Secure Smart Homes

Stanisic Vladimir - Fotolia

Abteilung Marktforschung, Oktober 2018

Studie zur digitalen Sicherheit für das intelligente Heim

Joanneum Research im Auftrag der Kammer für Arbeiter und Angestelle für Steiermark

Secure Smart Homes

Studie zur digitalen Sicherheit für das intelligente Heim

Joanneum Research Digital
Institut für Informations- und Kommunikationstechnologien

Kai Nahrgang; Stefan Marksteiner; Heribert Vallant

Graz, Oktober 2018

Im Auftrag der
Kammer für Arbeiter und Angestellte für Steiermark

Inhalt

1 Executive Summary

Smart Homes – durch so gennannte Internet of Things (IoT)-Technologien vernetzte Gebäude- und Haushaltstechnik – ist in letzter Zeit in den Blickpunkt von Sicherheitsdebatten gekommen. Dies einerseits, weil der Markt für diese Technologien stetig wächst [1] [2] [3] und andererseits, weil sich im gleichen Maße Sicherheitsvorfälle häufen. So wurden so genannte Botnetzte gebildet [4] [5] [6] oder gezeigt, dass z.B. Türschlösser gesteuert [7] werden und Privatsphäre von Konsumenten kompromittiert [8] werden kann.

Die Motive von Hackern bzw. Cyber-Kriminellen, in Smart Homes einzudringen sind dabei vielfältig und reichen von Themen, die die Privatsphäre berühren (siehe Abschnitte 6.1.1 und 8.1), über die Nutzung von ungesicherten IoT-Systemen als Eintrittspunkt (siehe Abschnitt 7.1), bis hin zur Nutzung vieler IoT-Systeme um gemeinsam Schaden zu verursachen (siehe Abschnitt 7.1) und zur Diskreditierung von Geräteherstellern aus unterschiedlichen Motiven (siehe Abschnitt 4).

Die Sicherheitsrisiken der Nutzung Smart Homes, welche Hacker für ihre Ziele ausnützen können, können prinzipiell in fünf Kategorien eingeteilt werden [9]:

- Hardware-Kategorie
- Software-Kategorie
- Informations-Kategorie
- Kommunikation-Kategorie
- Menschliche-Kategorie

Am schwerwiegendsten sind hierbei Risiken die aus physischem Zugriff, mangelnder Authentifizierung und Vertraulichkeit oder Social Engineering resultieren.

Exemplarisch für die Komposition eines Smart Homes wurden weiters fünf Bereiche näher untersucht:

- Sicherheitssysteme (Abschnitt 5)
- Energiemanagement (Abschnitt 6)
- Haushaltsgeräte (Abschnitt 7)
- Persönliche Assistenten (Abschnitt 8)
- Sowie Kommunikationsprotokolle als Querschnittsthema (Abschnitt 9)

Die Sicherheitssysteme leiden vor allem unter *State Consistency Attacks*, unabsichtlichem Entsperren und Replay-Angriffen. Erstere sind durch technische Maßnahmen seitens der Hersteller zumindest teilweise zu verhindern, die letzteren beiden Probleme durch zusätzliche physische Maßnahmen, die jedoch die Benutzerfreundlichkeit leicht einschränken (Drücken von Zusatzknöpfen). Energiemanagementsysteme werden vornehmlich von Risiken bezüglich der

Privatsphäre sowie Hard- und Softwarelücken bedroht. Hier ist vor allem auf Segregations- und Authentisierungsmaßnahmen, sowie auf Sofwareupdates und das Einhalten von *Best Practice*-Leitfäden zu achten. Analoges gilt auch bei Haushaltsgeräten während bei persönlichen Assistenten auch die nicht autorisierte Verwendung im Vordergrund steht. Letztere sollten so konfiguriert werden, dass nicht autorisierte Personen (Gäste, Handwerker aber evtl. auch Kinder) diese nicht oder nur stark eingeschränkt verwenden können; außerdem sollten kritische Funktionen (z.B. Türschlösser) nicht mit Assistent verknüpft werden, sowie diese nicht zum Merken von Passwörtern genutzt werden. Von Kommunikationsprotokollen sollte jeweils die neuste genutzt und, falls möglich, Rückwärtskompatibilität zu älteren deaktiviert werden. Obwohl prinzipiell Z-Wave und Bluetooth (in der jeweils neuesten Version) tendenziell sicherer sind als Zigbee, hängt die Sicherheit des jeweiligen Protokolls letzten Endes auch von der Implementierung durch den Hersteller in dessen Produkten ab, weswegen Produkte deswegen einzeln auf ihre Sicherheit getestet werden müssen.

Generell ist zu sagen, dass sich viele Schutzmaßnahmen entweder der Einflusssphäre der Konsumenten vollständig entziehen (da sie in der Hand von Herstellern oder Installateuren liegen) oder Know-how erfordern, dass von Verbrauchern nicht vorauszusetzen ist.

Empfehlenswert sind, unabhängig von den eingesetzten Produkten, folgende Vorgangsweisen (sofern möglich):

- Authentifizierung durch sichere Passwörter [10], die nicht dem Hersteller-Default entsprechen
- Falls möglich (speziell bei Gerät-zu-Gerät-Kommunikation) Authentifizierung durch kryptographische Maßnahmen (z.B. Zertifikate)
- Möglichst starke Segregation des Netzwerks
    - Trennung zwischen Internet und Heimnetz
    - Trennung Smart Home Geräte-Netz und allgemeinem Netz für Notebooks, etc.,
    - Trennung zwischen kritischen (z.B. Heizungsanlage) und weniger kritischen Bereichen.

  Hierbei sollte eine Firewall eingesetzt werden, die nur die unbedingt nötigen Verbindungen zulässt (*Whitelisting*).
- Einspielen der neuesten (Sicherheits-)Updates (idealerweise automatisiert)
- Verwenden jeweils neuester Protokollversionen (z.B. für Bluetooth Version 5) und, wenn möglich, deaktivieren älterer Versionen
- Verwenden von Protokollsicherheitsfeatures (Verschlüsselung z.B. via HTTPS)
- Deaktivieren nicht verwendeter Dienste (speziell solche, die Schnittstellen des Smart Homes im Internet zugänglich machen)
- Deaktivieren nicht verwendeter Datenverbindungen (speziell solche, die Daten in Internet z.B. an den Hersteller übertragen)
- Genaues Einsehen der Privacy-Einstellung (falls vorhanden)

2 Einführung

Der Markt rund um Smart Homes, also das Vernetzen von Haushaltsgeräten, Sicherheitssysteme und Haustechnik, erfährt in den letzten und kommenden Jahren einen immer größeren Zuwachs [1] [2] [3]. Diese steigende Nachfrage kommt jedoch Hand in Hand mit Bedenken bezüglich der Sicherheit solcher vernetzten und intelligenten Systeme.

Diese Bedenken werden durch zahlreiche Studien und Veröffentlichungen bekräftigt. So ist es etwa möglich, aus kompromittierten *Internet of Things (IoT)*-Geräten, welche die *intelligenten* Komponenten in einem Smart Home bilden [11], Botnetze zu erstellen [4] [5] [6]; mit Hilfe von Geräten mit visuellen und auditiven Funktionen die Privatsphäre des Endnutzer zu gefährden [8]; smarte Sicherheitssysteme zu kompromittieren und so etwa Türschlösser zu steuern [7]. Im Zuge dieser Arbeit wird in den kommenden Kapiteln auf die einzelnen Bedrohungen eingegangen werden.

Die Motive von Hackern bzw. Cyber-Kriminellen, in Smart Homes einzudringen sind dabei vielfältig und reichen von Themen die die Privatsphäre berühren (siehe Abschnitte 6.1 und 8.1) über die Nutzung von ungesicherten IoT-Systemen als Eintrittspunkt (siehe Abschnitt 7.1) bis hin zur Nutzung vieler IoT-Systeme um gemeinsam Schaden zu verursachen (siehe Abschnitt 7.1) und zur Diskreditierung von Geräteherstellern aus unterschiedlichen Motiven (siehe Abschnitt 4).

Daher wird in dieser Studie behandelt, welche Gefahren es in Smart Homes in Bezug auf Cybersicherheit gibt, wie der Endnutzer diese Bedrohungen entgegentreten kann und wie er seine Privatsphäre schützen kann.

3 Methodik

Diese Studie wurde mit Hilfe einer Literaturrecherche durchgeführt. Dazu wurden aktuelle wissenschaftliche Publikationen analysiert und ausgewertet. Auf Grundlage dieser wurden die verschiedenen Kapitel der Studie untergliedert.

Zunächst wurde auf allgemeine Risiken eingegangen. Diese sollen Benutzer von Smart Home Systemen aufzeigen, welche unterschiedlichen Gefahren von nicht sicheren Produkten ausgeht und wieso auch Normalverbraucher sich vor Angriffen schützen sollen.

Anschließend wurden verschiedene Komponenten eines Smart Home-Systems beschrieben, deren Risiken aufgezeigt und Lösungsvorschläge bzw. Gegenmaßnahmen evaluiert. Zu diesen gehören Sicherheitssysteme wie Türschlösser, Komponenten für Energiemanagement wie Thermostate und intelligente Energiezähler, Haushaltsgeräte wie etwa Glühbirnen und Sprinkleranlagen, persönliche Assistenten wie Sprachassistenten (z.B. Alexa) und Protokolle, mit denen Smart Home-Geräte kommunizieren.

Abschließend wurden alle Erkenntnisse zusammengefasst und Schlussfolgerungen gezogen.

4 Allgemeine Risiken

In diesem Kapitel werden unterschiedliche Gefahren von Smart Home aufgezeigt und beschrieben. Anschließend wird in den folgenden Kapiteln spezifisch auf die verschiedenen Einsatzbereiche von Smart Home eingegangen.

Neben den technischen Risiken, die später in diesem Kapitel beschrieben werden, sind monetäre Faktoren wesentliche Bestandteile der Cybersicherheit. Da viele Verbrechen in diesem Bereich nicht gemeldet werden, ist es relativ schwierig eine konkrete Zahl zu berechnen, die Cyberverbrechen verursachen. Sowohl Anderson et al. als auch Gañán, et al. argumentieren, dass es nicht möglich sei, globale Kosten für Cyberverbrechen zu berechnen und kritisieren die Zahlen, die von Unternehmen für die Berechnung der Kosten verwendet werden, da diese nicht nachvollziehbar seien [12] [13].

Trotzdem werden Zahlen weiter publiziert; laut diesen kann ein Wachstum an verursachten Kosten verzeichnet werden. In den Vereinigten Staaten wurden 2011 etwa neun Milliarden US-Dollar an Kosten verursacht; 2015 waren es bereits 400 Milliarden US-Dollar. Zu diesen Kosten zählen neben den verursachten Schäden auch die Reparaturkosten und die Reputation der Unternehmen und die nationale Ökonomie [14].

Jones analysiert in ihrer Fallstudie unteranderem die Auswirkung von Cyberverbrechen auf den Aktienmarkt anhand von Unternehmen, die Opfer von Hackerattacken wurden und diese auch meldeten. Die Studie zeigt, dass die meisten Aktienkurse nach dem Publizieren des Angriffes runter gingen, sich im Regelfall aber wieder erholten [14]. Daraus kann abgeleitet werden, dass das Ziel von Angriffen nicht zwingend die Endnutzer sein müssen, da die Reputation und Aktienpreise von Unternehmen damit beeinflussbar sind.

In der Risikoanalyse über Smart Home Systeme von Jacobsson et al. wurden 32 Risiken identifiziert, die in folgenden Kategorien zugewiesen wurden [9]:

- Hardware-Kategorie
- Software-Kategorie
- Informations-Kategorie
- Kommunikation-Kategorie
- Menschliche-Kategorie

Auf die schwerwiegendsten Risiken der jeweiligen Kategorien wird nun eingegangen.

Zur Hardware-Kategorie zählen alle Angriffe, die Hacker physisch vornehmen können. So ist es etwa möglich, Sensoren zu manipulieren oder das Produkt auf Werkeinstellung zurückzusetzen, um etwa Standardpasswörter wiederherzustellen und so Zugang zum jeweiligen Gerät zu erlangen [9].

Risiken im Bereich der Software-Kategorie sind die am häufigsten vertretenden.

- Dazu zählt etwa eine unzureichende Implementierung von Authentifizierung, dass den Angreifer erlaubt, sich ohne korrekten Zugangsdaten auf dem Gerät zu authentifizieren.
- Das ausreichende Protokollieren von Systemereignissen und Benutzeraktionen ist nicht nur für das Beheben und Rekonstruieren von Softwarefehlern notwendig, sondern ist auch essentiell um Angriffe und Versuche von eben diesen zu erkennen.
- Wie jedes System können auch Smart Home Komponenten das Ziel von Denial of Service (DoS) Attacken sein. Im Smart Home Bereich ist es etwa möglich, dass die Konfiguration von Cloud-Diensten das lokale Gateway mit Nachrichten flutet und das System so unerreichbar wird.

In der Informations-Kategorie geht es, wie auch schon in der Software-Kategorie angeschnitten, um Authentifizierung und Autorisierung. So wird etwa die mangelnde Implementierung eines Zugriffskontrollsystems kritisiert, da diese nur einen einzelnen User-Account, welcher zugleich der Administrator-Benutzer ist, unterstützt. Für Systeme mit einem fortgeschritteneren Zugriffskontrollsystems, welches nicht nur mehrere unabhängige Benutzer erlaubt, sondern auch ein Berechtigungsmanagement beinhaltet, ist es essenziell, dass das System richtig konfiguriert wird.

Im Bereich der (Netzwerk)-Kommunikations-Kategorie stellen vertrauliche Konfigurationen innerhalb von miteinander verbundenen Sensoren ein Risiko dar. So können etwa sensible Informationen innerhalb des Systems von einem Sensor zum anderen gesendet werden – wie zum Beispiel Kommandos um Sicherheitssystem wie Alarmanlagen ein und auszuschalten oder Türschlösser zu öffnen und zu schließen. Solche Befehle könnten von Angreifern abgefangen, analysiert und gegen das System verwendet werden.

Die letzte Kategorie spielt eine große Rolle, da der menschliche Faktor in Bezug auf Cybersicherheit immer ein essenzielles Risiko darstellt. So sind schwache Passwörter das größte Risiko in diesem Bereich. Das trifft insbesondere bei Systemen zu, welche nur einen einzigen Benutzer erlauben, da dieser gleichzeitig der Administrator-Benutzer ist.

Neben schwachen Passwörtern sind die Endbenutzer selbst von sogenannten Social-Engineering-Angriffen nicht gefeit. Bei solchen Angriffen werden die Benutzer vom Hacker so manipuliert, dass diese vertrauliche Informationen, wie etwa Passwörter, verraten.

5 Sicherheitssysteme

In diesem Kapitel werden Sicherheitssysteme wie Türschlösser begutachtet. In der Studie von Ho et al. wurden die fünf, zu diesem Zeitpunkt am beliebtesten, intelligenten Türschlösser auf Sicherheitslücken untersucht. Diese Studie wird als Referenz für dieses Kapitel verwendet [7].

5.1 Funktionsweise

Intelligente Türschlösser im Smart Home Bereich bestehen aus drei verschiedenen Komponenten: Einen elektronischen Türriegel, einer mobilen Applikation und einen Webserver.

Damit die Benutzer die Türschlösser mit der mobilen Applikation des Herstellers kontrollieren können, ist es notwendig, sich am Webserver des Herstellers zu registrieren. Anschließend können sich Geräte des Benutzers mit Wireless-Technologien wie Bluetooth Low Energie (BLE) mit dem Türschloss koppeln.

Es gibt zwei Architekturen, wie Türschlösser konzipiert werden. Einerseits ist es möglich, dass die Schlösser selbst eine Internetverbindung zum Server des Herstellers aufbauen können, andererseits können mobile Geräte, die eine Verbindung zum Schloss haben, als Internetgateway vom Türschloss verwendet werden um so eine Verbindung zum Server aufzubauen. Letztere Architektur wird häufiger verwendet und von Ho et al. als Device-Gateway-Cloud (DGC) Variante bezeichnet [7].

Alle Türschlösser haben eine erweiterte Implementierung der Zugriffskontrolle, die mit digitalen Schlüsseln funktioniert. So kann der Besitzer weiteren Benutzern einen digitalen Schlüssel ausstellen und die entsprechende Rolle dazu definieren, um unterschiedliche Zugriffe zu geben. Der Benutzer, der sich als erstes mit dem Türschloss verbindet, ist meistens der Administrator; im System der Türschlösser als *Owner* bezeichnet. Der Rolle des *Resident*, also einem Bewohner, ist es gestattet, wie auch dem *Owner*, das Schloss jederzeit zu öffnen und zu schließen. Es ist ihnen aber untersagt, administrative Tätigkeiten vorzunehmen. *Recurring guests*, also wiederkehrende Gäste wie etwa Putzpersonal, können zu gewissen Zeitspannen (z.B. an Wochenenden zwischen 09:00 – 15:00) die Türen öffnen und schließen. Zuletzt gibt es auch für Gäste eine letzte Rolle. Diese können für eine temporäre Zeitspanne das Türschloss bedienen (z.B. 24 Stunden lang).

Um ein Türschloss zu sperren oder zu entsperren, muss der Benutzer einen Knopf in der mobilen Applikation betätigen. Zusätzlich gibt es noch Systeme, die ein sperren bzw. entsperren des Schlosses erlaubt, wenn ein autorisiertes Gerät sich dem Schloss entfernt bzw. nähert. Manche Systeme kombinieren diesen Ansatz noch mit einem zusätzlichen Touch-Sensor. Wichtig zu erwähnen ist auch, dass jede Aktivität vom System protokolliert wird [7].

5.2 Risiken

Die Motivation von kriminellen ein Sicherheitssystem auszuhebeln ist offensichtlich: durch knacken der Sicherheitssysteme (v.a. Türschlösser und Alarmsysteme) werden Einbrüche und Diebstähle deutlich erleichtert. Um dies zu erreichen werden von Ho et al., neben Netzwerkangriffen und Malware, vier weiteren Risiken genannt [7]. Diese werden nachfolgend beschrieben, anschließend werden dazu mögliche Angriffe geschildert.

- Hier wird als erstes ein physisch anwesender Angreifer genannt. Es wird angenommen, dass dieser einen Besitzer observieren kann und so weiß, wenn das Schloss etwa nicht zugesperrt wurde. Weiters kann der Angreifer physisch mit dem Schloss interagieren, jedoch besitzt er kein autorisiertes mobiles Gerät.
- Als nächstes wird angenommen, dass der Angreifer bereits ein autorisiertes Gerät besitzt. Dieses Gerät wird jedoch in nächster Zeit von der Liste der autorisierten Geräte genommen.
- Ein Dieb kann ein autorisiertes Gerät von einem Bewohner stehlen.
- Angreifer können eine Relay-Attacke gegen das Türschloss durchführen. Dazu sind zwei Angreifer nötig. Einer muss in der Nähe eines Bewohners sein, ein weiterer muss in der Nähe des Schlosses sein. Beide Angreifer müssen Geräte besitzen, die miteinander mit Bluetooth verbunden sind; des Weiteren muss es möglich sein, dass diese Geräte noch mit zusätzlichen Geräten über Bluetooth kommunizieren können. Es wird angenommen, dass die Angreifer nicht über ein bereits autorisiertes Gerät verfügen.

Angriffe auf intelligente Türschlösser lassen sich in zwei Kategorien einteilen – State Consistency Attacks und Attacken, die zu einem ungewollten entsperren des Schlosses führen.

5.2.1 State Consistency Attacks

State Consistency Attacks lassen sich auf darauf zurückführen, dass die meisten Türschlösser keine eigene Internetverbindung haben (DGC Architektur). Hier wird angenommen, dass das mobile Gerät des Benutzers sowohl den Zustand des Schlosses zum Server des Herstellers, als auch die Updates des Servers zum Schloss weiterleitet. Unterbricht man diese Annahme, ist es möglich einige Angriffe durchzuführen [7].

5.2.1.1 Revocation Evasion

Bei Revocation Evasion Attacken ist es möglich, mit autorisierten Geräten, deren die Autorisierung widerrufen wurde, nach wie vor Schlösser zu sperren und zu entsperren. Dieser Angriff wird durch eine schlechte Implementierung der DGC Architektur ermöglicht. Wenn der Owner ein Gerät von den autorisierten Geräten entfernt, wird vom Server eine Push-Nachricht an das jeweilige Gerät gesendet. Wenn dieses Gerät jedoch nicht mit dem Internet verbunden ist, kommt diese Nachricht nicht an. Das Gerät kann die Nachricht dementsprechend nicht an das Türschloss weiterleiten. So ist es möglich, mit einem bereits unautorisierten Gerät das Türschloss zu bedienen.

5.2.1.2 Access Log Evasion

Bei diesem Angriff wird versucht, das Protokollieren von Zugriffen zu verhindert. Das wird durch, gleich wie bei der Revocation Evasion Attacke, das Entfernen der Verbindung zwischen dem mobilen Endgerät und dem Server des Herstellers möglich. Da die Schlösser die Zugriffe selbst nicht protokollieren, sondern das Protokoll vom mobilen Gerät selbst zum Server gesendet wird, reicht es, das Gerät vom Internet zu trennen. So ist es möglich, dass die Protokollevents nie den Server erreichen.

5.2.2 Ungewolltes Entsperren

Wie schon vorweggenommen, sperren und entsperren viele Türschlösser automatisch, sobald ein autorisiertes Gerät in Reichweite von BLE ist. Diese Funktion kann für zwei weitere Angriffe missbraucht werden [7].

5.2.2.1 Unabsichtliches Entsperren

Das automatische Sperren und Entsperren kann auf zwei Arten Implementiert werden. Einerseits rein durch das Eintreten der Reichweite von BLE, andererseits durch einen zusätzlichen Touch-Sensor der betätigt werden muss.

Erstere Implementierung hat den Nachteil, dass durch das simple Bewegen von autorisierten Geräten, Schlösser entsperrt werden. Wenn nun ein Bewohner etwa durch eine Hintertür die Wohnung betritt, ist es möglich, dass auch die Haupteingangstür automatisch und ungewollt entsperrt wird.

Die Implementierung durch einen zusätzlichen Touch-Sensor für das Entsperren der Tür umgeht solche Probleme. Trotzdem könnte man annehmen, dass etwa durch das Vergessen eines autorisierten Gerätes in der Wohnung ein Einbrecher lediglich den Sensor berühren kann, um die Wohnung zu betreten. Dieselbe Annahme kann man treffen, sobald ein Bewohner sich in der Wohnung befindet. Tatsächlich hat das untersuchte Gerät von Ho et al. eine Sicherheitsfunktion eingebaut, dass diese Umstände verhindern sollen. Dazu wird vom Gerät die Bluetooth-Funktion *directional sensing* verwendet. Diese Funktion erlaubt es festzustellen, ob sich das Gerät innerhalb oder außerhalb der Wohnung befindet. Diese Implementierung funktioniert für gewöhnlich sehr gut, kann jedoch bei verwinkelten Wohnungen zu Problemen führen, wie Abbildung 1 [7] zeigt.

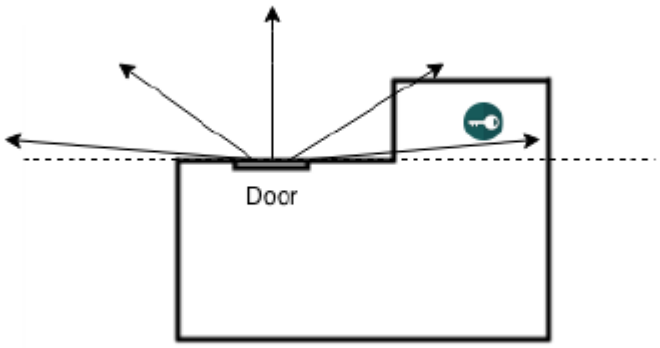

Abbildung 1: Probleme von Bluetooth Directional Sensing

Hier ist zu sehen, dass ein autorisiertes Gerät sich in einem Raum befinden kann, dass seitlich vor dem Schloss ist. Das Türsystem nimmt demnach an, dass sich das Gerät vor der Wohnung, also außerhalb, befindet.

5.2.2.2 Relay Angriffe

Relay Attacken wurden bereits erfolgreich bei Autos durchgeführt. Dasselbe Prinzip lässt sich auch auf Smart Home Türschlösser ableiten. Dazu muss ein Angreifer in der Nähe von einem Bewohner sein und ein weiterer betätigt etwa den Touch-Sensor des Türschlosses. Das Türschloss sendet eine Challenge zum Angreifer, dieser leitet diese zum Komplizen weiter, der diese Challenge an das Gerät vom Bewohner leitet. In umgekehrter Reihenfolge wird nun die Antwort des autorisierten Gerätes an das Türschloss geleitet. Bei erfolgreichem Angriff kann so das Schloss entriegelt werden.

Bei einer reinen Standortabfrage des Gerätes, ohne dass ein Touch-Sensor benötigt wird um das Schloss zu entsperren, kann diese Attacke mit geo-spoofing und weiterleiten der Challenge vom autorisierten Gerät erfolgreich sein [7].

5.3 Gegenmaßnahmen

In diesem Kapitel werden die Gegenmaßnahmen zu den in Kapitel 5.2 beschriebenen Risiken evaluiert.

5.3.1 State Consistency Attacks

Es gibt verschiedene Ansätze, State Consitency Attacks zu verhindern. Bei Türschlössern mit DGC Architektur tritt diese Schwachstelle auf, weil diese keine eigene Verbindung zum Server des Herstellers aufbauen kann. Im Normalfall wird eine Verbindung über das mobile Gerät des Benutzers aufgebaut; damit können sich Schloss und Server einerseits synchronisieren, was zu Konsistenz führt, andererseits werden so auch alle Zugänge zum Schloss autorisiert bzw. nicht autorisiert, was zur konstanten Erreichbarkeit des Dienstes führt. Wenn nun das Smartphone des Benutzers die Verbindung zum Server nicht aufbaut, gibt es für das Sicherheitssystem zwei Möglichkeiten. Zum einen kann, wenn das Schloss ohne auf die Abgleichung mit dem Server

Zutritte gestattet bzw. verweigert, die Konsistenz gefährdet werden. Zum anderen kann das Schloss auch verweigern Funktionen ohne Verbindung zum Server auszuführen, was jedoch der Erreichbarkeit des Dienstes schadet, da etwa Bewohner von ihrer Wohnung ausgesperrt werden können [7].

Ho et al. schlagen in ihrer Studie das Konzept der *Eventual Consistency* vor. Dieses besagt, dass Türschlösser zusätzlich eine Access Control List (ACL) haben, auf die zurückgegriffen wird, wenn der Server nicht verfügbar sein sollte. Um dieses Konzept zu implementieren, sollten Schloss und Server einen symmetrischen Schlüssel besitzen, der für eine sichere Ende-zu-Ende-Verschlüsselung verwendet wird. Die aktuelle ACL wird am Server gespeichert. Bei jedem Zugriff von einem mobilen Gerät auf das Schloss wird eine vom Server signierte und mit einem Timestamp versehene ACL geholt und zum Schloss weitergeleitet. Sollte die neu erhaltene ACL aktueller sein, als die vom Schloss gespeicherte, wird diese aktualisiert. Dieses Konzept verhindert eine im Kapitel 5.2.1.1 beschriebene Revocation Evasion nicht ganz. Jedoch ergibt sich dadurch ein relativ schmales Zeitfenster, in dem der Angreifer mit einem eigentlich nicht mehr autorisierten Gerät das Schloss öffnen kann, da ein legitimer Benutzer lediglich einmal mit dem Schloss interagieren muss, um die Liste zu aktualisieren [7].

Auch die im Kapitel 5.2.1.2 beschriebene Access Log Evasion Attacke kann damit verhindert werden, wenn das Schloss nicht nur eine ACL speichert, sondern auch die Protokolleinträge. Diese werden bei jedem Interagieren mit dem Schloss an den Server gesendet. Wie schon für den vorherigen Angriff gilt hier, dass der Angreifer nur eine kurze Zeitspanne hat, bis der Server alle aktuellen Einträge bekommt.

Für Sicherheitssysteme, die eine direkte Internetverbindung haben, kann der Server direkte Updates an das Schloss senden; das passiert ganz unabhängig von dem Endgerät des Benutzers. Der Grund, warum dieses Konzept nicht sehr häufig vertreten ist, ist, dass es zum einen die Geräte teurer macht, da zusätzliche Komponenten verbaut werden müssen und zum anderen, da es weitere Sicherheitslücken ermöglicht, da das Türschloss direkt mit dem Internet verbunden ist [7].

5.3.2 Ungewolltes Entsperren

Die Risiken beim ungewollten Entsperren entstehen, da die Sicherheitssysteme versuchen auf Kosten der Sicherheit besserer Usability zu bekommen. Durch das simple Anwesendsein eines Benutzers mit einem autorisierten Gerät werden Türschlösser entsperrt, sobald eine gewisse Nähe erreicht wird. Stattdessen sollte von den Sicherheitssystemen versucht werden, die Absicht des Benutzers zu erkennen [7].

Dafür können zwei Technologien verwendet werden: Near Field Communication (NFC) und Distance Bounding Protokolle. NFC ist ein Protokoll, das Kommunikation innerhalb einer sehr geringen Distanz (max. 10cm) ermöglicht. Innerhalb dieser Reichweite könnte angenommen werden, dass der Benutzer beabsichtigt, mit dem Türschloss zu interagieren. Studien haben jedoch ergeben, dass NFC anfällig für Relay Attacken sind, was wieder eine neue Angriffsfläche für Smart Home Komponenten bietet. Zudem ist es auch möglich, dass Angreifer die Reichweite von NFC durch das Einsetzen von Antennen auf bis zu 50 Metern erweitern können [7] [15].

Die bessere Option wäre das Verwenden von Distance Bounding Protokolle. Diese Protokolle setzen auf mehrere Challenge-Response Schritte bei denen jeweils Round Trip Time (RTT), also die Durchlaufzeit, berechnet wird. So kann die Distanz der Geräte genau und sicher berechnet werden. Distance Bounding Protokolle werden derzeit jedoch nicht von BLE unterstützt. Zudem besitzen Smartphones nicht über die nötige Hardware, um diese Verfahren durchführen zu können [7].

6 Energiemanagement

Zum Energiemanagement in Smart Homes gehören Smart Home Energy Management Systems (SHEMS), die Funktionen wie Messung, Kontrolle, Monitoring und die daraus mögliche Optimierung für den Verbrauch von etwa Gas, Wasser und Strom. Zu einem SHEMS gehören fünf Komponenten [16]:

- Verbrauchszähler – zum Erfassen des Verbrauches
- Sensoren – zum Erkennen von Temperatur, Bewegung, Licht, Rauch, etc.
- Integration von Information and Communication Technology (ICT) – ICT wird verwendet um alle Komponenten miteinander zu verbinden. Dazu werden verschiedene Technologien und Protokolle wie Wi-Fi, Z-Wave und ZigBee verwendet
- Smarte Haushaltsgeräte – diese werden in Kapitel 7 näher behandelt
- Energy Management System – Abhängig von Hersteller, kann ein Energy Management System aus eines der folgenden Punkte bestehen. (1) grafische Übersicht über Energieverbrauch, (2) Information, Automatisierung und Kontrolle über den Energieverbrauch, (3) alle Funktionen aus vorherigem Punkt inklusive Vorhersage des Energieverbrauchs

6.1 Risiken

Auch Heizungssteuerungen wurden in der Vergangenheit bereits Cyberattacken ausgesetzt. So wurde beispielsweise im Winter 2016 im finnischen Lappeenranta (bei Minustemperaturen) die Steuerungscomputer der Heizung von mindestens zwei Wohnblocks außer Betrieb gesetzt wurden [17].

6.1.1 Potenzielle Privatsphärenrisiken

Mit Smart Metern, also smarten Verbraucherzählern, kann der Verbrauch unterschiedlicher Energien viel detaillierter analysiert werden. Das führt zu erheblichen Sicherheits- und Privatsphärenbedenken. So ist es etwa möglich, vom Stromverbrauch der Bewohner auf Handlungen und Gewohnheiten zu schließen. Ein niedriger Stromverbrauch lässt etwa darauf schließen, dass die Bewohner gerade schlafen oder nicht zu Hause sind; ein größerer und schwankender Stromverbrauch auf Aktivitäten schließen lassen. Durch eine genauere Analyse können auch sensiblere Gewohnheiten herausgefunden werden:

- Wann gehen die Bewohner zur Arbeit?
- Wie lange arbeiten die Bewohner?
- Was für Fernsehprogramm interessiert die Bewohner?
- Essen die Bewohner warme Speisen zum Frühstück?

Solche harmlosen Fragen können auf den ersten Blick belanglos wirken, können jedoch für Drittanbieter als Werbeinformation oder auch für Versicherungen interessant sein [18]. Zusätzlich dienen diese Informationen auch potentiell Einbrechern oder anderen Kriminellen als Informationsquelle (beispielsweise um herauszufinden wann die Bewohner eines Haushalts nicht zu Hause sind um ungestört einbrechen zu können). Auch Arbeitgeber könnten ein Interesse daran haben, ihre Arbeitnehmer (potentiell widerrechtlich) zu überwachen um Beispielsweise illegitime Krankenstände aufzudecken [19].

6.1.2 Software-Sicherheitslücken

Ein Vorfall in 2014 zeigte anschaulich, dass auch Teile eines SHEMS Implementierungsfehler vorweisen können. Durch verschiedene Sicherheitslücken konnten intelligente Thermostate, die durch falsche Konfiguration vom Internet aus zugänglich waren, manipuliert werden. Angreifer konnten durch unterschiedliche Szenarien in die bereitgestellte Webapplikation eindringen [20] [21]:

- Standard Administrator Zugangsdaten
    - Durch das schlichte nicht Konfigurieren der Webapplikation konnten Angreifer mit einem Blick in die Dokumentation des Produkts eindringen.
- Offenlegung des Administrator Passworts
    - Durch die nicht vorhandene Netzwerkverschlüsselung (HTTP) konnten Passwörter durch simples Sniffing Passwörter ergriffen werden.
- Cross-Site-Scripting (XSS)
    - Unterschiedliche Seiten der Webapplikationen waren anfällig für XSS-Attacken.
- Auslesbare WLAN-Informationen
    - Sobald ein Benutzer an der Webapplikation eingeloggt war, konnten sensible Informationen aus dem Quelltext der Webseite ausgelesen werden. Dazu gehörten Username, Passwort, SSID, WLAN Passwort.
- Clientseitige Inputvalidierung
    - Im Quelltext verschiedener Seiten der Applikation war auch die Inputvalidierung ersichtlich. Validierungen, die ausschließlich durch den Client, welcher normalerweise ein Browser repräsentiert, durchgeführt werden, können jedoch sehr einfach umgangen werden. So kann etwa die Validierung auf korrekte Eingabe von Username und Passwort umgangen werden.
- Unsichere Mobile-Applikation
    - Zusätzlich zu der Webapplikation wurde vom Hersteller auch eine Mobile-Applikation zur Verfügung gestellt. Diese Apps kommunizieren mit dem Thermostat über ein vom Hersteller entwickeltes Protokoll, das zur Sicherheit einen vierstelligen Pin erfordert, der vom Benutzer konfiguriert werden kann. Da das Endgerät jedoch keine Limitierung auf Fehlversuche bereitstellt, kann dieser durch einen simplen Bruteforce-Angriff in kürzester Zeit erraten werden. Dazu

werden alle möglichen Zahlenkombinationen durchprobiert, was bei einer maximalen Anzahl von 10000 Zahlen etwa 1,5 Stunden dauert.

- Fehlerhafte Einschränkung von Ressourcen
    - Sobald einen User die Namen der Ressourcen der Webapplikation bekannt waren, konnten diese ohne Authentifizierung durch die Anmeldeseite erreicht werden. Teilweise wurde versucht diesen Vorgang durch Javascript zu verhindern. Der Angreifer kann jedoch einfach Javascript in seinem Browser abschalten, um diese Sicherheitsmaßnahme zu umgehen.
- Schwieriges Firmware-Upgrade
    - Das Produkt hatte keine Funktion für den Benutzer, um die Firmware zu aktualisieren. Ein Upgrade konnte so nur von einem Techniker des Herstellers durchgeführt werden. Das führte zum Problem, dass Benutzer offensichtliche Sicherheitslücken nicht durch ein simples Aktualisieren durch einen Knopfdruck schließen konnten.

6.1.3 Hardware-Sicherheitslücken

Abseits von klassischen Software Sicherheitslücken wird oft außer Acht gelassen, dass auch die dazugehörige Hardware abgesichert werden muss. Hernandez et al. zeigen in ihrer Studie, dass es bei einem Thermostatprodukt durch zurücksetzen des Produkts möglich ist, von einem USB-Stick zu booten. Da der Thermostat keine kryptografischen Überprüfungen vornimmt, wird automatisch beliebiger Code, der auf dem USB-Stick bereitgestellt wird, ausgeführt. So ist es möglich, dass Unbefugte schädlichen Code einschleusen um etwa Backdoors zu installieren. Durch so einen Angriff kann der Angreifer sich sowohl dauerhaft Zugang zum Netzwerk verschaffen als auch Daten vom Gerät stehlen. Ein solcher Angriff auf das Produkt kann nicht nur durch Personen im eigenen Haus, wie etwa Gäste oder Einbrecher, vorgenommen werden, sondern durchaus auch während der Auslieferung durch den Hersteller oder der Installation durch eine Drittfirma [22].

6.2 Gegenmaßnahmen

Wie allgemein in Smart Homes, sind Zugriffskontrollen wichtig um Heizungssteuersysteme zu schützen. Dies Betrifft einerseits Einschränken des Netzwerkverkehrs durch Segregation und *Rate-Limiting*[1] (siehe Abschnitt 10) und andererseits durch Authentisierung (durch sichere Passwörter und/oder kryptographische Maßnahmen) durchgeführt werden.

6.2.1 Potenzielle Privatsphärenrisiken

Benutzer sollten generell durch gewissenhafte Konfiguration sicherstellen, dass Unbefugte keinen Zugriff auf aufgezeichnete Daten bekommen. Das kann in erster Linie etwa durch ein

[1] Dies war auch zur Behebung des Falles in Abschnitt 6.1 wirksam.

sicheres WLAN-Passwort und aktuelle WLAN-Protokolle (WPA2) geschehen. Weiters sollte sichergestellt werden, dass keine Geräte vom Internet aus erreichbar werden können.

6.2.2 Software-Sicherheitslücken

Viele Sicherheitslücken in Software lassen sich durch richtige Konfiguration schließen bzw. treten erst gar nicht auf. Daher ist es essentiell, dass der Benutzer bei jedem Gerät die dazugehörige Dokumentation durchliest und das jeweilige Produkt sicher konfiguriert. So kann verhindert werden, dass etwa Geräte nicht gewollt vom Internet aus erreichbar sind oder dass voreingestellte Passwörter verwendet werden.

Bekannte Implementierungsfehler seitens der Hersteller können meist durch stetiges Aktualisieren der Software geschlossen werden, sofern solche Features unterstützt werden. Grundsätzlich ist den Herstellern anzuraten Best-Practice-Methoden in der Entwicklung von jeglicher Software zu verwenden, um viele der häufigsten Sicherheitslücken vorbeugen zu können [23].

6.2.3 Hardware-Sicherheitslücken

Um die Sicherheit von Produkten vor dem beschriebenen Angriff zu garantieren, muss der Mikroprozessor des Geräts bei jedem Start den zu ausführenden Code authentifizieren. Viele Prozessoren unterstützen dieses Feature bereits, einige jedoch nicht. Es ist wichtig festzuhalten, dass es weit mehr hardwarebezogenen Sicherheitslücken gibt und der Kunde selbst entscheiden muss, ob er den jeweiligen Hersteller und dessen Produkte vertraut [22].

7 Haushaltsgeräte

In diesem Kapitel werden Haushaltsgeräte begutachtet. Dazu werden Studien über smarte Glühbirnen und Sprinkleranlagen verwendet und analysiert.

7.1 Risiken

Zunächst werden intelligente Glühbirnen näher beleuchtet. Dazu gibt es mehrere, unterschiedlich aktuelle Studien, die nach wie vor dieseleben Probleme aufzeigen, die in Folge beschrieben werden. Grundsätzlich können smarte Glühbirnen dazu verwendet werden, um via Smartphone Applikation oder Webapplikation Lichter ein bzw. auszuschalten und auch die Lichtfarbe zu kontrollieren. Die Kontrolle über die Glühbirnen erfolgt durch eine sich im Netzwerk befindende *Bridge*, die von den jeweiligen Applikationen angesprochen werden kann. Die Funktionen können über Application Programming Interface (API) Endpunkte, die von jedem Gerät innerhalb desselben Netzwerkes aufgerufen werden können, kontrolliert werden. Alle Studien und Berichte über denselben Hersteller zeigen zwar eine stetige Entwicklung, jedoch wurde noch keine endgültige Lösung des Problems entwickelt. Die API-Endpunkte des Kontrollsystems werden alle im Klartext, ohne Verschlüsselung, zwischen den Geräten kommuniziert und lassen sich so leicht mitverfolgen und analysieren. So ist es möglich, API-Token und Keys entweder mitzulesen und für eigene Abfragen zu missbrauchen, oder eigene zu generieren. Hacker, die es schaffen sich zum Netzwerk Zugang zu verschaffen, bzw. Malware können so etwa alle Funktionen kontrollieren und einen permanenten Blackout verursachen [24] [25] [26]. Umgekehrt kann es für Hacker auch interessant sein, Schwachstellen von etwa Glühbirnen auszunutzen, um einen Eintrittspunkt in das Netzwerk zu bekommen.

Auch smarte Bewässerungsanlagen können Risiken beherbergen. Diese Anlagen werden wie auch andere IoT-Geräte über Smartphone Applikationen oder Server gesteuert. Intelligente Sprinkleranlagen können, abhängig von der Wettervorhersage von Drittanbietern oder durch Messungen von eingebauten Sensoren, bestimmen, wann die Bewässerung durchgeführt wird. Die Studie von Nassi et al. hat folgende Motivationen für Angreifer festgelegt [4]:

1. Wasserverschwendung, was in vielen Bereichen der Erde zu einer ernsten Lage führen kann.
2. Finanzschäden verursachen. Dies hat nicht nur Auswirkung auf den Endkunden, sondern auch auf die Städte, die die Wasserversorgung bereitstellt.
3. Den Wasserdruck schwächen. Das kann durch einen gezielten, verteilten Angriff auf mehrere Bewässerungsanlagen versucht werden.

Um diese Risiken zu verifizieren wurde in der Studie gezeigt, wie man diese mit Hilfe eines Botnetzes umsetzen kann. Dazu ist es möglich, die Sprinkleranlagen selbst mit Bots zu infizieren oder aber auch Geräte zu infizieren, die mit dem Internet verbunden sind und im selben lokalen Netzwerk sind wie die Bewässerungsanlagen. Dazu gehören etwa Laptops,

Smartphones, Router, etc. Sobald ein Gerät infiziert wurde, kann durch Netzwerksniffing innerhalb von maximal 15 Minuten erkannt werden, ob sich eine Sprinkleranlage im Netzwerk befindet. Das ist möglich, da die Anlagen mehrmals innerhalb einer gewissen Zeit sich zu Servern des Herstellers verbinden. Diese Server werden unter anderem dazu verwendet, Konfigurationen an die Anlagen zu senden. Die Anlagen überprüfen mittels Timestamps, ob die Konfiguration neuer als die bereits verwendete ist und aktualisieren diese gegebenenfalls. Mittels Address Resolution Protocol (ARP)-Spoofing wurde in der Studie der Datenverkehr zu einem mit einem Bot infizierten Rechner geleitet. Dieser ist in der Lage eine neue Konfiguration mit einem weit in der Zukunft liegenden Timestamp zu versehen und diese an die Bewässerungsanlage zu schicken. So ist es etwa möglich, je nach Absicht des Angreifers, die Anlagen permanent eingeschalten bzw. ausgeschalten zu lassen.

Manche Bewässerungsanlagen machen den Wasserverbrauch auch abhängig von Wettervorhersagen von Drittanbietern. Dazu werden Representational State Transfer (REST)-Schnittstellen der jeweiligen Anbieter verwendet. Durch Spoofing-Attacken können beim Abfragen der REST-Schnittstelle des Anbieters Parameter wie etwa Koordinaten verändert werden um so die Konfiguration zu beeinflussen. Die Studie hat gezeigt, dass smarte Bewässerungsanlagen blind auf die Daten der Drittanbieter vertrauen, auch wenn diese Koordinaten beinhalten, die nicht zum Standort der Anlagen passen.

Beide Methoden lassen sich durch Botnetze zu großflächigen Angriffen umwandeln und können so große Schäden anrichten. Neben finanzielle Schäden sind auch schwerwiegende, katastrophenähnliche Zustände möglich. Nassi et al. haben gezeigt, dass möglich ist, einen durchschnittlichen Wasserturm mittels eines Botnetzes von lediglich 1355 Sprinkleranlagen innerhalb einer Stunde zu leeren.

7.2 Gegenmaßnahmen

Potenzielle Gegenmaßnahmen in Bezug auf das im vorherigen Kapitel analysierte Risiko der smarten Glühbirnen durch fehlende Netzwerkverschlüsselung gibt es für den Endbenutzer kaum. Es ist vor allem notwendig, das Netzwerk vor unbefugten Zutritt, etwa durch starke WLAN-Passwörter und aktuelle Sicherheitsprotokolle zu schützen. Den Herstellern von IoT-Geräten ist anzuraten, aktuelle Verschlüsselungs-, und Autorisierungsverfahren zu implementieren, um solchen Risiken zu vorzubeugen [24].

Auch bei smarten Bewässerungsanlagen wurde festgestellt, dass keinerlei Verschlüsselung angewandt wurde. Durch das Einsetzen von *Transport Layer Security (TLS)* im HTTP-Protokoll (HTTPS) können etwa Spoofing-Angriffe verhindert werden. Eine weitere Maßnahme wäre das Einsetzen von Überwachungssystemen, die ungewöhnlichen Wasserverbrauch früh genug aufzeigen können [4].

8 Persönliche Assistenten

In diesem Kapitel werden persönliche Assistenten untersucht. Dazu wird der Fokus auf Smart Speaker gesetzt, da diese in den letzten Jahren stark an Popularität gewonnen haben. Diese Smart Speaker sollen dabei helfen, das Leben zu vereinfachen indem sie etwa Musik abspielen, Rezepte vorlesen oder auch Produkte bestellen. Obwohl es viele verschiedene Smart Speaker auf dem Markt gibt, funktionieren alle nach demselben Prinzip. Unter den populärsten gehören Alexa (Amazon), Google Assistent (Google), Siri (Apple) und Cordana (Mircrosoft).

8.1 Risiken

Smart Speaker kommen nicht nur mit vielen Funktionen, sondern vor allem mit Bedenken in den Bereichen Sicherheit und Privatsphäre. Da diese Sprachassistenten erst auf ein Signalwort reagieren, ist es notwendig, dass das verarbeitete Mikrofon durchgehend eingeschalten ist. Sobald das Signalwort erkannt wurde, kann ein Befehl an den Speaker gesprochen werden. Dieser Befehl wird mit einem Bruchstück von einer Sekunde vor dem Signalwort aufgezeichnet, in eine Audiodatei konvertiert und zur Cloud des Herstellers gesendet, verarbeitet und bei manchen Produkten auch gespeichert [27]. Kompromittierte Geräte könnten etwa durch das durchgehend eingeschaltete Mikrofon missbraucht werden, um Benutzer auszuspionieren und Daten zu missbrauchen. So könnten Benutzerdaten für zielgerichtete Werbung oder in autoritären Staaten für politische Unterdrückung missbraucht werden.

8.1.1 Nicht autorisierte Verwendung

Ein Risiko das diese Implementation öffnet, besteht darin, dass etwa Gäste, Einbrecher, Kinder oder auch auditive Medien ohne das Wissen der Besitzer, das Gerät bedienen können [8]. So sind etwa Fälle bekannt, in denen Kinder etwa ohne Einverständnis der Eltern Spielzeug bestellen konnten [28]. Smart Speaker konnten auch schon von Fernsehwerbungen und Sendungen aktiviert werden [29] [30]. Neben diesen Attacken, die man als Besitzer zumindest durch Kontrolle und anwesend sein verhindern kann, haben Forscher die *DolphinAttack* nachweisen können. Diese Attacke basiert darauf, dass valide Sprachkommandos auf eine für Menschen nicht hörbare Frequenz konvertiert und abgespielt werden. Dadurch, dass die Frequenz von Mikrofonen und somit auch für Smart Speaker leicht erkannt werden, können so Befehle abgesetzt werden [31].

Neben auditive Angriffe können Angriffe auch von innerhalb des Netzwerkes kommen. So können Angreifer zum Beispiel den Google Chromecast Service nutzen um Einstellungen am Google Home Smart Speaker zu ändern. Beispiele dafür sind etwa die Lautstärke von Geräten, das Einschalten des Gast Modus und Auslesen des PIN Codes. Weiters ist möglich, das Gerät auf Werkeinstellung zurückzusetzen, was einer DoS-Attacke gleicht [8].

8.1.2 Privatsphäre

Wie zu Beginn von Kapitel 8.1 schon erwähnt, warten Smart Speaker auf ein konfiguriertes Signalwort, bevor es mit dem Aufzeichnen und Verarbeiten des Kommandos beginnt. Nachdem dafür das Mikrofon der Geräte permanent eingeschaltet sein muss, kommen verständlicherweise Bedenken hinsichtlich der Privatsphäre auf. Zudem können Benutzer dem Gerät auch Zugriff auf private Kalender und Emails geben, was eine mögliche Kompromittierung noch gefährlicher macht. Sobald ein Befehl vom Gerät erkannt und aufgezeichnet wurde, wird dieser verschlüsselt zum Backend-Service des Herstellers verschickt und gespeichert. Alle Daten können etwa bei Google und Amazon mit dem jeweiligen Benutzerkonto gesehen, gelöscht und nochmal abgespielt werden. Zudem werden die gespeicherten Daten vom Hersteller verwendet, um das Service zu trainieren und besser zu machen. Nichtsdestotrotz können diese Daten an falsche Hände gelangen, sollte ein Hacker Zugriff auf das Benutzerkonto bekommen [8].

8.2 Gegenmaßnahmen

Die Gegenmaßnahmen zu den in Kapitel 8.1 beschriebenen Risiken belaufen sich in erster Linie auf richtiges Konfigurieren der Devices, so dass diese nicht von unautorisierten Personen und anderen Medien missbraucht werden können.

Generell sollte vermieden werden, sicherheitskritische Funktionen wie Türschlösser oder Alarmanlagen mit Sprachassistenten zu verknüpfen. Damit wird verhindert, dass fremde Personen, wie etwa Einbrecher, ungehindert die Wohnung betreten können. Weiters sollten Sprachassistenten nicht dazu verwendet werden, sich sensible Informationen wie Passwörter oder Kreditkartennummern zu merken. Es ist auch möglich, einen Signalton zu aktivieren, der zu Beginn und zu Ende von Aufzeichnungen abgespielt wird. Außerdem ist es möglich, alle aufgezeichneten Audiodateien in der Cloud des Herstellers zu löschen. Das kann zwar den Service daran hintern, die Aussprache des Benutzers zu lernen und sich so zu verbessern, kann jedoch auch die Privatsphäre des Benutzers verbessern [8].

Eine weitere Absicherung gegenüber unautorisiertes Verwenden von Smart Speakern ist, das voreingestellte Signalwort in ein neutrales, nicht häufig gebrauchtes Wort zu ändern. Zudem kann es hilfreich sein, den Sprachassistenten nicht in der Nähe von Fenstern, Türen und Geräten wie Fernseher und Radios zu platzieren. So kann nicht nur verhindert werden, dass etwa Kriminelle versuchen Türen zu öffnen, sondern auch, dass durch andere Medien wie Fernsehwerbungen das Gerät aktiviert wird [27].

Um nicht gewollte Bestellungen zu verhindern, ist es möglich diese Funktion ganz auszuschalten. Alternativ ist es bei vielen Geräten möglich, einen PIN-Code für Einkäufe einzustellen [8] [27].

9 Kommunikationsprotokolle

Kommunikationsprotokolle sind ein Querschnittsthema, das sich über alle in den vorhergehenden Kapiteln beschriebenen Anwendungsfelder spannt. Die hier beschriebenen Protokolle stehen exemplarisch für spezifische IoT-Protokolle, die in Smart Homes verbreitet sind. Die möglichst sichere Konfiguration der Protokolle selbst befindet sich meist außerhalb der Einflusssphäre von Anwendern, die Sicherheit der Protokolle selbst auch außerhalb jener von Experten. Dieses Kapitel soll daher eine Hilfestellung geben, welche Protokolle prinzipiell sicherer oder unsicherer sind um Anwendern Hinweise aus Sicherheitssicht zu geben welche Produkte sie größerer Gefahr aussetzen. Die Entscheidung ist auch wichtig, da die Produkte mit ihrer Kommunikation untereinander kompatibel sein müssen.

Prinzipiell bieten die hier vorgestellten Protokolle Sicherheitsmechanismen zur Gewährleistung der Vertraulichkeit, Integrität und Authentizität der übertragenen Daten durch Verwendung des *Advanced Encryption Standard (AES)*. Einerseits gibt es jedoch teilweise Unterschiede in der Konfiguration (z.B. *Cipher Modes*) dieses kryptographischen Standards und andererseits auch Unterschiede in der Ausgestaltung sicherheitskritischer Prozesse.

Während von den Protokollen selbst her neuere Versionen von Bluetooth und Z-Wave als sicherer anzusehen sind als Zigbee, können sich auch in an sich sichereren Protokollen Verwundbarkeiten durch die jeweilige Herstellerimplementierung ergeben. Hier kann lediglich auf Tests von Einzelprodukten zurückgegriffen werden.

Allgemein ist es wichtig, darauf zu achten, dass jeweils die neuste Protokollversion sowie die jeweiligen Sicherheitsfeatures, die diese bereitstellt, zu verwenden. Fall dies (durch Konfiguration) möglich ist, sollte dabei die Rückwärtskomptabilität deaktiviert sein, um Unsicherheiten durch ältere Sicherheitsmechanismen bzw. *Downgrade-Attacken* zu vermeiden.

9.1 Z-Wave

Abbildung 2 : Z-Wave Logo

Neuere Versionen von Z-Wave definieren zwei Sicherheitsklassen: *Security 0 (S0)* und *Security 2 (S2)*; daneben können sich auch ungesicherte Geräte in einem Z-Wave-Netzwerk befinden. Erstere Klasse entspricht der Sicherheit früherer Versionen und ist als Maßnahme zur Rückwärtskomptabilität zu

sehen. S2 ist die höhere Sicherheitsklasse, die sich wiederum in drei Unterklassen gliedert: *S2 Access Control, S2 Authenticated* und *S2 Unauthenticated*. Alle diese Klassen verwenden AES-128-CCM Verschlüsselung und das Elliptic Curve Diffie Hellman (ECDH) Verfahren mit Curve25519-256, was den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entspricht [32]. Die Subklassen *Access Control* und *Authenticated* sind im Wesentlichen ident und dienen dazu, sicherheitskritische Geräte (wie Türschlösser o.Ä. – *Access Control*) von anderen, potentiell verwundbaren Haushaltsgeräten (*Authenticated*) zu trennen. Die *Unauthenticated*-Subklasse dient dazu, mit Geräten zu kommunizieren, die keine Authentisierung unterstützen. Kommunikation mit *S0*-Geräten (zur Rückwärtskomptabilität) wird ebenfalls über diese Subklasse abgewickelt. Dieses Schichtenmodell soll gewährleisten, dass unsichere Geräte, bei bestehender Interoperabilität, die Sicherheit höherwertiger Geräte nicht gefährden. Die Durchsetzung obliegt dabei dem jeweiligen Controller [33].

Unabhängig von diesen Subklassen kann aufgrund der Abwärtskompabilität durch eine *Downgrade*-Attacke der initiale Schlüsselaustausch (*Pairing*) mit einem Sicherheitsgerät von S2 auf jenen von S0 zu zwingen[2]. Dieser gilt deshalb als verwundbar, weil er den Netzwerkschlüssel ungesichert[3] überträgt und daher abgehört werden [34]. Sicherheit dagegen bietet nur die Zurückweisung von S0-Pairings; der Standard sieht hier jedoch lediglich eine Warnpflicht eines entsprechenden Z-Wave Controller-Geräts vor. Verbraucher sind daher dazu angehalten, falls möglich, nur Geräte zu kaufen, die S0 nicht unterstützen (was jedoch in der Praxis mangels sowohl Kundenexpertise als auch Herstellerinformation oft schwierig ist) oder zumindest entsprechende Warnungen eines Controller-Gerätes nicht zu ignorieren.

9.2 Zigbee

Abbildung 3 : ZigBee Logo

Zigbee verwendet acht Levels (0-7) um die Kommunikationssicherheit zu gewährleisten [35], wobei nur die oberen vier Levels verschlüsselt und nur die obersten drei Levels ausreichende Integrität und Authentizität der Daten (mittels AES-128-CCM*[4] [36]) sichern[5] [37]. Diese Sicherung kann auf Netzwerk- oder Applikationsebene stattfinden. Ersteres ist für eine alleinige Sicherheit kaum ausreichend, da der dazugehörige Schlüssel entweder statisch

[2] Da die Sicherheitsklasse ungesichert übertragen wird und daher manipulierbar ist.

[3] Mit einem fixen Schlüssel von *„0000000000000000“*

[4] Eine leicht modifizierte Variante von AES-128-CCM.

[5] Die Levels 0 und 4 sind unauthentifiziert. Die Levels 1-3 verwenden zwar Authentifizierung und Integritätsprüfung, welche jedoch ohne die Kombination mit Verschlüsselung nicht empfohlen wird, da sie alleinstehend Schwachstellen aufweist.

oder über einen unverschlüsselten Kanal verteilt werden muss und überdies dem gesamten Netzwerk bekannt ist, was durch das Kompromittieren eines Gerätes die Sicherheit des gesamten Zigbee-Netzes gefährdet [36]. Zusätzlich kann durch Ausnutzen eines eingebauten Fall-back-Mechanismus auf einen öffentlich bekannten Schlüssel[6] zurückgegriffen werden [38]. Für die Schlüsselverteilung auf Applikationsebene verweist die Zigbee-Spezifikation auf höhere Protokolle [35]. Dadurch lässt sich durch Zigbee alleine ohne Hilfe durch höher liegende Mechanismen (z.B. eine *Transport Layer Security (TLS)*-gesicherte Schlüsselübertragung auf Anwendungsebene) keine ausreichende Sicherheit herstellen.

9.3 EnOcean

Abbildung 4 : EnOcean Logo

Um die Authentifizierung, Integritätsprüfung und Verschlüsselung, sowie Schutz gegen Replay-Attacken zu gewährleisten verwendet EnOcean den AES in zwei Varianten: mit *Cipher Block Chaining* (AES-CBC) und *Variable AES* (VAES). Die erste Variante hat in EnOcean eine kleine Schwachstelle. Der *Initialisierungsvektor (IV)* sollte nicht vorhersehbar sein [39], da sonst potentiell *Dictionary*-Attacken möglich sind, die eventuell das Auslesen und Manipulieren von Daten und/oder das Aushebeln der Authentifizierung ermöglicht[7]. Dies ist jedoch in EnOcean der Fall, da die Spezifikation einen konstanten Initialisierungsvektor[8] vorsieht [40]. Die zweite Variante, VAES, ist eine in EnOcean spezifizierte Abwandlung des AES im *Counter Mode (AES-CTR)*, wobei sich der benötigte Zähler aus einem öffentlich bekannten Teil und einem fortlaufenden *Rolling Code* zusammensetzt. Dieser sollte, ähnlich wie der IV in der ersten Variante, mit einem nicht vorhersehbaren, d.h. (pseudo-)zufälligen, Wert beginnen. Wie bei andren Protokollen müssen bei beiden Varianten zuvor Parameter (inklusive eines *Sitzungsschlüssels* zur Verschlüsselung der Kommunikation) ausgetauscht werden. Dies kann über vorher festgelegte Schlüssel (*Pre-shared Keys*) abgesichert werden. Diese, für eine größere Anzahl an Geräten jedoch recht umständliche, Methode ist der einzige Weg zur Absicherung dieses (auch *Pairing* genannten) Vorgangs. Sonst werden diese Daten auf komplett ungesicherte Weise im so genannten *Teach-in Mode* übertragen, daher sollten unbedingt *Pre-shared Keys* verwendet werden. Prinzipiell muss der Schlüsselaustausch allerdings physisch initialisiert werden, was eine zusätzliche Hürde für

[6] „ZigBeeAlliance09"

[7] https://cwe.mitre.org/data/definitions/329.html

[8] Alle Bytes sollten auf 0 gesetzt werden.

Angreifer darstellt, weshalb EnOcean (mit den obigen Einschränkungen) als relativ sicheres Protokoll gelten kann [41].

9.4 Bluetooth Low Energy (BLE)

Abbildung 5 : Bluetooth Smart Logo

Wie die anderen behandelten Protokolle verwendet prinzipiell auch BLE (auch *Bluetooth Smart*) den AES (128 Bit im CCM-Modus) zur Absicherung der Kommunikation [42]. 2014 wurde die Version 4.2 von *Bluetooth Low Energy (BLE)* veröffentlicht. Diese brachte aus Sicherheitssicht zwei große Neuerungen: einerseits die Integration von IPv6 mit all seinen Stärken und Schwächen gegenüber IPv4 (vor allem der Möglichkeit genereller Ende-zu-Ende-Verbdinungen für viele kleine IoT-Geräte) und andererseits *LE Secure Connections.* Ersteres macht IoT-Geräte aus dem Internet zu- und damit angreifbar, was erweiterte Techniken zur Absicherung notwendig macht. Parallel wurde für den Schlüsselaustausch das unsichere [43], sogenannte *LE Legacy Pairing* durch die *Secure Connections* ersetzt, dass *Elliptic Curve Diffie Hellman (ECDH)* zum Schlüsselaustausch einsetzt. Allerdings ist, wie bei *Z-Wave* (siehe 9.1) auch hier anzunehmen, dass ein *Downgrade*-Angriff möglich ist. Um jedoch Man-in-the-Middle Attacken beim Pairing zu erschweren, kann dieser, wie auch bei EnOcean, physisch abgesichert werden. BLE bietet hierzu vier Möglichkeiten: keine Interaktion oder einfaches Bestätigen (*Just Works*), Prüfziffernvergleich auf beiden Geräten (*Numeric Comparison*), Eingabe einer Prüfziffer (*Passkey Entry*) oder Authentisierung über ein separates Protokoll (*Out of Band*) [42].

10 Conclusio

Dieses Dokument fasst gängige Risiken zusammen, die in einem gängigen, State of the Art Smart Home auftreten. Generell ist dazu zu sagen, dass sich viele Schutzmaßnahmen entweder der Einflusssphäre der Konsumenten vollständig entziehen (da sie in der Hand von Herstellern oder Installateuren liegen) oder Know-how erfordern, dass von Verbrauchern nicht vorauszusetzen ist. Dies führt dazu, dass Systeme auch bei verfügbaren technisch sehr ausgereiften Sicherheitskonzepten durch deren mangelnde oder falsche Nutzung potentiell verwundbar sind [44].

Die Open Web Application Security Project (OWASP) Foundation stellt regelmäßig die häufigsten Schwachstellen in unterschiedlichen Bereichen zusammen, das Ergebnis ist als OWASP Top 10 bekannt. Auch im IoT-Bereich gibt es von OWASP eine Liste der Top zehn verbreitetsten Schwachstellen. Diese werden in Table 1 OWASP Top 10 IoT Schwachstellen aufgelistet [45].

BEZEICHNUNG	TITLE
I1	Insecure Web Interface
I2	Insufficient Authentication/Authorization
I3	Insecure Network Services
I4	Lack of Transport Encryption/Integrity Verification
I5	Privacy Concerns
I6	Insecure Cloud Interface
I7	Insecure Mobile Interface
I8	Insufficient Security Configurability
I9	Insecure Software/Firmware
I10	Poor Physical Security

Table 1 OWASP Top 10 IoT Schwachstellen [45]

In den beschriebenen Risiken und Gegenmaßnahmen der unterschiedlichen Kapitel in dieser Studie wurden alle Punkte der Tabelle behandelt und beschrieben. Viele sind vom Endnutzer nicht beeinflussbar, da die von den Herstellern ausgehend behandelt werden müssen. Dem Endnutzer ist anzuraten, sich über die verwendeten Standards und Technologien des Produktes zu informieren.

Generell empfehlenswert ist, unabhängig von den eingesetzten Produkten, folgende Vorgangsweisen (sofern möglich):

- Authentifizierung durch sichere Passwörter [10], die nicht dem Hersteller-Default entsprechen
- Falls möglich (speziell bei Gerät-zu-Gerät-Kommunikation) Authentifizierung durch kryptographische Maßnahmen (z.B. Zertifikate)
- Möglichst starke Segregation des Netzwerks
    - Trennung zwischen Internet und Heimnetz
    - Trennung Smart Home Geräte-Netz und allgemeinem Netz für Notebooks, etc.,
    - Trennung zwischen kritischen (z.B. Heizungsanlage) und weniger kritischen Bereichen.

  Hierbei sollte eine Firewall eingesetzt werden, die nur die unbedingt nötigen Verbindungen zulässt (*Whitelisting*).
- Einspielen der neuesten (Sicherheits-)Updates (idealerweise automatisiert)
- Verwenden jeweils neuester Protokollversionen (z.B. für Bluetooth Version 5) und, wenn möglich, deaktivieren älterer Versionen
- Verwenden von Protokollsicherheitsfeatures (Verschlüsselung z.B. via HTTPS)
- Deaktivieren nicht verwendeter Dienste (speziell solche, die Schnittstellen des Smart Homes im Internet zugänglich machen)
- Deaktivieren nicht verwendeter Datenverbindungen (speziell solche, die Daten in Internet z.B. an den Hersteller übertragen)
- Genaues Einsehen der Privacy-Einstellung (falls vorhanden)

11 Referenzen

[1] A. Berg, „Home Smart Home," bitkom, Berlin, 2018.

[2] Connected Living, Mücke und Company & Sturm, „Smart Home Index 2017," Connected Living, 2017.

[3] Deloitte, „Smart Home Consumer Survey 2018," Deloitte, 2018.

[4] B. Nassi, M. Sror, I. Lavi, Y. Meidan, A. Shabtai und Y. Elovici, „Piping Botnet - Turning Green Technology into a Water Disaster," Ben-Gurion University of the Negev, Beersheba, 2018.

[5] K. Angrishi, „Turning Internet of Things(IoT) into Internet of Vulnerabilities (IoV) : IoT Botnets," 2017.

[6] C. Kolias, G. Kambourakis, A. Stavrou und J. Voas, „DDoS in the IoT: Mirai and Other Botnets," IEEE COMPUTER SOCIETY, 2017.

[7] G. Ho, D. Leung, P. Mishra, A. Hosseini, D. Song und D. Wagner, „Smart Locks: Lessons for Securing Commodity Internet of Things Devices," Proceedings of the 11th ACM on Asia conference on computer and communications security (pp. 461-472), 2016.

[8] C. Wueest, „A guide to the security of voice-activated smart speakers," Symantec, 2017.

[9] A. Jacobssona, M. Boldt und B. Carlsson, „A Risk Analysis of a Smart Home Automation System," Future Generation Computer Systems 56, 2016.

[10] P. Grassi, J. Fenton, E. Newton, R. Perlner, A. Regenscheid, W. Burr, J. Richer, N. Lefkovitz, J. Danker, Y. Y. Choong, K. Greene und M. Theofanos, „Digital identity guidelines: authentication and lifecycle management," National Institute of Standards and Technology, 2017.

[11] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli und O. Mehani, „Network-level security and privacy control for smart-home IoT devices," in *2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)*, Abu Dhabi, United Arab Emirates, 2015.

[12] C. H. Gañán, M. Ciere und M. van Eeten, „Beyond the pretty penny: the Economic Impact of Cybercrime," Proceedings of the 2017 New Security Paradigms Workshop on ZZZ (pp. 35-45), 2017.

[13] R. Anderson, C. Barton, R. Böhme, R. Clayton, M. J. G. van Eeten, M. Levi, T. Moore und S. Savage, „Measuring the Cost of Cybercrime," Springer, Berlin, Heidelberg, 2013.

[14] A. Jones, „Cybercrime Effects on Stock Prices," Murray State University, 2016.

[15] Z. Kfir und A. Wool, „Picking Virtual Pockets using Relay Attacks on Contactless Smartcard Systems," IEEE, Tel Aviv, 2005.

[16] Y. Liu, B. Qiu, X. Fan, H. Zhu und B. Han, „Review of Smart Home Energy Management Systems," 2016.

[17] Janita, „DDoS attack halts heating in Finland amidst winter," 07 11 2016. [Online]. Available: http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter. [Zugriff am 30 10 2018].

[18] S. Mikkelsen, „Enforcement of Security and Privacy in a Service-Oriented Smart Grid," Aarhus, 2016.

[19] M. Jawurek, M. Johns und K. Rieck, „Smart metering de-pseudonymization," in *Proceedings of the 27th Annual Computer Security Applications Conference*, Orlando, Florida, USA, 2011.

[20] D. Freamon, „The Darius Freamon Blog," 10 September 2013. [Online]. Available: https://dariusfreamon.wordpress.com/2013/10/09/heatmiser-netmonitor-multiple-vulnerabilities/. [Zugriff am 27 September 2018].

[21] Cybergibbons, „Cybergibbons," 20 September 2014. [Online]. Available: https://cybergibbons.com/security-2/heatmiser-wifi-thermostat-vulnerabilities/. [Zugriff am 27 September 2018].

[22] G. Hernandez, O. Arias, D. Buentellod und Y. Jin, „Smart Nest Thermostat: A Smart Spy in Your Home," Florida, 2014.

[23] OWASP, „OWASP Secure Coding Practices - Quick Reference Guide," 2010.

[24] D. Lodge, „Pen Test Partners," 16 Mai 2018. [Online]. Available: https://www.pentestpartners.com/security-blog/hijacking-philips-hue/. [Zugriff am 18 September 2018].

[25] S. Notray, M. Siddiqiy, H. Gharakheiliy, V. Sivaramany und R. Boreli, „An Experimental Study of Security and Privacy," IEEE, Sydney, 2014.

[26] N. Dhanjani, „Hacking lightbulbs: Security evaluation of the philips hue personal wireless lighting system," 2013.

[27] J. Catherine und A. Orebaugh, „A study of security and privacy issues associated with the Amazon Echo," International Journal of Internet of Things and Cyber-Assurance, 1.1, pp.91-100., Charlottesville, 2018.

[28] A. Liptak, „Amazon's Alexa started ordering people dollhouses after hearing its name on TV," 7 Jänner 2017. [Online]. Available: https://www.theverge.com/2017/1/7/14200210/amazon-alexa-tech-news-anchor-order-dollhouse. [Zugriff am 17 September 2018].

[29] K. Opam, „Google's Super Bowl ad accidentally set off a lot of Google Homes," 5 Februar 2017. [Online]. Available: https://www.theverge.com/2017/2/5/14517314/google-home-super-bowl-ad-2017. [Zugriff am 17 September 2018].

[30] J. Kastrenakes, „Burger King's new ad forces Google Home to advertise the Whopper," 12 April 2017. [Online]. Available: https://www.theverge.com/2017/4/12/15259400/burger-king-google-home-ad-wikipedia. [Zugriff am 17 September 2018].

[31] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang und W. Xu, „DolphinAttack: Inaudible Voice Commands," ACM, Hangzhou, 2017.

[32] Bundesamt für Sicherheit in der Informationstechnik, „Cryptographic Mechanisms: Recommendations and Key Lengths," 2017.

[33] Sigma Designs, „Introduction to the Z-Wave Security Ecosystem," 2016.

[34] A. Tierney, „Z-Shave. Exploiting Z-Wave downgrade attacks," 2018. [Online]. Available: https://www.pentestpartners.com/security-blog/z-shave-exploiting-z-wave-downgrade-attacks/ . [Zugriff am 17 07 2018].

[35] Zigbee Alliance, „Zigbee Specification 05-347-21," 2015.

[36] M. Kraußе und R. Konrad, „ZigBee-Sicherheit," in *Drahtlose ZigBee-Netzwerke: Ein Kompendium*, Wiesbaden, : Springer Fachmedien Wiesbaden, 2014, pp. 333-356.

[37] S. Marksteiner, E. a. J. V. Jiménez, H. Vallant und H. Zeiner, „An overview of wireless IoT protocol security in the smart home domain," in *Proceedings of 2017 Internet of Things Business Models, Users, and Networks Conference (CTTE)*, New York, NY, USA, 2017.

[38] T. Zillner, „ZigBee Exploited - The good, the bad and the ugly," in *Presented as part of the BlackHat 2015 Conference*, Las, 2015.

[39] M. Dworkin, „Recommendation for Block Cipher Modes of Operation," National Institute of Standards and Technology, 2001.

[40] EnOcean GmbH, „Security of EnOcean Radio Networks V1.9," 2013.

[41] K. Jonas, B. Vogl und M. Rademacher, „Security Mechanisms of wireless Building Automation Systems," Hochschule Bonn-Rhein-Sieg, Sankt Augustin, 2017.

[42] Bluetooth SIG, „Bluetooth Core Specification v5.0," 2016.

[43] M. Ryan, „Bluetooth: With Low Energy Comes Low Security," in *Presented as part of the 7th {USENIX} Workshop on Offensive Technologies*, Washington, D.C., 2013.

[44] D. N. Kalofonos und S. Shakhshir, „IntuiSec: a framework for intuitive user interaction with smart home security using mobile devices," in *The 18th Annual IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'07)*, Athens, Greece , 2007.

[45] OWASP, „OWASP," 18 May 2016. [Online]. Available:

https://www.owasp.org/index.php/Top_IoT_Vulnerabilities. [Zugriff am 25 10 2018].

[46] E. Fernandes, J. Jung und A. Prakash, „Security Analysis of Emerging Smart Home Applications,“ IEEE Symposium on Security and Privacy (SP), pp. 636-654, 2016.