS20 Komponenten verarbeiten Nachrichten, welche an sie adressiert wurden, ohne zu überprüfen, ob der Absender berechtigt ist. Ein Angreifer kann eine Nachricht mithören und diese erneut senden. Da die mitgehörte Nachricht die Empfänger-Adresse enthält, kann der Angreifer diese Information nutzen, um eine selbst erstellte Nachricht zu senden.

Die FS20 Komponenten kommunizieren per Funk auf der Frequenz 868,35 MHz. Wird diese Frequenz gestört oder ist sie belegt, können die FS20 Komponenten nicht kommunizieren. Ein Wechsel der Frequenz ist nicht möglich. Sollte die Übertragung auf der Frequenz gestört sein, hat ein Anwender keine Möglichkeit, sein FS20 System zu nutzen. Mit der Einführung von LTE bemerkten einige FS20 Benutzer, dass der Empfang gestört wurde [fs2e]. Der Hersteller führte an, dass einige FS20 Komponenten nicht LTE störfest sind. Um dieses Problem zu lösen, mussten die Benutzer die FS20 Komponenten austauschen oder umrüsten.

7.8 Ergebnis

Bei FS20 Komponenten gibt es keine Sicherheitsvorkehrungen, um die Daten vor Unbefugten zu schützen oder unbefugten Zugriff zu verhindern. Der Funkverkehr ist nicht verschlüsselt und somit verfügt jeder in Reichweite des FS20 Systems über die Möglichkeit, die Nachrichten abzufangen. Dies ermöglicht es einem Angreifer, Informationen über das eingesetzte System zu erlangen beziehungsweise Rückschlüsse auf Verhalten und Anwesenheit zu ziehen. Da die FS20 Komponenten keine Authentifizierung einsetzen, ist nicht sichergestellt, dass Nachrichten von befugten Sendern gesendet wurden.

8 HomeMatic

HomeMatic ist der Name, mit dem Komponenten für die Heimautomatisierung der Firma eQ-3 entwickelt und verkauft werden. Die Firma eQ-3 bietet seit 30 Jahren Lösungen für Heimautomatisierung an [hom15]. eQ-3 hat die HomeMatic Komponenten entwickelt und ist Partner für Heimautomatisierungsprodukte bei RWE Smarthome und dem von der Deutschen Telekom initiierten QIVICON. HomeMatic RF verwendet zur Kommunikation das bidirektionale und proprietäre Protokoll BidCoS. In diesem Kapitel erfolgt Untersuchung, wie die Komponenten bei HomeMatic RF kommunizieren beziehungsweise ob es Sicherheitsmechanismen gibt, um die Kommunikation abzusichern.

8.1 Herstellerangaben laut Dokumentation

Der Hersteller gibt an, dass viele der HomeMatic Komponenten eine gesicherte Funkübertragung unterstützen. Für den Einsatz für sicherheitsrelevante Bereiche, wie zum Beispiel HomeMatic KeyMatic, bezeichnet er die gesicherte Funkübertragung als erforderlich. KeyMatic ist der Name für einen Türschlossantrieb. Dieser kann an Türen nachgerüstet werden, um diese per Funk zu ent- beziehungsweise verriegeln. Die gesicherte Verbindung weist den Nachteil auf, dass das Kommunikationsaufkommen dadurch erhöht und die Abarbeitung der Befehle geringfügig verzögert wird. Bei batteriebetriebenen Geräten verringert sich zudem die Lebensdauer der Batterie. Es wird beschrieben, dass für die Sicherung das symmetrische Kryptoverfahren AES genutzt wird. Dieses findet Einsatz, um bei einer gesicherten Funkverbindung zu überprüfen, ob der Sender dazu berechtigt ist, dem Empfänger einen Befehl zu schicken. Berechtigt sind lediglich Sender, die einen korrekten individuellen AES-Sicherheitsschlüssel generiert haben. In dem Handbuch von HomeMatic wird vermerkt, dass eine benutzerdefinierte Vergabe eines Schlüssels für die AES Authentifizierung nicht erforderlich sei, da sämtliche HomeMatic-Komponenten, die eine gesicherte Datenübertragung unterstützen, bereits bei der Auslieferung über einen voreingestellten AES-Sicherheitsschlüssel verfügen. HomeMatic nennt diesen voreingestellten AES-Sicherheitsschlüssel Default-Sicherheitsschlüssel (an anderer Stelle wird er als System-Sicherheitsschlüssels bezeichnet). Es wird empfohlen, diesen Default-Sicherheitsschlüssel zu nutzen. Als Gründe hierfür wird angegeben, dass dieses erlaubt, sein HomeMatic-System mit geringem Aufwand wieder in die Werkseinstellung zurückzusetzen. Sollte der Benutzer einen benutzerdefinierten AES-Sicherheitsschlüssel vergeben haben, muss man jede Komponente einzeln in den Werkszustand versetzen.

8.2 Aufbau

In einem selbst durchgeführten Versuch wird eine Umgebung mit HomeMatic Komponenten aufgebaut. Im Rahmen dessen wird untersucht, welche Sicherheitsmaßnahmen konfiguriert werden können. Hierzu gelangen die Komponenten aus Tabelle 10 zur Verwendung.

	Model	Seriennummer	Firmware Version
Zentrale CCU2	HM-Cen-OTW-x-x-2	LEQ1009574	2.13.7
Funk-Schaltaktor	HM-ES-PMSw1-Pl	LEQ0537221	1.6

Tabelle 10: HomeMatic Komponenten

Die Zentrale wurde an den Strom angeschlossen sowie per USB mit einem Laptop verbunden. Auf der Zentrale befinden sich drei grüne LEDs mit folgenden Beschriftungen: Power, Internet und Info. Die Power LED leuchtet durchgängig, nachdem Strom angeschlossen wurde. Die Internet LED ist nicht aktiv, da die Zentrale nicht an ein Netzwerk angeschlossen wurde. Während des Boot Vorgangs blinkt die Info LED schnell, sobald dieser abgeschlossen ist und die Zentrale bereit ist, blinkt die Info LED langsamer. Sobald die Zentrale per USB mit einem Computer verbunden wird, erkennt der Computer ein CD-Laufwerk. Dieses enthält Treiber, Dokumentation, Lizenzinformationen und eine Installationsdatei. Die Installationsdatei installiert eine USB Netzwerkkarte. Wenn die Zentrale per USB angeschlossen wird und der Treiber installiert ist, erkennt der Computer eine Netzwerkkarte. Die Zentrale weist dieser per DHCP die IP Adresse `10.101.82.52` zu. Auf der Zentrale läuft ebenso ein Web Server, welcher per http unter der Adresse `http://10.101.82.51/` zu erreichen ist.

8.3 Gerät anlernen

Damit die Funksteckdose Befehle von der Zentrale akzeptiert, muss die Zentrale mit der Steckdose gepairt werden. Dies soll gewährleisten, dass die Steckdose nur Befehle von der Zentrale entgegennehmen sollte. Dafür muss in der Oberfläche des Web Interfaces der Button anlernen gedrückt werden. Hierdurch wird die Zentrale für 60 Sekunden in einen Modus versetzt, in dem nach Geräten gesucht wird, die sich ebenfalls im Anlernmodus befinden. Um bei der Steckdose den Anlernmodus zu aktivieren, muss der Knopf auf der Steckdose für 5 Sekunden gedrückt werden. Wenn die Steckdose sich im Anlernmodus befindet, blinkt die LED orange. Bei der Zentrale erscheint die Steckdose als Nachricht im Posteingang und wird mit Betätigen des Fertig Buttons mit der Zentrale gepairt.

Tabelle 11: Interpretation HomeMatic Nachricht

Byte	Bezeichnung	Hex	Beschreibung
1	Kommando	A	AskSin
2	Länge	14	Dezimal = 20 Bytes
3	Zähler	65	Dezimal = 101
4	Flag	84	•
5	Typ	5E	Status Steckdose
6,7,8	Sender	2C0EA8	HomeMatic ID Sender
9,10,11	Empfänger	000000	Broadcast
12-22	Nutzdaten	800002000006000008EF01	•
23	Unbekannt	16	•

8.4 Protokoll

HomeMatic verwendet das Protokoll Bidirectional Communication Standard (BidCoS), welches proprietär und nicht frei verfügbar ist. Das Open Source Project FHEM unterstützt HomeMatic Komponenten und das BidCoS Protokoll. In dem öffentlich zugänglichen Quellcode des FHEM Projekts ist beschrieben, wie sich die Nachrichten des Protokolls zusammensetzen [fhe13b].

8.5 Kommunikation mithören

Sobald die Steckdose an den Strom angeschlossen wurde, wird ca. alle drei Minuten eine Meldung gesendet, die folgendermaßen aussieht:

```
A 14 65 845E 2C0EA8 000000 800002000006000008EF0116
```

Dabei handelt es sich um eine Status Nachricht der Steckdose, um mitzuteilen, wie die aktuellen Sensor-Werte der Steckdose sind. Wie diese Nachricht zu interpretieren ist, steht in Tabelle 11. Die Nachricht enthält neben den Kontrolldaten die Nutzdaten. In Tabelle 12 ist beschrieben, wie diese zu interpretieren sind. Der Vergleich der Werte

Tabelle 12: Interpretation HomeMatic Nutzdaten Statusmeldung Steckdose

Byte	Bezeichnung	Hex	Umrechnung	Ergebnis	Einheit
1,2,3	Energie	800002	$\frac{Hex}{10}$	$\frac{8388610}{10} = 838861$	Wattstunde
4,5,6	Leistung	000006	$\frac{Hex}{100}$	$\frac{6}{100} = 0{,}06$	Watt
7,8	Strom	0000	$\frac{Hex}{1}$	$\frac{0}{1} = 0$	Milliampere
9,10	Spannung	08EF	$\frac{Hex}{10}$	$\frac{2287}{10} = 288{,}7$	Volt
11	Frequenz	01	$\frac{Hex}{100+50}$	$\frac{1}{100+50} = 50{,}01$	Hertz

mit den Werten aus der Status-Seite der Zentrale zeigt, dass diese Interpretation der Nachricht korrekt sein muss. Nur der Wert Wattstunde hat einen anderen Wert als in der Zentrale angezeigt. Der Wert für die untersuchte Nachricht wurde als 1 in der Zentrale angegeben. Zieht man vom ausgerechneten Wert 838860 ab, ist das Ergebnis 1, wie in der Zentrale. Theorie ist, dass der Zähler für Wattstunde bei 838860 beginnt und die Zentrale zieht diesen Wert vor dem Anzeigen ab. Zur Überprüfung dessen wurde die Steckdose vom Strom getrennt und nach ein paar Minuten wieder eingesteckt. Der Wert für Wattstunde begann erneut bei 838861, was darauf hindeutet, dass der Zähler bei 838860 beginnt.

8.6 Befehle senden

Das Web-Interface der Zentrale bietet die Funktion die Steckdose, EIN und AUS zu schalten. Sobald der Knopf für die jeweilige Aktion gedrückt wurde, sendet die Zentrale einen Befehl wie diesen:

```
A 0E 2A A0 11 F11034 2C0EA8 0201C8
```

Wie diese Nachricht zu interpretieren ist, wurde in Tabelle 13 beschrieben. Um selbst einen Schaltbefehl zu senden, wurde die Steckdose wieder ausgeschaltet. Mit einem CUL wurde derselbe Befehl erneut gesendet. Die Steckdose reagierte sofort und schaltete sich ein. Es wäre zu erwarten, dass die Steckdose den Befehl verwirft, da der Zähler nicht mehr korrekt ist - zumal die Steckdose dies auch erkennt, denn sie meldet, dass sie eine Nachricht mit falschem Zähler empfangen hat. Da der Aufbau des Befehls bekannt ist, ist es möglich, den Zähler vor dem Senden hochzuzählen und damit zu verhindern, dass erkannt wird, dass die Nachricht nicht von der Zentrale gesendet wurde. Dies geht nur so lange gut, bis die Zentrale erneut einen Befehl sendet, da der Zähler der Zentrale mit dem Zähler der Steckdose nicht mehr übereinstimmt.

Tabelle 13: Interpretation HomeMatic Befehl senden

Byte	Bezeichnung	Hex	Beschreibung
1	Kommando	A	AskSin
2	Länge	0E	14
3	Zähler	2A	42
4	Flag	A0	160
5	Typ	11	17
6,7,8	Sender	F11034	HomeMatic Sender ID
9,10,11	Empfänger	2C0EA8	HomeMatic Empfänger ID
12,13,14	Nachricht	0201C8	Steckdose EIN

8.7 HomeMatic ID

Zum Senden eines nicht autorisierten Befehls muss die HomeMatic ID des Empfängers sowie dessen gepairten Gerätes, hier der Zentrale, bekannt sein. Im Fall einer falschen HomeMatic Empfänger ID ignoriert die Steckdose den Befehl. Ebenso muss die HomeMatic ID der Zentrale bekannt sein. Ein Befehl mit korrekter HomeMatic Empfänger ID wird lediglich dann akzeptiert, wenn die HomeMatic Sender ID mit der von der Steckdose gepairten ID übereinstimmt. Das Abfangen der Sender und Empfänger ID stellt allerdings keine besondere Herausforderung dar. Die Steckdose sendet regelmäßig ihren Status. Um die HomeMatic ID der Zentrale zu erfahren, genügt es, einen beliebigen Befehl der Zentrale abzufangen. Dies ist jedoch nur möglich, wenn dieser beliebige Befehl von der Zentrale gesendet wurde, die auch mit der Steckdose gepairt wurde. Es ist theoretisch ebenfalls möglich, die HomeMatic ID der Zentrale zu erraten, anstatt sie aus dem Funkverkehr abzuhören. Praktisch ist dies jedoch nicht, eine HomeMatic ID hat sechs Stellen, die alle Werte aus dem Hexadezimalsystem annehmen können. Somit sind 16,7 Millionen verschiedene IDs möglich. Angenommen, ein Angreifer probiert jede Sekunde eine ID aus, so würde es ca. ein halbes Jahr dauern, bis alle IDs durchprobiert wurden.

8.8 Gesicherte Kommunikation

Die Zentrale erlaubt es unter Einstellungen, die Geräte zu konfigurieren. Bei Auswahl der Steckdose werden für die Steckdose und jeden Sensor der Steckdose diverse Einstellmöglichkeiten angeboten. Es ist möglich, den Übertragungsmodus in den Modus „Standard“ oder „Gesichert“ zu schalten. Nach dem Anlernen der Steckdose ist der Modus „Standard“ aktiviert. Zur Untersuchung der gesicherten Kommunikation wurde nun der Modus „Gesichert“ für Leistungssensor ausgewählt. Die Konfiguration der Zentrale zeigt an, dass die Kommunikation jetzt gesichert ist. Um dies zu überprüfen, wurden erneut Pakete von der Steckdose mitgehört. Diese unterscheiden sich, abgesehen von Zähler in der Nachricht, nicht von Nachrichten, die ohne gesicherte Kommunikation geschickt wurden. Die Bezeichnung gesicherte Kommunikation ist irreführend an dieser Stelle. In der Dokumentation wird angeführt, dass es für gesicherte Kommunikation das Challenge-Response-Authentifizierungsverfahren einsetzt. Dabei wird die Kommunikation nicht verschlüsselt und ist für jeden lesbar. Es wird nur sichergestellt, dass lediglich ein Kommunikationspartner mit dem richtigen AES Schlüssel Befehle senden kann. Für Sensoren ist die Bezeichnung nicht korrekt, da die Kommunikation so abläuft, als sei es die nicht gesicherte Kommunikation.

8.9 Gesicherte Befehle

Um zu verhindern, dass Unbefugte Befehle senden, kann der gesicherte Übertragungsmodus aktiviert werden. Nachdem in der Zentrale die gesicherte Kommunikation aktiviert wurde und die Zentrale den Befehl zum Einschalten der Steckdose geschickt hat, konnte der CUL diese Befehle empfangen.

1. A 0E78A011318EC02C0EA80201C80000
2. A 1178A0022C0EA8318EC0044F1E66D0C65B00
3. A 1978A003318EC02C0EA85394CD90BF455F1F066AEB343415028D
4. A 127880022C0EA8318EC00101C8001CBCB0986A

Der Befehl 1) A0E78A011318EC02C0EA80201C80000 enthält die Nachricht 0201C8. Die Zentrale sendet der Steckdose den Befehl, sich einzuschalten. Um zu verifizieren, dass der Befehl von einem berechtigten Sender stammt, sendet die Steckdose den Befehl 2) A1178A0022C0EA8318EC0044F1E66D0C65B00. Die Nachricht aus diesem Befehl lautet 044F1E66D0C65B00. Dies ist die Challenge, welche gelöst werden muss, um zu gewährleisten, dass die Gegenseite berechtigt ist. Die Zentrale wendet eine Funktion an, um die Challenge mit AES zu verschlüsseln. Das Resultat ist die Response, um sich gegenüber der Steckdose zu authentifizieren. Die Nachricht aus dem Befehl 3) ist 5394CD90BF455F1F066AEB343415028D. Dies ist die Response auf die Challenge. Die Steckdose wendet eine Funktion an, um zu prüfen, ob die Response zu der gesendeten Challenge passt. Ist dies der Fall, dann geht die Steckdose davon aus, dass die Gegenseite zum Senden von Befehlen berechtigt gewesen ist, und führt die Aktion aus. Dies bestätigt sie der Zentrale mit dem Befehl 4). Sie sendet ein Acknowledgement (ACK), dass der Befehl verarbeitet wurde, und teilt den Zustand der Steckdose mit. Die Funktion zum Bestimmen der Response zum Senden von Nachricht 3) ist folgendermaßen aufgebaut. Zuerst wird ein temporärer Schlüssel `tS'` erzeugt. Dieser setzt sich aus der Challenge sowie den ersten 12 Zeichen des eingestellten AES Schlüssel zusammen. Die Werte werden mit XOR verknüpft:

```
tS' = XOR(Challenge, aesSchlüssel[0:12])
```

Dies ist der erste Teil des temporären Schlüssels `tS`. Dieser wird mit den restlichen Zeichen des AES Schlüssels ergänzt.

```
tS = tS' + aesSchlüssel[12:]
```

Die hier angewandte Verschlüsselungsmethode ist AES im Modus CBC. Um diese Methode auf einen Text anzuwenden, sind ein Schlüssel und ein IV nötig. Im ersten Schritt findet ein IV Verwendung, der aus 32 Nullen besteht – `IV0`. Die Nachricht, die verschlüsselt wird, besteht aus zwei Teilen. Die ersten 12 Zeichen sind eine Art Zeitstempel, gefolgt von einem Teil des Kommandos, welches zum Schalten der Steckdose gesendet wurde – siehe 1).

```
Nachricht = Zeitstempel + Kommando[2:-8]
Encrypt1 = AES( tS , Nachricht , IV0 )]
```

Der verschlüsselte Text `Encrypt1` wird erneut mit dem Schlüssel `tS` verschlüsselt, allerdings mit einem anderen IV. Dieser IV besteht aus den letzten acht Stellen des Kommandos und wird mit Nullen aufgefüllt.

```
IV = Kommando[-8:]+padLeft(32, 0)
Encrypt2 = AES( tS , Encrypt1, IV )
```

Der verschlüsselte Text `Encrypt2` ist die Response, die von der Steckdose erwartet wird [Ger15].

Erhält die Steckdose ein Schaltkommando, sendet sie eine Challenge aus. Bekommt sie keine Antwort auf die Challenge oder eine Antwort mit falscher Response, reagiert sie nicht auf dieses Kommando. Anstatt einen 128 Bit Schlüssel für das Verschlüsseln zu benutzen, bestehen die ersten 48 Bit aus einem bekannten Text, der zuvor gesendeten Challenge. Der geheime Teil des Schlüssels ist somit nur 80 Bit lang. Dies stellt kein besonderes Sicherheitsrisiko dar. Selbst bei einem 64 Bit Schlüssel würde das Erraten mehrere Jahre dauern, unter der Annahme, es können Millionen verschiedene Schlüssel pro Sekunde ausprobiert werden [sta].

Den Komponenten bei der Heimautomatisierung stehen nur wenige Ressourcen zur Verfügung. Ein Brute-Force Ansatz ist darauf angewiesen, dass die Heimautomatisierungs-Komponenten sehr viele Anfragen pro Sekunde beantworten. Es würde wahrscheinlich daran scheitern, dass nicht genügend Versuche pro Sekunde durchgeführt werden können.

8.10 Problem mit dem Default-Sicherheitsschlüssel

HomeMatic hat einen Default Schlüssel für die AES Verschlüsslung in seinen Geräten hinterlegt. Es ist möglich, diesen mit einem eigenen Schlüssel zu ersetzen, jedoch wird davon in der Dokumentation abgeraten. Wird ein neuer Schlüssel gesetzt, sendet die

Zentrale diesen an ihre gepairten Geräte. Damit Unbefugte diesen neuen Schlüssel nicht abfangen, ist die Übertragung mit AES verschlüsselt. Das Problem diesbezüglich ist, dass dies mit dem Default Schlüssel verschlüsselt ist und dieser Schlüssel bekannt ist. Er wurde im November 2014 im Internet veröffentlicht und ist frei zugänglich [Hom14]. Mit dem Default Schlüssel ist es möglich, den neuen Schlüssel aus dem Verkehr auszulesen.

8.11 System-Sicherheitsschlüssel ersetzen

Der Benutzer hat die Möglichkeit, einen eigenen Sicherheitsschlüssel für die AES Authentifizierung zu setzen. Dafür muss er im Web-Interface Einstellungen öffnen und dort Sicherheit auswählen. Dann wird eine Maske geöffnet, in der ein System-Sicherheitsschlüssel eingegeben werden kann. Es folgt der Hinweis, dass der Schlüssel mindestens fünf Zeichen lang sein muss. Hat der Benutzer den Sicherheitsschlüssel eingegeben und auf Schlüssel übernehmen geklickt, wird dieser mit Message-Digest Algorithm 5 (MD5) gehasht und in der Zentrale gespeichert. Der neue Schlüssel wird per AES verschlüsselt und an sämtliche gepairten Geräte übertragen. Bei der Wahl eines eigenen Sicherheitsschlüssels sollte dieser mehr als fünf Zeichen aufweisen und aus rein zufälligen Zeichen bestehen. Geht ein Angreifer davon aus, dass der Schlüssel nur aus fünf Zeichen besteht, könnte er für diese fünf Zeichen alle MD5 Werte erzeugen. Hat er einmal das Challenge-Response-Verfahren mitgehört, kann er jeden Schlüssel probieren, um mit dieser Challenge die gleiche Response zu bekommen. Bei 26 Großbuchstaben und 26 Kleinbuchstaben und zehn Ziffern sind das 62 mögliche Zeichen auf fünf Stellen. Dies stellen 916 Millionen verschiedene Schlüssel dar. Diese durchzuprobieren, würde mit einem durchschnittlichen Computer wenige Minuten dauern [Ple15].

8.12 Sicherheitsziele

Hier wird beschrieben, ob die in 2.1 definierten Sicherheitsziele erfüllt werden.

Bevor die HomeMatic Komponenten Daten senden, wenden sie eine XOR-Operation auf den zu sendenden Daten an. Der Schlüssel ist das erste Byte, welches die Länge der zu sendenden Nachricht beschreibt. Da bekannt ist, mit welchem Schlüssel die XOR-Operation angewendet wird, ist der Inhalt der Nachricht nicht davor geschützt, abgehört zu werden. Die frei verfügbare Firmware auf dem CUL hat den Algorithmus zum Verschlüsseln und Entschlüsseln der HomeMatic XOR Verschlüsselung implementiert [cul]. Bei HomeMatic werden die Daten nicht verschlüsselt und können von jedem interpretiert werden. Eine vertrauliche Kommunikation ist nicht möglich.

Die Nachrichten, die bei HomeMatic im Modus „Standard“ übertragen werden, sind nicht gegen Veränderung geschützt. Solche mitgehörten Nachrichten können verändert und erneut gesendet werden. Der Empfänger hat keine Möglichkeit, hierbei festzustellen, ob die Nachricht verändert wurde. Wird eine Nachricht als gesicherter Befehl im Modus „Gesichert“ gesendet, ist die Nachricht Teil des Challenge-Response-Verfahrens. Sollte die Nachricht verändert worden sein, ist das Ergebnis des Challenge-Response-Verfahrens nicht identisch und die HomeMatic Komponenten ignoriert den Befehl. Wird HomeMatic im Modus Gesichert betrieben, ist die Integrität der Nachrichten geschützt.

Die Kommunikation im Modus „Standard“ unterstützt keine Authentifizierung. Alle gesendeten Befehle werden verarbeitet und ausgeführt. Im Modus „Gesichert“ sendet der Empfänger eine Challenge aus, welche der Sender beantworten muss. Zur Berechnung dieser Challenge muss der Sender den identischen Sicherheitsschlüssel besitzen wie der Empfänger. Der besitzt des Sicherheitsschlüssel stellt die Vertrauenswürdigkeit sicher.

Die HomeMatic Komponenten kommunizieren per Funk auf der Frequenz 868 MHz. Wird diese Frequenz gestört oder ist sie belegt, können die HomeMatic Komponenten nicht kommunizieren. Ein Wechsel der Frequenz ist nicht möglich.

8.13 Ergebnis

Die Daten werden unverschlüsselt übertragen und können von jedem empfangen und interpretiert werden. Um zu gewährleisten, dass nur berechtigte Sender Befehle senden, gelangte das Challenge-Response-Authentifizierungsverfahren zur Umsetzung. Da der HomeMatic AES System-Sicherheitsschlüssel frei im Internet zugänglich ist, sollte dringend ein eigener Schlüssel gesetzt werden. Diesbezüglich ist darauf zu achten, dass dieser zufällig gewählt ist und mindestens 20 Zeichen lang ist [bsi]. Das Setzen eines eigenen Schlüssel ist durch ein paar einfache Schritte im Web-Interface möglich. Es bedarf keine besonderen Kenntnisse des Benutzers und sollte einfach zu realisieren sein.

9 DECT

Der internationale Standard Digital Enhanced Cordless Telecommunications (ursprünglich Digital European Cordless Telephony), auch DECT gennant, findet hauptsächlich für Sprachtelefonie Verwendung. Die Technik wird zudem auch bei Gegensprechanlagen, Babyphones und EC-Kartenterminals eingesetzt. Der Standard wurde 1992 durch die ETSI verabschiedet. Seitdem erweiterte sich der Standard um weitere Funktionen [KN10a]. Für die Heimautomatisierung gibt es Komponenten, die mit dem DECT Protokoll kommunizieren. Die am meisten verbreiteten sind schaltbare Steckdosen der Firma FRITZ!. In diesem Kapitel erfolgt eine Untersuchung der Sicherheitsmechanismen bei DECT. In einem selbst durchgeführten Test wird analysiert, wie vorhandene Sicherheitsmechanismen eingesetzt werden.

9.1 Herstellerangaben laut Dokumentation

Auf der Website des Herstellers AVM ist angegeben, dass die FRITZ!DECT 200 Steckdose bereits bei der Auslieferung so konfiguriert ist, dass sie mit einer sicheren Verschlüsselung kommuniziert [dec]. Weiter Einstellungsmöglichkeiten sind über die Benutzeroberfläche der FRITZ!Box möglich. Wie die Verschlüsselung funktioniert beziehungsweise ob es weitere Sicherheitsmechanismen gibt, wird nicht beschrieben.
Auf der Website des European Telecommunications Standards Institute, auch ETSI genannt, ist die Spezifikation der Sicherheitsfeatures der DECT Kommunikation veröffentlicht. Dort wird in einem 160 Seiten Dokument beschrieben, welche Sicherheitsmerkmale bei DECT zur Verwendung gelangen können [dec15, 11].

9.2 FRITZ Smart Home

Um zu untersuchen, wie die Komponenten der Heimautomatisierung bei DECT konfiguriert werden, findet ein Versuchsaufbau statt. Bei diesem Aufbau werden die Komponenten aus Tabelle 14 verwendet. Um mit der Fritzbox zu kommunizieren, ist ein Netz-

	Bezeichnung	weitere Bezeichnung
Fritzbox	FRITZ!Box Fon WLAN 7390	FRITZ!OS 84.06.23
Steckdose	FRITZ!DECT 200	Artikel-Nr.: 2000 2572

Tabelle 14: DECT Komponenten

werkzugang zum Netzwerk der Fritzbox notwendig. Die Steuerung der Fritzbox erfolgt über eine Website. Im Menü, unter Heimnetz, befindet sich ein Eintrag Smart Home.

Dort finden sich keine Komponente, die Steckdose muss zunächst mit der Fritzbox verbunden werden. Die Steckdose wird an den Strom angeschlossen. Nach dem Einstecken blinkt die mit DECT beschriftete LED in regelmäßigen Abständen. Laut Anleitung bedeutet dies, dass die Steckdose bereit ist, sich bei der Fritzbox anzumelden. Auf der Fritzbox wird der mit DECT bezeichnete Knopf gedrückt. Nachdem der DECT Knopf auf der Fritzbox gedrückt wurde, sucht die Fritzbox für ca. zwei Minuten nach DECT Komponenten. Die LED auf der DECT Steckdose blinkt in kurzen Abständen, während sie sich mit der Fritzbox verbindet. Nachdem die DECT LED auf der Steckdose durchgehend leuchtet, erscheint auf der Website der Fritzbox die Steckdose mit dem Namen `FRITZ!DECT 200 1`. Die Steckdose lässt sich über die Website EIN und AUS schalten. Auf der Webseite wird der aktuelle und historische Energieverbrauch der Steckdose angezeigt. Es gibt nur eine Anzeige, dass die Fritzbox mit der Steckdose verbunden ist. Ob diese Verbindung mit Sicherheitsmaßnahmen geschützt ist, wird nicht angezeigt. Im Menü der Fritzbox besteht unter dem Eintrag DECT die Möglichkeit, die Sicherheit der Basisstation zu konfigurieren. Eine Konfiguration dahingehend ist möglich, dass die Fritzbox nur sichere DECT-Verbindungen zulässt beziehungsweise kann eingestellt werden, dass Nicht-verschlüsselte DECT-Verbindungen zugelassen werden.

9.3 Sicherheitsprobleme mit DECT

Eine Gruppe von Sicherheitsforschern hat DECT untersucht. Mithilfe einer selbst geschriebenen Firmware für eine DECT-Karte haben sie nach Sicherheitsproblemen bei DECT gesucht. In diesem Kapitel gelangt die Arbeit von Karsten Nohl, Erik Tews, und Ralf-Philipp Weinmann zur Beschreibung [KN10b].
Der Einsatz von Verschlüsselung bei DECT ist optional. Zur Verschlüsselung wird bei DECT die proprietäre DECT Standard Cipher (DSC) verwendet. Sollte keine Verschlüsselung Einsatz finden, ist es möglich, Telefongespräche abzuhören. Hierfür wird lediglich eine DECT-Karte für den Computer mit der passenden, im Internet frei verfügbaren, Software benötigt. Hierbei zeichnet die Software den Datenstrom zwischen Telefon und Basisstation auf. Aus diesem Datenstrom wird eine Audiodatei erzeugt, welche das Telefonat enthält [Wei08, 28].
Eine Authentifizierung ist optional. Zur Authentifizierung wird bei DECT der proprietäre DECT Standard Authentication Algorithm (DSAA) verwendet. Verzichtet ein Telefon darauf, die Basisstation zu authentifizieren, ist es möglich, das Telefon zu übernehmen, indem ein Angreifer vorgibt, er sei die Basisstation. Dies ermöglicht es einem Angreifer, die Verschlüsselung für Telefonate abzuschalten. Zudem hat er die Möglichkeit, Anrufe umzuleiten [Wei08, 29]. Verzichtet die Basisstation darauf, ein Telefon zu authentifizieren, ist es möglich, über die Basisstation zu telefonieren. Ein Angreifer kann so etwa Telefonate unter falscher Identität führen [KN10a, 2].

Für die Verschlüsselung bei DECT wird die DECT Standard Cipher, auch DSC genannt, eingesetzt. Dabei handelt es sich um eine proprietäre Stromverschlüsselung mit einem geheimen 64 Bit Schlüssel mit einem 35 Bit IV [KN10b, 2]. Die Sicherheitsforscher haben die DSC Implementierung nachkonstruiert und eine Software geschrieben, die durch Probieren versucht, den geheimen Schlüssel zu finden. Auf einer Grafikkarte GeForce GTX 260 CUDA probiert die Software 148 Millionen Schlüssel pro Sekunde und findet einen Schlüssel innerhalb von Minuten [KN10b].
Die Arbeit von Karsten Nohl, Erik Tews, und Ralf-Philipp Weinmann hat erwiesen, dass der DECT Standard keine verlässlichen Sicherheitsmechanismen verwendet.

9.4 DECT Security

DECT hat 2012 einen neuen Standard verabschiedet, um die bekannten Sicherheitsprobleme zu beheben. Eine Basisstation muss in einen Anlernmodus geschaltet werden, damit ein nicht autorisiertes Gerät verbunden werden kann. Erfolgte keine Anmeldung eines neuen Geräts innerhalb von 120 Sekunden, wird der Anlernmodus beendet. Somit wird verhindert, dass Geräte, die nicht autorisiert sind, versuchen, sich mit der Basisstation zu verbinden. Telefone und Basisstationen müssen Verschlüsselung unterstützen und verwenden. Sobald ein Telefon an einer Basisstation angelernt wird, muss die Verschlüsselung aktiviert sein. Ist das Aktivieren der Verschlüsselung nicht möglich oder die Verschlüsselung wird nach dem Anlernen abgeschaltet, beendet die Basisstation die Kommunikation mit dem Telefon. Die Sicherheitsmechanismen DSC und DSAA wurden erneuert. DSC2 [dec12, 60] und DSAA2 [dec12, 62] basieren auf AES und verwenden einen Schlüssel mit 128 Bit.

9.5 Sicherheitsziele

Hier wird beschrieben, ob die in 2.1 definierten Sicherheitsziele erfüllt werden.

Bei Komponenten, bei denen der alte DECT Standard implementiert ist, kann die Kommunikation ausschließlich mit dem obsoleten Algorithmus DSC geschützt werden. Zudem ist der Einsatz der Verschlüsselung optional. Dem Benutzer ist nicht ersichtlich, ob bei seinen Komponenten Verschlüsselung zum Einsatz gelangt. Durch die bekannten Sicherheitsprobleme mit diesem Algorithmus kann die Kommunikation nicht als vertraulich betrachtet werden. Der Nachfolger von DSC basiert auf dem sicheren Verschlüsselungsalgorithmus AES und verwendet einen 128 Bit Schlüssel, um die Kommunikation abzusichern. Komponenten, die den neuen DECT Standard implementiert haben, sichern die Kommunikation laut Spezifikation stets mit DSC2 ab. Unverschlüsselte Kommunikation sollten nicht zugelassen werden. Diese Kommunikation lässt sich

als vertraulich bezeichnen. Zum aktuellen Stand gibt es keine bekannten Sicherheitsprobleme bei DSC2.

Weder bei dem veralteten DSC Algorithmus, noch bei dem neuen Algorithmus DSC2 ist die Integrität der Daten gesichert [dec12, 59]. Komponenten, die den neuen DECT Standard implementiert haben, verwenden gemäß der Spezifikation immer die DSC2 Verschlüsselung. Weitere Maßnahmen zum Schutz der Integrität der Daten existieren nicht.

Die Authentifizierung bei DECT findet bei dem alten DECT Standard mit dem Algorithmus DSAA statt. Infolge der bekannten Sicherheitsprobleme mit diesem Algorithmus ist die Authentizität nicht gewährleistet. Zudem ist bei dem alten DECT Standard die Authentifizierung der Basisstation gegenüber dem Telefon optional. Bei dem neuen DECT Standard erfolgt die Authentifizierung mit DSAA2. Dieser Algorithmus basiert auf AES und gilt als sicher.

Den DECT Komponenten stehen in Europa zehn Kanäle auf der Frequenz 1881,7 MHz bis 1897,3 MHz zur Verfügung. In Nordamerika werden fünf Kanäle auf der Frequenz 1921,5 MHz bis 1928,4 MHz geboten. Sollten diese Frequenzen belegt oder gestört sein, können die Komponenten nicht per DECT kommunizieren.

9.6 Ergebnis

Beim alten DECT Standard gibt es keine verlässlichen Sicherheitsmechanismen. Verschlüsselung und Authentifizierung sind optional. Die Verschlüsselung beim alten DECT Standard verwendet einen zu schwachen Schlüssel und lässt sich, mit der Rechenleistung aktueller Computerhardware, relativ schnell brechen. Die Sicherheitsmaßnahmen des neuen DECT Standard basieren auf dem sicheren Verschlüsselungsalgorithmus AES. Die Spezifikation der Sicherheitsfeatures bei DECT ist öffentlich zugänglich und lässt sich überprüfen. Zum aktuellen Stand sind keine Schwächen in den Sicherheitsmechanismen des neuen DECT Standards bekannt.

10 Zusammenfassung

Im Rahmen dieser Arbeit erfolgte die Untersuchung verschiedener Techniken in der Heimautomatisierung. In Kapitel 3 wird beschrieben, dass die aktuelle Implementierung von ZigBee nicht sicher ist. Die bei ZigBee verwendeten Methoden zum Absichern der Kommunikation sind gut, allerdings können diese in der aktuellen ZigBee Spezifizierung durch das unsichere Beitreten umgangen werden. Das Kapitel 4 erörtert, welche Sicherheitsmechanismen Einsatz finden können, um die Komponenten der Heimautomatisierung bei EnOcean abzusichern. Falls die eingesetzten Komponenten sichere Kommunikation unterstützen, kann der Anwender selbst konfigurieren, welches Maß an Sicherheit er einsetzen möchte. Die Sicherheitsmechanismen bei Z-Wave werden in Kapitel 5 beschrieben. Es werden sichere Methoden verwendet, um die Komponenten abzusichern. Die Informationen zu den Sicherheitsmethoden bei KNX in Kapitel 6 gibt es lediglich in Form einer Spezifikation. Wird die Spezifikation von KNX und den Herstellern richtig implementiert, könnte bei KNX-RF sicher kommuniziert werden. Bei FS20 in Kapitel 7 werden keine Sicherheitsmethoden eingesetzt, um die Kommunikation zu schützen. Die Beschreibung der Sicherheitsmechanismen bei HomeMatic erfolgt in Kapitel 8. Wird der voreingestellte Sicherheitsschlüssel durch einen selbst gewählten ersetzt, ist die Kommunikation bei HomeMatic mit dem Challenge-Response-Verfahren abgesichert, allerdings nicht verschlüsselt. Die Sicherheitsmaßnahmen bei dem neuen DECT Security Standard in Kapitel 9 sind sicher. Jedoch ist für den Benutzer nicht ohne Weiteres zu erkennen, ob seine Komponenten den alten oder neuen DECT Standard verwenden.

Die Resultate werden in Tabelle 15 zusammengefasst. Dort ist abzulesen, wie der Austausch des geheimen Schlüssels stattfindet. Es wird beschrieben, ob der Anlernmodus manuell durch einen Benutzer aktiviert werden muss. Überdies gelangt der Algorithmus zur Verschlüsselung und Integritätsprüfung zur Darstellung. Zum Schluss wird angegeben, mit welcher Methode dafür gesorgt wird, dass eine Nachricht aktuell beziehungsweise gegen Replay Angriffe geschützt ist.

	Schlüsseltausch	Anlernmodus	Verschlüsselung	Integrität	Aktualität
ZigBee	Verschlüsselt[1]	Immer[4] - (unsicheres Beitreten)	CCM	CCM	Nonce
KNX RF	Gerätespezifischer Schlüssel	Aktiviert durch Benutzer	CCM	CCM	Sequenz-nummern
Z-Wave	Verschlüsselt[1]	Aktiviert durch Benutzer	OFB	CBC-MAC	Nonce
FS20	/	Aktiviert durch Benutzer	/	/	/
HomeMatic RF	Verschlüsselt[2]	Aktiviert durch Benutzer	/	/[5]	Challenge
EnOcean	Unverschlüsselt[3]	Aktiviert durch Benutzer	CBC oder VXOR	CMAC	Rolling Code
DECT	PIN	Aktiviert durch Benutzer	CCM	/	Nonce

Tabelle 15: Zusammenfassung

[1] Schlüssel ist bekannt.

[2] Default Schlüssel ist bekannt. Nur sicher, wenn ein anderer Schlüssel konfiguriert wurde.

[3] Verschlüsselter Schlüsseltausch ist möglich, wenn vom Hersteller ein Schlüssel konfiguriert wurde.

[4] ZigBee Version 1.2.

[5] Kommando ist Teil der Antwort beim Challenge-Response-Verfahren.

11 Ergebnis

Die Betrachtung der verschiedenen Techniken in der Heimautomatisierung hat belegt, dass einige von ihnen empfindliche Sicherheitslücken aufweisen. Gemessen daran, wie die Unternehmen das Thema Sicherheit in ihren Produkten darstellen, scheint es für die Kunden uninteressant zu sein. Wahrscheinlich würden die Hersteller mehr mit dem Thema Sicherheit werben, wenn ihre Kunden sich mehr dafür interessieren würden. Wie das Beispiel an DECT und Z-Wave gezeigt hat, sind Systeme nicht sicherer, wenn der Hersteller die Funktionsweise der Sicherheitsmechanismen geheim hält. Entscheidet sich ein Hersteller dafür, die Funktionsweise und Sicherheitsmethoden seiner Technik öffentlich zu machen, haben unabhängige Sicherheitsforscher die Möglichkeit, diese zu überprüfen sowie auf Probleme zu untersuchen.

Literatur

[bsi] Wahl der richtigen Passwörter. https://www.bsi-fuer-buerger.de/BSIFB/DE/MeinPC/Passwoerter/passwoerter_node.html. Accessed: 02/01/2016.

[cbc13] Why I hate CBC-MAC. http://blog.cryptographyengineering.com/2013/02/why-i-hate-cbc-mac.html, 02 2013. Accessed: 26/11/2015.

[ccm02] On the Security of CTR + CBC-MAC. http://csrc.nist.gov/groups/ST/toolkit/BCM/documents/proposedmodes/ccm/ccm-ad1.pdf, 2002. Accessed: 26/11/2015.

[Cry] Cryptography used in IEEE 802.15.4. http://www.atmel.com/Images/doc8260.pdf. Accessed: 31/01/2016.

[cul] culfw. http://culfw.de/culfw.html. Accessed: 31/01/2016.

[dec] FRITZ!DECT 200. http://avm.de/produkte/fritzdect/fritzdect-200/details/. Accessed: 18/01/2016.

[dec12] DECT Security Analysis. http://tuprints.ulb.tu-darmstadt.de/2932/1/thesis-webview.pdf, 05 2012. Accessed: 18/01/2016.

[dec15] Digital Enhanced Cordless Telecommunications (DECT) Common Interface (CI) Part 7: Security features. http://www.etsi.org/deliver/etsi_en/300100_300199/30017507/02.06.01_60/en_30017507v020601p.pdf, 07 2015. Accessed: 18/01/2016.

[DF14] J. Durech and M. Franekova. Security attacks to ZigBee technology and their practical realization. In *Applied Machine Intelligence and Informatics (SAMI), 2014 IEEE 12th International Symposium on*, pages 345–349, Jan 2014.

[enO13a] Security of EnOcean Radio Networks. https://www.enocean.com/fileadmin/redaktion/pdf/tec_docs/Security_of_EnOcean_Radio_Networks.pdf, 07 2013. Accessed: 09/01/2016.

[enO13b] Transceiver Module. http://datasheet.octopart.com/S3053-K320-EnOcean-datasheet-19979652.pdf, 09 2013. Accessed: 09/01/2016.

[enO14] EnOcean Serial Protocol 3 (ESP3). https://www.enocean.com/fileadmin/redaktion/pdf/tec_docs/EnOceanSerialProtocol3.pdf, 07 2014. Accessed: 09/01/2016.

[enO15a] Batterielose Schalter und Sensoren und Empfänger. https://www.enocean-alliance.org/de/produkte/, 2015. Accessed: 09/01/2016.

[enO15b] EnOcean Starter Kit. https://www.enocean.com/en/enocean_modules/esk-300/user-manual-pdf/, 09 2015. Accessed: 09/01/2016.

[enO15c] Frequently Asked Questions zu Technologie, Produkte und Lösungen. https://www.enocean-alliance.org/fileadmin/redaktion/enocean_alliance/pdf/Downloads/white_paper_FAQ_DE.pdf, 11 2015. Accessed: 09/01/2016.

[eno16] Mit EnOcean wird das Smart Home noch smarter. https://www.enocean.com/de/applications/smart-home-und-heimautomation/, 2016. Accessed: 09/01/2016.

[Far08] S. Farahani. ZigBee Wireless Networks and Transceivers, 2008. Accessed: 30/11/2015.

[fhe] FS20 Adressumrechnung. http://www.fhemwiki.de/wiki/FS20_Allgemein#FS20_Adressumrechnung. Accessed: 25/12/2015.

[fhe13a] Fhem - FS20. https://github.com/mhop/fhem-mirror/blob/master/fhem/FHEM/10_FS20.pm, 2013. Accessed: 25/12/2015.

[fhe13b] Fhem - HomeMatic. https://github.com/mhop/fhem-mirror/blob/master/fhem/FHEM/HMConfig.pm, 2013. Accessed: 02/01/2016.

[fs2a] Das FS20-Funk-Steuersystem in der Praxis - Planung und Einrichtung des FS20 Haus-Steuersystems. http://www.elv.de/Das-FS20-Funk-Steuersystem-in-der-Praxis-Planung-und-Einrichtung-des-FS20-Haus-Steuersystems/x.aspx/cid_726/detail_31466. Accessed: 25/12/2015.

[FS2b] Das FS20 System können Sie weiterhin z.B hier bei ELV erwerben. http://www.ehomeportal.de/MAX-FS20-u-a-/FS20-System.htm?shop=shop&a=catalog&t=1597&c=1597&p=1597. Accessed: 25/12/2015.

[fs2c] FAQ: Plant eQ-3 angesichts des Erfolgs von HomeMatic die Einstellung von FS20? http://www.eq-3.de/faq.html?id=84. Accessed: 25/12/2015.

[FS2d] FS20-Funkschaltsystem - Sicherheit und Verschlusstechnik. http://www.elv.de/sicherheit-und-verschlusstechnik-einsatzmoeglichkeiten-1.html. Accessed: 25/12/2015.

[fs2e] LTE-Router stört Heimkino-Steuerung FS20. http://www.heise.de/ct/hotline/LTE-Router-stoert-Heimkino-Steuerung-FS20-2056794.html. Accessed: 25/12/2015.

[fs215] FS20 Sicherheitsbedenken. http://forum.fhem.de/index.php?topic=34962.0, 03 2015. Accessed: 25/12/2015.

[Ger15] M. Gernoth. Dissecting HomeMatic AES. https://git.zerfleddert.de/hmcfgusb/AES/, 06 2015. Accessed: 02/01/2016.

[Gis08] D. Gislason. *Zigbee Wireless Networking*. Newnes, 2008.

[GR15] N. Garcia and J. Rodrigues. *Ambient Assisted Living*. Rehabilitation Science in Practice Series. CRC Press, 2015.

[Gra13] D. Gratton. *The Handbook of Personal Area Networking Technologies and Protocols*. Cambridge University Press, 2013.

[Hom14] homematic bidcos default aes key. http://pastebin.com/eiDnuS8N, 11 2014. Accessed: 02/01/2016.

[hom15] Über eQ-3. http://www.eq-3.de/unternehmen.html, 2015. Accessed: 02/01/2016.

[Kak16] A. Kak. Using Block and Stream Ciphers for Secure Wired and WiFi Communications. https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture9.pdf, 2016. Accessed: 31/01/2016.

[Kan12] R. Kancheva. Trojanersichere Fenster: Verschl/üsselung und Entschl/üsselung. http://www-ti.informatik.uni-tuebingen.de/~borchert/Troja/studdiplfiles/KanchevaDiplomarbeit.pdf, 12 2012. Accessed: 31/01/2016.

[KN10a] E. T. Karsten Nohl. Kann man mit DECT noch vertraulich telefonieren? https://www.cdc.informatik.tu-darmstadt.de/~e_tews/NohlTews_DuD11-2010.pdf, 11 2010. Accessed: 18/01/2016.

[KN10b] R.-P. W. Karsten Nohl, Erik Tews. Cryptanalysis of the DECT Standard Cipher. CryptanalysisoftheDECTStandardCipher, 02 2010. Accessed: 18/01/2016.

[KNXa] Einfach sorgenfrei wohnen. https://www.becker-antriebe.de/nutzen/sicherheit.html. Accessed: 08/12/2015.

[knxb] Jalousiesteuerbaustein. http://www.knx-gebaeudesysteme.de/sto_g/English/PRODUCT_MANUALS/JSBS_11_PH_DE_V1-0_2CDC506030D0101.PDF. Accessed: 08/12/2015.

[KNXc] KNX Grundlagenwissen. http://www.knx.org/media/docs/Flyers/KNX-Basics/KNX-Basics_de.pdf. Accessed: 08/12/2015.

[KNXd] KNX RF - Then, Now, Future. http://knx-professionals.nl/files/bijeenkomsten/29/01_20joost_20demarest_20-_20knx_20association.pdf. Accessed: 08/12/2015.

[KNXe] KNX User Manual. http://www.radiocrafts.com/uploads/knx_user_manual_0_30.pdf. Accessed: 08/12/2015.

[KNX07] KNX-RF Implementation based on MSP430 and CC1101. http://www.ti.com/lit/an/slaa390/slaa390.pdf, 2007. Accessed: 08/12/2015.

[KNX13] KNX System Specifications. https://www.knx.org/media/docs/downloads/KNX-Standard/Architecture.pdf, 11 2013. Accessed: 08/12/2015.

[KNX15] KNX Sicherheit. https://www.knx.org/media/docs/downloads/Marketing/Flyers/KNX-Security-Position-Paper/KNX-Security-Position-Paper_en.pdf, 04 2015. Accessed: 08/12/2015.

[KS07] G. Kupris and A. Sikora. *ZigBee: Datenfunk mit IEEE 802.15.4 und ZigBee*. Franzis, 2007.

[May15] MayaZigBee. This Tweet from @MayaZigBee has been withheld in response to a report from the copyright holder. https://twitter.com/MayaZigBee/status/579723961661022209, 03 2015. Accessed: 30/11/2015.

[Ple15] H. Pleotz. On the Security of AES in HomeMatic. https://blog.ploetzli.ch/2015/on-the-security-of-aes-in-homematic/, 09 2015. Accessed: 02/01/2016.

[rwe15] ENTR: Intelligentes T/ürschloss f/ür RWE SmartHome. http://www.housecontrollers.de/hausautomatisierung/rwe-smarthome/entr-intelligentes-tuerschloss-fuer-rwe-smarthome/, 2015. Accessed: 31/01/2016.

[Sik03] A. Sikora. *Technische Grundlagen der Rechnerkommunikation*. Carl Hanser Verlag GmbH & Co. KG, 2003.

[sma16] Intelligentes Thermostat Lyric: Nest-Alternative von Honeywell. http://www.housecontrollers.de/heizungssteuerung/thermostat-honeywell-lyric-nest-alternative/, 2016. Accessed: 26/11/2015.

[sta] RC5-64 - Aggregate Statistics. http://stats.distributed.net/projects.php?project_id=5. Accessed: 31/01/2016.

[VHPA+13] N. Vidgren, K. Haataja, J. L. Patino-Andres, J. J. Ramirez-Sanchis, and P. Toivanen. Security Threats in ZigBee-Enabled Systems: Vulnerability Evaluation, Practical Experiments, Countermeasures, and Lessons Learned. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on*, pages 5132–5138, Jan 2013.

[Wei08] A. S. E. T. R.-P. Weinmann. deDECTed.org. http://www.fredsforum.nl/FredAmateur/talk-25c3.pdf, 10 2008. Accessed: 18/01/2016.

[wir07] Wireless Communication in Home and Building Automation. http://www.auto.tuwien.ac.at/~creinisch/Wireless%20Communication%20in%20Home%20and%20Building%20Automation.pdf, 02 2007. Accessed: 26/11/2015.

[ZBf] ZLL Functionality. http://www.nxp.com/documents/user_manual/JN-UG-3091.pdf. Accessed: 30/11/2015.

[ZBha] Hue Schutz und Sicherheit. http://origin.www2.meethue.com/de-de/was-tut-hue/schutz-und-sicherheit/. Accessed: 30/11/2015.

[ZBhb] Was ist Hue - Immer aktuell. http://www2.meethue.com/de-de/ueber-hue/das-ist-hue/. Accessed: 30/11/2015.

[ZBs10a] ZIGBEE HOME AUTOMATION PUBLIC APPLICATION PROFILE. https://docs.zigbee.org/zigbee-docs/dcn/07/docs-07-5367-02-0afg-home-automation-profile-for-public-download.pdf31, 02 2010. Accessed: 30/11/2015.

[ZBs10b] ZIGBEE SPECIFICATION. http://www.deyisupport.com/cfs-file.ashx/__key/communityserver-discussions-components-files/104/0257.Zigbee-Speccification_5F00_2010.pdf, 10 2010. Accessed: 30/11/2015.

[ZBz12] Exploring New Lighting Opportunities with ZigBee Light Link™ Webinar. https://docs.zigbee.org/zigbee-docs/dcn/12/docs-12-0255-00-0mwg-exploring-new-opportunities-with-zigbee-light-link.pdf, 05 2012. Accessed: 30/11/2015.

[zig14] ZigBee PRO Stack User Guide. http://www.nxp.com/documents/user_manual/JN-UG-3048.pdf, 06 2014. Accessed: 16/12/2015.

[Zil15] T. Zillner. ZIGBEE EXPLOITED. http://cognosec.com/zigbee_exploited_8F_Ca9.pdf, 08 2015. Accessed: 30/11/2015.

[zwa] Home Control Technologies. http://z-wave.sigmadesigns.com/docs/Z-Wave_Technology_Comparison.pdf. Accessed: 16/12/2015.

[zwa13] Security Evaluation of the Z-Wave Wireless Protocol. http://drive.google.com/uc?export=view&id=0B8l07E7STihRTDB3WmEza1ludEk&nonsesnse=something.pdf, 2013. Accessed: 16/12/2015.

[zwa14] Metering Plug MT02646 (devolo). http://products.z-wavealliance.org/products/1129, 4 2014. Accessed: 16/12/2015.

[zwa15a] Is Z-Wave secure? http://www.z-wave.com/faq, 2015. Accessed: 16/12/2015.

[zwa15b] Open-ZWave Library. https://github.com/OpenZWave/open-zwave, 2015. Accessed: 16/12/2015.

[zwa15c] Technische Angaben. http://www.devolo.de/fileadmin/user_upload/Products/devolo-Home-Control-Control-Center/Documents/Datenblatt-devolo-Home-Control-Zentrale-de.pdf, 10 2015. Accessed: 16/12/2015.

[zwa15d] What is Z-Wave? http://z-wave.sigmadesigns.com/about_z-wave, 2015. Accessed: 16/12/2015.

[zwa15e] Z-Wave. http://www.devolo.de/article/devolo-home-control-zentrale/, 2015. Accessed: 16/12/2015.