TU Graz

KNOW Center

TÜV AUSTRIA

WhitePaper

Figure: shutterstock.com (A. Suslov)

IoT im Smart Home

Seitenkanalangriffe als neue Angriffsform

IoT im Smart Home

Seitenkanalangriffe als neue Angriffsform

Wien, 02/04/2019

TÜV AUSTRIA
HOLDING AG
TÜV AUSTRIA-Platz 1
A-2345 Brunn am Gebirge

DI Hendrik Dettmer
Dipl. Ök. Thomas Doms
DI Christoph Schwald
DI Edvin Spahovic

Technische Universität Graz
Rechbauerstraße 12
A-8010 Graz

DI Peter Aufner
DI Herbert Leitold

Impressum

Abstract

IoT-Geräte werden immer vernetzter. Der rapide Zuwachs an vernetzten Geräten in Haushalten, die zu „Smart Homes“ werden, führt zu einem erheblichen Datenaustausch zwischen den Geräten und auch mit der Außenwelt. Demgegenüber steht häufig eine relativ schwache Absicherung neuer auf den Markt kommender IoT-Geräte gegen unbefugte Zugriffe von außen – und damit gegen Cyberangriffe.

Immer größere Bedeutung erlangen dabei auch relativ neue Angriffsformen wie Seitenkanalangriffe, mit denen sich aus dem permanenten Datenverkehr der Geräte eine Vielzahl an Informationen über die Nutzer in einem Haushalt herausfinden lassen. Dieser Problematik widmet sich der TÜV AUSTRIA zusammen mit dem Know Center und der TU Graz in einem Forschungsprojekt im Rahmen einer Dissertation. Ziel dieser Zusammenarbeit ist die Erarbeitung eines wissenschaftlich fundierten Konzepts zur Bedrohungsanalyse von IoT-Geräten in Heimnetzwerken. Auf Grundlage eines Bedrohungsmodells, das vor allem den generierten Datenverkehr und dessen Absicherung gegen Angreifer betrachtet, wird auf Basis dieses Modells eine Methodik erstellt, um das Vorhandensein möglicher Bedrohungen zu erkennen und ihre Auswirkung auf das Gerät, Anwenderinnen und Anwender sowie das Netzwerk, in dem das Gerät betrieben wird, zu beurteilen.

Insbesondere fokussiert die Methodik auf die Beurteilung der Sicherheit von Consumer-IoT-Geräten hinsichtlich passiven Angriffen auf die Netzwerkkommunikation und gezielter Angriffe aus dem Netzwerk. Die Ergebnisse dieser Untersuchungen werden in die Weiterentwicklung des bestehenden TÜV AUSTRIA-Prüfkataloges für Trusted-IoT-Devices Eingang finden.

Das vorliegende Whitepaper von TÜV AUSTRIA, Know Center und TU Graz soll Herstellern und Anwendern von IoT-Geräten wertvolle Tipps geben, wie Produkte besser vor Angriffen zu schützen sind und wie Endanwender IoT-Produkte in ihren Netzwerken sicherer implementieren können.

Seitenkanalangriffe als neue Angriffsform

Inhalt

1 Smart Home – schöne neue Welt?

Die Zukunftsvision des digitalisierten „smarten" Haushaltes wird Realität. In einem „Smart Home" interagieren Haushalts- sowie Multimediageräte miteinander und werden zentral ferngesteuert. Immer mehr Consumer-IoT (Internet-of-Things)-Hersteller bringen vernetzte Haushaltsgeräte, die einen Mehrwert an Komfort liefern sollen, auf den Markt. Von der Lichtsteuerung, die sich beim Betreten automatisch einschaltet bis zum Kühlschrank, der Einkaufslisten mit dem Internet abgleicht, scheinen die Möglichkeiten nahezu unbegrenzt zu sein.

Zum heutigen Tag gibt es aber keine einheitliche und exakte Definition von Consumer-IoT. Eine sehr schlichte Definition wäre es jeden Gegenstand im Haushalt, der mit dem Internet verbunden ist, als „Internet of Thing" zu bezeichnen. Dies hätte zur Folge, dass damit Gegenstände umfasst werden, welche im Allgemeinen nicht als IoT zu betrachten sind, wie z.B. Laptops.

Die ENISA (europäische Behörde für IT-Sicherheit) definiert IoT frei übersetzt als „cyber-physische Ökosysteme von vernetzten Sensoren und Aktoren, die es erlauben Entscheidungen zu treffen". Des Weiteren liegt IoT laut dieser Definition ein stetiger Zyklus von Messen, Entscheiden und Handeln zu Grunde. [1]

In den nachfolgenden Ausführungen wird ein Bezug auf Consumer-IoT im Sinne eines Smart Homes genommen. Damit sind jene Gegenstände gemeint, welche schon länger in vorwiegend privaten Haushalten zum Einsatz kommen, jedoch erst seit jüngerer Zeit um Internet-Konnektivität erweitert und mit App-Integration auf Smartphones versehen wurden.

1.1 State of the Art – Realitätscheck

Bereits heute sind viele alltägliche Haushaltsgeräte mit zusätzlichen digitalen Funktionalitäten bestückt. Stand der aktuellen Technik sind z.B. Sprachassistenten. Dabei handelt es sich um Geräte, welche mittels Sprachbefehlen gesteuert werden können, um so, z.B. Musik per Sprachbefehl abspielen zu können. Gängige Staubsaugerroboter kommunizieren z.B. über W-LAN mit dem Smartphone und können somit von außen gesteuert werden. W-LAN-Überwachungskameras sind ebenfalls mit dem Internet verbunden und senden laufend Daten. Mit Smart-Locks (Türöffner) kommunizieren sogar Türklingeln, die mit einer Kamera versehen sind, über das Internet mit dem Smartphone. Es kann somit, nach Verifikation der Person mittels Kamera, auch die Haustür über das Internet geöffnet werden ohne dass der Bewohner zu Hause sein muss. Mit smarten Glühbirnen ist es möglich diese per Sprachbefehl oder Smartphone anzusteuern.

Smarte Funktionalitäten findet man aber auch in auf den ersten Blick unscheinbaren Haushaltsgeräten, wie z.B. in auf dem Markt erhältlichen smarten Kopfkissen. Mit einem Schlafqualitätstracker ist der Schlafsensor mittels Bluetooth in der Lage Daten zu senden und zu empfangen. Selbst ein Teekocher hat die Möglichkeit Datenaustausch über W-LAN zu betreiben.

1.2 Smart Home – Quo vadis?

Für die technischen Analysen wurde zunächst überlegt, welche Nutzungsszenarien im Bereich Smart Home zu erwarten sind. In naher Zukunft wird möglicherweise nachfolgendes Beispiel ein Szenario eines Smart Homes darstellen. Diverse Geräte, wie z.B. elektrische Zahnbürste, Smart Watches, Radiowecker u.v.m., sind im Smart Home miteinander vernetzt und die Bewohner werden deren Funktionalitäten weitgehend vollumfänglich nutzen.

Bei den vielen Geräten muss zunächst zwischen verschiedenen Konnektivitätsarten unterschieden werden. Hierbei sind besonders W-LAN und Bluetooth zu nennen, die häufig in diesem Umfeld benutzt werden und als Hauptkanäle für mögliche Angreifer interessant sind.

Mittels Bluetooth wird das Gerät mit einem Smartphone und/oder anderen Geräten gekoppelt auf denen eine App installiert ist, welche die erweiterten Fähigkeiten des Gerätes zugänglich und nutzbar macht. Zum Beispiel bietet die App der elektrischen Zahnbürste eine Übersicht über die Qualität der Zahnpflege. Zukünftig könnten diese Daten eventuell auch mit dem eigenen Zahnarzt live als Fortschrittsmonitoring geteilt werden. Es ist möglich mit besonderen technischen Werkzeugen, wie z.B. einem „Ubertooth“ die Kommunikation zwischen Bluetooth-Geräten wie einer solchen Zahnbürsten auszulesen oder zu stören. Hierfür muss man in der Nähe des Gerätes (ca. 10m) sein um idealerweise das erste Pairing der Geräte mithören zu können. Nachdem die Daten vom Gerät auf das Mobiltelefon transferiert wurden, werden diese oft in eine Cloud weitergeleitet.

W-LAN stellt für potenzielle Angreifer aber eine noch interessantere Alternative im Smart-Home-Umfeld dar. Die beste Absicherung für W-LAN ist die Verschlüsselung, aber selbst aktuelle Algorithmen wie WPA2 weisen immer wieder Schwachstellen auf. Um diese auszunutzen muss sich der Angreifer auch wieder in der Nähe des W-LAN aufhalten, kann sich aber aufgrund der größeren Verbindungsreichweite im Vergleich zu Bluetooth, etwas weiter außerhalb der Räumlichkeiten befinden.
Im Fall dass der Verschlüsselungsalgorithmus oder das Passwort nicht sicher gewählt sind, hat ein Angreifer leichtes Spiel mit einem handelsüblichen Notebook und einigen leicht zu beschaffenden Tools, z.B. W-LAN-Sniffer, in das W-LAN einzudringen. Auch wenn immer mehr Hersteller größeren Wert auf Sicherheit legen – und somit die reine Datenübertragung der Geräte auch noch zusätzlich verschlüsseln –, kann der bloße Datenstrom eines Gerätes für einen potenziellen Angreifer sehr aufschlussreich sein. Ebenso steckt die Verschlüsselung von DNS-Anfragen (Anfragen zur Namensauflösung im Internet) noch in den Kinderschuhen. Somit sollte es noch für längere Zeit leicht abzuleiten sein, welchem Hersteller ein bestimmtes Gerät zuzuordnen ist.

Die Sicherheit der Cloudinfrastruktur ist im Allgemeinen als hoch anzusehen. Die meisten großen und bekannten Cloudanbieter sichern ihre Infrastruktur sehr gut ab. Dies kann man auch daran erkennen, dass alle großen Cloudanbieter mit IT-Sicherheitszertifizierungen wie z.B. ISO 27000 werben. Natürlich gibt es auch immer noch genügend Implementierungsfehler auf Seiten der Applikationsentwickler und somit kann man manchmal mit Standardpasswörtern oder einfachen SQL-Injection-Angriffen (Ausnutzen einer Sicherheitslücke in Zusammenhang mit SQL-Datenbanken, die durch mangelnde Maskierung oder Überprüfung von Metazeichen in Benutzereingaben entsteht) diese Webapplikationen angreifen, die auf der Cloud laufen. Diese Backendsysteme werden in diesem Paper nicht detaillierter betrachtet.

Mit diesen Grundlagen beginnen wir unseren Ausflug in das Smart Home der Zukunft.

Zentrales Element dieses Szenarios bildet ein Smart Home, welches als Ausgangspunkt für Angriffe dient. Der Angreifer, ein technisch versierterer Hacker, versucht dabei potenzielle Sicherheitslücken bzw. den Datenaustausch von IoT-Geräten für Manipulationszwecke zu missbrauchen. Der Hacker hat durch eine Sicherheitslücke Zugang zum W-LAN-Router des Hauses bekommen und kann so die Kommunikation von allen Geräten zum Internet mitverfolgen. Diese Art von Sicherheitslücken sind in der Vergangenheit bereits in größerem Umfang aufgetreten.

Die Bewohner des Smart Homes tragen Smartwatches, welche sich zu Hause sofort mit dem W-LAN verbinden. Gelingt es dem Angreifer zuzuordnen wem welche Watch gehört, hat er ein sehr genaues Bild davon, wann wer zu Hause ist.

Geweckt werden sie von ihrem internetverbundenen Radiowecker oder Musiksystem, welche zur bevorzugten Internetradiostation verbinden oder Musik vom bevorzugten Anbieter streamen. Somit lässt sich der Zeitpunkt, wann die Bewohner geweckt werden, sehr genau bestimmen. Noch im Bett liegend werden Kaffeemaschine und Teekocher aktiviert, sowie der Herd für das Frühstücksei vorgeheizt. Da einer der Bewohner immer Kaffee trinkt, die andere Person nur Tee, erhält der Angreifer einen guten Einblick darüber, wer an dem Tag daheim ist.

Zusätzlich werden alle Smart-Light-Profile gesteuert. So spielt nicht nur Musik zum munter werden, es schalten sich zusätzlich auch die Lampen im Schlafzimmer ein. Ein Ereignis, das, wie bereits gezeigt, zumindest ungefähr nachverfolgt werden kann.

In der Küche angekommen entnimmt eine Person die letzten Eier aus dem Kühlschrank, was diesen dazu veranlasst die Shoppingliste zu befüllen. Der Angreifer weiß zumindest, dass dem Kühlschrank etwas entnommen wurde, da dieser eine Kommunikation in die Cloud startet. Diese Kommunikation wird durchgeführt, um dem Benutzer auch unterwegs immer die Möglichkeit zu geben über sein Mobiltelefon den Status seiner Lebensmittel im Kühlschrank mitzuverfolgen. Selbst bei einer gut verschlüsselten Kommunikation mit TLS 1.3 über HTTPS oder ähnlichen Applikationsprotokollen, kann der Angreifer den Zugriff auf den Server und die entsprechende API erkennen und daraus den Schluss ziehen, dass es sich um eine Kühlschrankentnahme handelt.

Sprachassistenten bieten inzwischen die Möglichkeit „Anrufe“ innerhalb des Hauses zu machen. So kann beispielsweise eine Person Essen zubereiten und dann die andere Person im Schlafzimmer anrufen. Die so entstehenden Datenströme erlauben einen Einblick darüber, dass die Personen in unterschiedlichen Zimmern sind. Durch die Architektur dieser Sprachassistenten laufen alle Kommunikationen auch immer über die entsprechenden Cloudanbieter und können über Korrelationen den entsprechenden physischen Systemen im Haus zugeordnet werden.

Nach dem Frühstück gehen die Bewohner ins Badezimmer, der smarte Spiegel lädt sofort Nachrichten und den Wetterbericht herunter um sie den Bewohnern anzuzeigen. Auf diese Weise kann der Angreifer höchstwahrscheinlich erfahren, welche Nachrichten die Personen konsumieren und wann sie im Badezimmer ankommen. Welche Nachrichten konsumiert werden kann für sich eine sehr interessante Informationsquelle sein, da es oftmals auf politische Gesinnung, Hobbies, sexuelle Orientierung, etc. schließen lässt. Die Nachrichten werden von den entsprechenden Servern heruntergeladen, wie z.B. Spiegel, Tagesschau, ORF. Daher kann man alleine durch die DNS-Anfragen zu den Servern schon vermuten, welche Artikel zum Spiegel geladen werden.

Die Bewohner verlassen das Haus, die Bewegungsmelder der Überwachungskameras lösen aus und fotografieren sie dabei, bevor sie die Alarmanlage scharf stellen. Beide Aktionen sind wieder eindeutig im Datenstrom zu sehen, da auch die Alarmanlage die Fotos in die Cloud stellt, um den Bewohnern diese Information immer und überall anzeigen zu können.

Es wäre naheliegend zu vermuten, dass es für die nächsten Stunden sehr ruhig im Netzwerk wird, jedoch bleibt das Smart Home sehr aktiv. Der Staubsaugerroboter beginnt seine Tätigkeit und meldet fleißig den Fortschritt, der

Pflanzenmonitor erinnert daran, dass es abends Zeit wird, die Topfpflanzen zu gießen, während die Bewässerungsanlage außen dafür sorgt, dass der Garten schön bleibt. Inzwischen fahren die Rollos automatisch herunter, weil die Sonne auf die Fenster strahlt und es im Haus beginnt warm zu werden.

Der Thermostat schaltet am späteren Nachmittag automatisch die Klimaanlage ein, damit die Bewohner des Smart Homes sich bei ihrer Heimkehr gleich wohl fühlen. Auch hierbei entstehen viele Datenströme, teilweise zwischen den Geräten direkt, teilweise über Herstellerserver in der Cloud, die ein Angreifer wieder über das Netzwerk sehen kann. Auch mit diesen Datenströmen wird das Wissensnetz dichter.

Am Abend kommen die Bewohner von der Arbeit heim, die Alarmanlage wird abgeschaltet und bald darauf kann der Angreifer Datenströme von abspielender Musik beobachten, die auch wieder über den W-LAN-Router zu den entsprechenden Streamingdiensten, wie z.B. Spotify, stattfinden. Einen Moment später wird eine smarte Steckdose umgeschaltet. Die Bewohner haben ihre Heim-Fitnessgeräte eingeschaltet und trainieren bei Musikbeschallung über das Netzwerk.

Schließlich steht noch ein Film-Abend vor dem Smart-TV an. Die Filme werden von Streamingdiensten bezogen und per W-LAN wird der Ton an das Audiosystem gestreamt. Auch hier kann der Angreifer zumindest über die Netzwerkverkehrsanalyse und die entsprechenden DNS-Requests erkennen, welcher Streaming-Service genutzt wird und wie lange.

Schließlich lädt der Spiegel im Badezimmer nochmals die Nachrichten und ein kurzer Schwall an Datenpaketen sorgt dafür, dass die Lichter im Haus ausgehen.

Diese Skizze soll eine mögliche Zukunft von Smart Homes darstellen. Auch wenn die Hersteller immer mehr Wert auf Sicherheit legen werden, bleiben Seitenkanalangriffswege (siehe 1.5) weiter bestehen. Durch diese kann man viele bis nahezu alle Informationen über das Leben der Bewohner erhalten, ohne Angriffe gegen die eigentlichen kryptographischen Primitiven in den Protokollen, wie z.B. TLS 1.3, vorzugehen. Die Entscheidung, wieviel des eigenen Lebensstils man mit dem Internet teilen möchte, liegt somit bei jedem selbst und sollte im Rahmen einer abgewogenen Risikoeinschätzung getroffen werden.

1.3 Die Bedrohung ist real

Die unsachgemäße Bedienung bzw. die nicht vorhandene Erkenntnis über Gefahren von smarten Haushaltsgeräten führten in der jüngeren Vergangenheit zu einer Vielzahl von Vorfällen, die in den Medien breit diskutiert wurden. An dieser Stelle wollen wir exemplarisch und zur Sensibilisierung nur einige Fälle nennen, welche im Frühjahr 2019 aufgetreten sind. Diese Liste ließe sich beliebig weiterführen.

Ein Sicherheitsunternehmen hat beispielsweise Scooter des chinesischen Unternehmens Xiaomi auf Schwachstellen überprüft und eine potenziell lebensgefährliche Sicherheitslücke entdeckt. Ohne großen Aufwand kann grundsätzlich jeder mit einem Smartphone den Scooter über Bluetooth zum Bremsen oder Beschleunigen bringen. Die zum E-Scooter gehörende App verlangt zwar die Eingabe des Passworts, diese wird jedoch nicht überprüft. Somit können Befehle per Bluetooth entgegengenommen und ausgeführt werden. [2]

Sicherheitsforscher haben bei Kühlsystemen der Firma „Ressource Data Management“ Sicherheitslücken aufgedeckt. Mit einem Default-Benutzernamen in Kombination mit dem Standardpasswort „1234“ können Angreifer via Webbrowser auf weltweit Tausende von Kühlsystemen zugreifen. Zudem fand man heraus, dass diese Kühlsysteme in Supermärkten und Bäckereien bis hin zu Krankenhäusern in Verwendung sind. [3]

Eine Kinder-Smart-Watch des Herstellers Safe-KID-One kann wie in [4] geschildert von Dritten ausspioniert werden. Die Uhr überträgt unverschlüsselt alle Daten zu einem Server und auf diesem kann man ohne jegliche Authentifizierung alle Daten von allen Uhren abfragen. Dies ermöglicht Fremden aus dem Internet die Träger in Echtzeit zu verfolgen und abzuhören. Außerdem könnte ein Angreifer alle vom Benutzer eingepflegten Telefonnummern aus dem Server-Backend der Geräte auslesen.

Und nicht nur im Smart Home-Bereich, sondern generell bei vernetzten Systemen und Geräten gibt es einen dramatischen Anstieg der Angriffszahlen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat 2018 einen erheblichen Zuwachs an Angriffen im britischen Stromnetz festgestellt. In Deutschland zählen Organisationen und Einrichtungen aus den Bereichen Energie, Informationstechnik und Telekommunikation, Transport und Verkehr,

Gesundheit, Wasser, Ernährung, Finanz- und Versicherungswesen, Staat und Verwaltung sowie Medien und Kultur zu den Betreibern kritischer Infrastrukturen. In der zweiten Jahreshälfte gingen 157 Meldungen über IT-Sicherheitsvorfälle auf verschiedenste kritische Infrastrukturen ein. [5]

1.4 Zukünftige Herausforderung in der IT-Sicherheit

Zwar bietet das zuvor beschriebene Zukunftsszenario jede Menge erlebbare Vorteile und einen Komfortgewinn für die Nutzer im Alltag, doch die Realität zeigt, dass auch sehr viel Schaden verursacht werden kann. Die Vernetzung von Haushaltsgegenständen mit dem Internet liefert viele potenzielle Eingriffspunkte über die Geräte und deren Datenkommunikation in das Leben der Bewohner eines Smart Home-Haushaltes. So kann man aus dem Datenverkehr von Geräten verschiedene Informationen über das Leben der Bewohner ableiten. Dies kann beispielsweise erfolgen, wenn schwache Verschlüsselung des Datenverkehres ausgenutzt werden kann. Hierbei muss der Angreifer erst einen Man-in-the-Middle-Angriff auf die Kommunikationsverbindung ausführen. Bei diesem Angriff steht der Angreifer zwischen den beiden Kommunikationspartnern, hat dabei mit seinem System vollständige Kontrolle über den Datenverkehr zwischen zwei oder mehreren Netzwerkteilnehmern und kann die Informationen nach Belieben einsehen und sogar manipulieren. Darüber hinaus müssen die möglichen kryptographischen Schwachstellen wie z.B. ein LUCKY13-Angriff durchgeführt werden. Hierbei ist darauf zu achten, dass immer der korrekte Angriffsvektor für die entsprechende Verschlüsselungsmethode gewählt wird. Bei gravierenden Schwachstellen in kryptographischen Protokollen oder Applikationsschnittstellen kann ein potenzieller Angreifer sogar eine Störung bzw. Manipulation der Geräte hervorrufen, die darüber hinaus das Leben des Bewohners beeinflussen können.

Auch gesellschaftliche Aspekte werden in der Beurteilung der schönen neuen Smart Home-Welt eine immer größere Rolle spielen. Der Mensch läuft Gefahr sich zu sehr auf die Technik zu verlassen, was im Endeffekt zu einer hohen Technikabhängigkeit führen kann. Wenn die Haustür nur noch mittels Smart-Lock geöffnet wird, könnten Stromausfälle einen weitaus größeren Schaden mit sich bringen als in unserer bisherigen analogen Türschlösserwelt.

Ein weiteres großes Thema ist die Datensicherheit. Durch das Hacken von IoT-Geräten können sehr viele Informationen über den Haushalt gewonnen werden und ermöglichen z.B. das Ausspähen der Privatsphäre der Bewohner.

Ein weiteres potenziell verheerendes Szenario bei Smart Grids wird in [6] skizziert. Das Stromnetz bzw. die Stromversorgung einer Stadt bzw. eines Landes wird als kritische Infrastruktur angesehen. Hier stand die Überlegung im Zentrum, was bei Übernahme mehrerer Smart Homes passieren würde. In Zukunft könnten koordinierte Angriffe auf eine Vielzahl an Smart Homes mit hoher Consumer-IoT-Durchdringung erfolgen, um elektrische Verbraucher (Geräte in Smart Home Haushalten) zeitgleich einzuschalten, mit der resultierenden Folge des Zusammenbruchs des gesamten Stromnetzes z.B. in Europa.

1.5 Seitenkanalangriffe

Bei Seitenkanalangriffen handelt es sich um ein relativ neues Forschungsgebiet der IT-Sicherheit. Der Begriff wird daher in unterschiedlichen Bereichen genutzt. Im Bereich der Hardware-Security werden mit der Seitenkanalanalyse physikalische Messgrößen wie z.B. Stromverbrauch, Temperatur, EMV-Abstrahlung etc. messtechnisch erfasst. Aus diesen lassen sich anschließend zusätzliche Informationen für die kryptographische Analyse extrahieren. Die grundlegende Idee dahinter ist, dass während der Bearbeitung der kryptographischen Operation Daten auftreten, die sich direkt auf die Messgrößen auswirken. Aus diesen Änderungen der physikalischen Messgrößen kann nun ein vermeintlich sicherer kryptographischer Schlüssel extrahiert bzw. auch manipuliert werden. [7]

Im Bereich IoT und Smart Home werden Seitenkanalangriffe auch als Analyse von zusätzlichen Informationsquellen betrachtet, um Daten zu extrahieren, die eigentlich vor schweren kryptographischen Problemen geschützt sind. Hierfür werden Datenströme im Netzwerkverkehr gemessen, um aus diesen die Mehrinformationen zu gewinnen. Damit sind auch triviale Mehrinformationen, wie z.B. wann ein Gerät mit seinem Server kommuniziert hat, und nicht unbedingt die Ableitung eines kryptographischen Schlüssels oder anderen sensiblen kryptographischen Informationen wie bei Hardwareseitenkanalangriffen für den Angreifer und sein erfolgreiches Vorgehen von Bedeutung.

2 Side-Channels im Smart Home – eine technische Analyse

2.1 Versuchsaufbau

Der TÜV AUSTRIA beschäftigt sich mit Sicherheitsaspekten, die sich aus dem Zusammenspiel von Consumer-IoT-Geräten im Smart Home ergeben. In Kooperation mit dem Know Center und der TU Graz wurden anhand einer Simulation eines Muster-Smart Homes mögliche Angriffspfade bzw. Manipulationen eines beispielhaften Haushaltes untersucht. Dabei wurden folgende Kernfragen analysiert:

- Ist es möglich ein Zusammenspiel von Geräten aus der Überwachung des Datenverkehrs abzuleiten?
- Ist es möglich aus dem Zusammenspiel von Geräten Informationen über das Leben der Bewohner abzuleiten?

Im Zusammenhang mit der Beantwortung dieser Fragen werden folgende Zusatzfragen beantwortet:

- Nutzen alle eingesetzten Geräte Übertragungsverschlüsselung?
- Welche Informationen können aus dem Datenverkehr einzelner Geräte abgeleitet werden, auch wenn der Datenverkehr nicht entschlüsselt werden kann?
- Können aus den gewonnen Informationen neue Assets abgeleitet werden (z.B. wenn Gerät A und B kommunizieren, muss X stattfinden)?
- Wenn Wege zur Manipulation gefunden wurden, welche Möglichkeiten ergeben sich?

2.1.1 Muster-Smart Home

Zur Veranschaulichung wird eine Auswahl an möglichst unterschiedlichen IoT-Geräten getroffen, die in einem Smart Home zu erwarten sind. Dabei wird kein Anspruch auf Vollständigkeit erhoben, sondern darauf geachtet, dass die gewählten Geräte einen Grad an Zusammenspiel vorweisen. Diese Voraussetzung ist wichtig, da es auch Teil der Analyse ist, mögliche Bedrohungsszenarien, die sich aus genau diesem Zusammenspiel ergeben, zu betrachten.

- Sprachassistent
- W-LAN-Überwachungskamera
- Staubsaugerroboter
- Türöffner
- Lichtsteuerung für das Smart Home

Es wurde vorerst gezielt darauf verzichtet, Geräte, die aktuell noch über keine hohe Verbreitung verfügen, miteinzubeziehen. Beispiele für ein solches Gerät wären ein IoT-Wasserkocher oder eine elektrische Zahnbürste mit App-Anbindung. Beide Geräte würden wohl detaillierte Annahmen über das Verhalten der Bewohner zulassen, jedoch haben sie noch keine hohe Marktpenetration erreicht und würden so das Ergebnis abschwächen, indem sie ein unüblich genaues Netz an Information bereitstellen. Es ist jedoch wichtig, dass sich die Gegenstände der Zukunft genau in diese Richtung entwickeln werden und damit ein genaues Informationsnetz ermöglichen könnten.

Zur Vernetzung der Geräte wird ein Router verwendet. Dieser verfügt über einen ähnlichen Funktionsumfang, wie Modelle, die von Internetprovidern zur Verfügung gestellt werden.

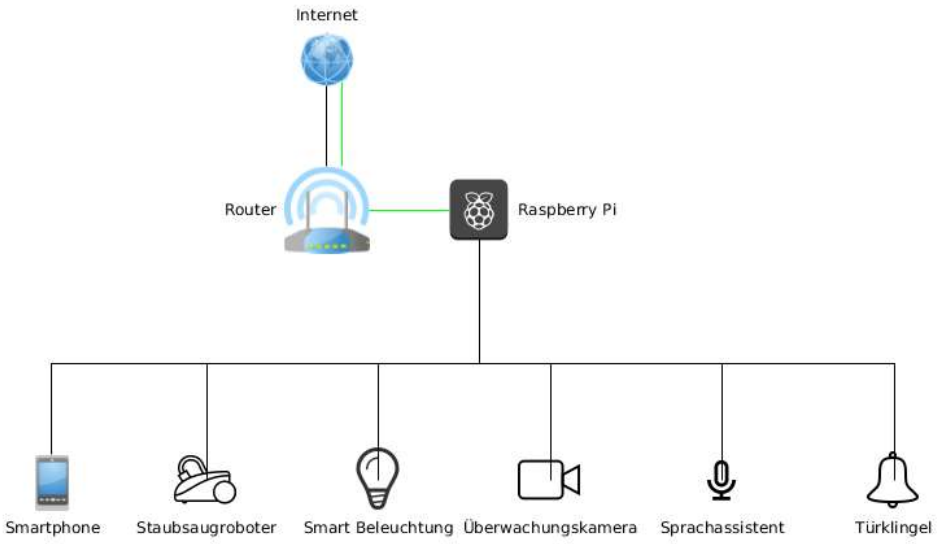


Abbildung 1: Topologie des Netzwerks

Ein Raspberry Pi wird zur Überwachung des Datenverkehrs im Netzwerk genutzt. Zur Simulation des Angriffs wird der Raspberry Pi zwischen die IoT-Geräte und den Router geschaltet, siehe Abbildung 1. In einem echten Smart Home könnte ein Angreifer einen W-LAN-Router, der am Internet angebunden ist, angreifen und übernehmen um an die gleichen oder noch detaillierteren Datenströme zu gelangen. Deswegen stellt die Schaltung des Raspberry Pi keine Verletzung eines realistischen Bedrohungsszenarios dar, da es auch in echten Netzwerken Möglichkeiten, wie z.B. über ARP-Cache-Poisoning gibt, um den gesamten Datenverkehr innerhalb des Netzwerkes über ein beliebiges Gerät zu lenken. Ein ARP-Cache-Poisoning-Angriff muss durchgeführt werden, wenn nicht direkt der Router, sondern nur ein beliebiges Gerät im Netzwerk, wie z.B. ein ungeschütztes IoT-Gerät, vom Angreifer übernommen worden ist.

2.1.2 Bedrohungsmodell

Zur Betrachtung möglicher Bedrohungen lohnt es sich zuerst die Interaktionen zwischen den Geräten und Cloud-Diensten zu betrachten. Annahmen über diese Interaktionen sind in Abbildung 2 dargestellt. Rote Pfeile bedeuten Datenströme zwischen dem Smartphone und einer Cloud, grüne Pfeile zwischen zwei Clouds und blaue Pfeile zwischen einem IoT-Gerät und der Hersteller-Cloud.

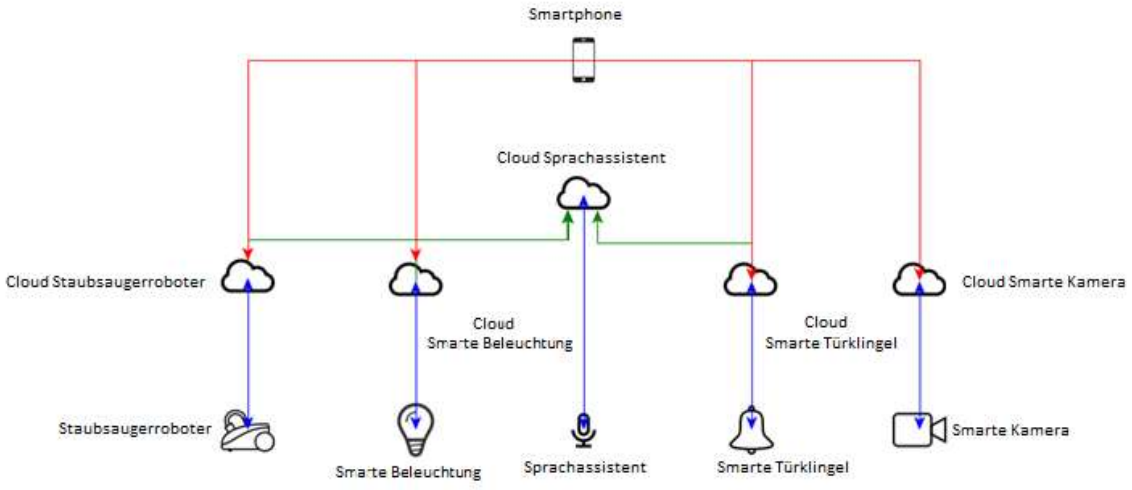


Abbildung 2: Interaktion zwischen Geräten und Clouds

Grundsätzlich wird davon ausgegangen, dass die einzelnen IoT-Geräte nicht untereinander kommunizieren, sondern ausschließlich über die jeweiligen Clouds. Diese Annahme wird dadurch bekräftigt, dass beispielsweise bei der Verbindung zwischen Smart-Light und Sprachassistent während der Installation eine Verbindung zwischen den jeweiligen Cloud-Diensten der Hersteller geschaffen werden muss.

Eine weitere Annahme ist, dass die Steuerung der Geräte entweder über den Sprachassistent von innerhalb des Heimnetzwerkes erfolgt, oder per Smartphone-App sowohl innerhalb als auch außerhalb des Heimnetzwerkes erfolgt.

Daraus ergibt sich, dass die Steuerung via Sprachassistent immer zu Datenströmen sowohl innerhalb als auch außerhalb des Heimnetzwerkes führt. Ebenso führt die Steuerung via Smartphone zu Datenströmen zwischen den Clouds und dem Smartphone, auch wenn dies theoretisch innerhalb des Heimnetzwerkes nicht notwendig wäre.

2.1.3 Modell der Assets

Da sich diese Untersuchung ausschließlich auf die Beobachtung des Datenverkehrs zwischen IoT-Geräten, dazugehörigen Clouds und Steuergeräten wie Smartphones oder Sprachassistenten beschränkt, werden auch nur die hierfür relevanten Teile der IoT-Geräte betrachtet. In ihrer einfachsten Definition können IoT-Geräte als drei-schichtig betrachtet werden:

- Anwendung (Anwenderseite)
- Cloud
- Sensoren und Aktuatoren (Hardwareseite)

Die oberste Schicht, Anwendungen, bezeichnet sowohl die Steuerungsanwendungen auf Smartphones oder Sprachkommandos, aber auch komplexe Anwendungen, die sich aus der Verknüpfung mehrerer IoT-Geräte ergeben.

Die mittlere Schicht bezeichnet Server im Internet, welche Daten von den IoT-Geräten sammeln und sie mit einer höheren Intelligenz ausstatten als es direkt im Gerät möglich wäre.

Die unterste Schicht bildet das Gerät, welches physisch mit der Umwelt interagiert, z.B. indem es den Boden reinigt oder ein Schloss öffnet.

Für die Kommunikation zwischen den drei Schichten ist Datenverkehr über das Heimnetzwerk und über das Internet notwendig.

2.1.4 Modell der Bewohner

Die Bewohner des Smart Homes verfügen über ausreichende technische Kenntnisse zur Inbetriebnahme ihrer Geräte, eventuell unter Zuhilfenahme der Gebrauchsanweisung bzw. dem Befolgen von Anleitungen in Apps. Sie sind keine Experten im Feld der IT-Sicherheit oder von IT-Netzwerken und verwenden ihre Geräte ausschließlich mit Standardeinstellungen. Sollte ein Gerät Härtungsmaßnahmen anbieten, werden diese nicht genutzt. Die Bewohner des Smart Homes sind erwachsen und berufstätig. Üblicherweise sind sie also zu Geschäftszeiten (08:00-18:00) nicht zu Hause. An Wochenenden unternehmen sie gelegentlich Ausflüge, können aber auch die ganze Zeit zu Hause sein.

2.1.5 Modell des Angreifers

Es werden zwei mögliche Angriffsszenarien betrachtet:

- Innerhalb des Heimnetzwerkes
- Außerhalb des Heimnetzwerkes

In beiden Fällen wird davon ausgegangen, dass der Angreifer die gesamte Kommunikation, welche über den jeweiligen Kanal stattfindet, belauschen kann. Es gibt also keine Einschränkungen wie Paketverluste. Bei Angriffen innerhalb des Heimnetzwerkes hat der Angreifer ein Gerät, wie z.B. ein angreifbares IoT-Gerät oder einen Computer im Heimnetzwerk, unter seine Kontrolle gebracht und nutzt Netzwerkumleitungsangriffe wie ARP-Cache-Poisoning um alle Netzwerkdaten zu erhalten. Ein Angriffsszenario außerhalb des Netzwerkes bedeutet, dass der Angreifer es geschafft hat, die Datenweiterleitung vom Heimnetzwerk in das Internet über seinen Knotenpunkt zu leiten. Hierfür gibt es Netzwerkprotokollangriffe wie z.B. BGP Protocol Attacks, um Routinginformationen zu manipulieren und Datenströme umzuleiten.

Der Angreifer weiß vorab nicht, welche Geräte sich im Heimnetzwerk befinden. Er kann nur davon ausgehen, dass sich neben den IoT-Geräten noch höchstens ein Smartphone im Heimnetzwerk befindet.

Der Angreifer versucht zunächst, einen Überblick über den Datenverkehr zu erlangen und Interaktionen zwischen den Geräten abzuleiten, wobei dieser kein Interesse daran hat, die IoT-Geräte oder andere Geräte im Netzwerk zu kompromittieren. Er will ausschließlich passiv den Datenverkehr belauschen und daraus das Verhalten der Bewohner ableiten. Der einzige Eingriff in den Datenverkehr erfolgt, wenn sich für den Angreifer die Chance abzeichnet, durch beispielsweise Ausnutzen schwacher Verschlüsselung mehr Informationen über die Bewohner zu erlangen.

Bei Auffinden gravierender Schwachstellen wird der Angreifer versuchen, diese zur Störung bzw. Manipulation der IoT-Geräte zu nutzen.

Die Manipulation am Smart Home wird nicht aktiv verfolgt, jedoch betrachtet, wenn sich offensichtliche Schwachstellen bemerkbar machen sollten. Diese wären vor allem in mangelhafter oder fehlender Verschlüsselung zu suchen. Sollte dies der Fall sein, werden folgende Angriffe versucht:

- Manipulation der Abläufe im Smart Home
- Störung der Abläufe im Smart Home

Mit Störung sind hier keine Denial of Service-Angriffe im Sinne von Packet Flooding o.ä. gemeint, sondern gezielte Signale, die z.B. zur Unterbrechung der Funktionalität von Geräten führen sollen.

2.1.6 Bewertung der gefundenen Bedrohungen

Nach dem Auffinden von Bedrohungen wird nun eine Bewertung vorgenommen. Diese dient sowohl dazu, die Bedrohungen zueinander in Relation zu setzen, als auch absolut zu bewerten.

Hierfür werden die folgenden zwei Dimensionen betrachtet:

- Wie sicher ist der Rückschluss, den die Bedrohung auf das Leben der Bewohner zulässt?
- Welcher Schaden kann dadurch entstehen?

Die Sicherheit des Rückschlusses wird wie folgt bewertet:

Grad	Bedeutung
Sehr sicher	Der Angreifer kann auf Grund der Interaktion eine definitive Annahme über die Person treffen.
Sicher	Der Angreifer hat eine sehr konkrete Vermutung. Wäre die Absicht beispielsweise, sich unbefugten Zutritt zu verschaffen und die Indikation, dass niemand zu Hause ist, würde der Angreifer seinem Vorhaben nachgehen.
Unsicher	Der Angreifer erkennt zwar eine Interaktion, kann daraus alleine keine nützlichen Informationen ableiten.
Kein Rückschluss	Es ist zwar eine Interaktion erkennbar, jedoch ist die Aussagekraft so gering, dass auch weitere, gleichzeitig stattfindende Interaktionen, das Bild nicht klarer machen könnten.

Der Schaden wird wie folgt bewertet:

Grad	Bedeutung
Hoch	Die Sicherheit der Bewohner ist unmittelbar gefährdet.
Mittel	Die Information kann für die Planung eines physischen Verbrechens genutzt werden, bietet aber keine vollständige Sicherheit.
Gering	Die Information ist für den Angreifer (nahezu) irrelevant.

2.1.7 Exemplarische Ergebnisse

Die nachfolgende Abbildung 3 zeigt eine exemplarische Netzwerkdatenübertragung zwischen Smartphone und einer smarten Kamera.

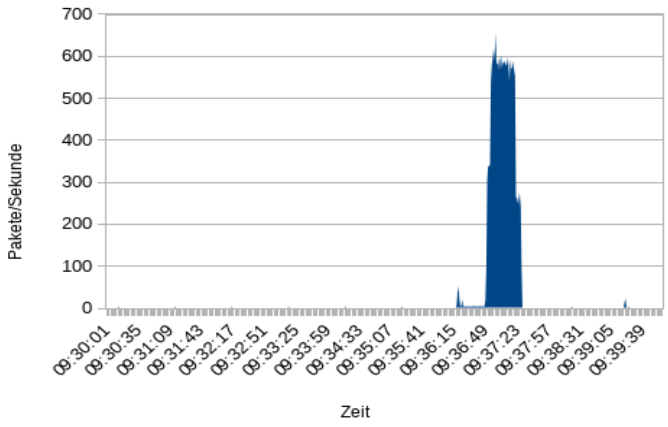


Abbildung 3: Netzwerkgraph, Smart-Kamera

Der Zugriff auf die Kamera ausgehend vom Smartphone (Live-Viewing) startet ab ca. 9:36 Uhr und dauerte in etwa eine Minute. Da die Kamera im Ruhezustand fast keinen Datenverkehr produziert, kann dieses Ereignis sehr deutlich im Graph gesehen werden. Die Datenübertragung erfolgt unverschlüsselt, sodass es einem Angreifer potenziell möglich wäre, das übermittelte Videomaterial zu rekonstruieren.

Neben dem Live-Viewing versendet die Kamera auch per FTP Fotos. Dies enthüllt einerseits die Zugangsdaten zu dem FTP-Server und erlaubt andererseits künftig Rückschlüsse darauf, wann die Kamera Bewegungen im abgedeckten Bereich wahrnimmt.

Diese Information ist enorm wertvoll, wenn die Kamera an einem zentralen Ort ist, weil durch Rekonstruktion oder bei Austreten aus der komplett passiven Rolle, durch Download, ein Bild über Aktivität im Bereich angefertigt werden kann.

Die für das Experiment gewählte Cloud-Kamera ist aus Security-Sicht besonders schwach. Es handelt sich hier jedoch nicht um eine prinzipielle Schwachstelle von Cloud-Kameras. Sie bietet keinerlei Verschlüsselung an, weder für die Live-View-Funktion am Smartphone noch zur Übertragung von Aufnahmen der Motion-Detection. Ein passiver Angreifer muss also nur darauf warten, dass die Kamera in irgendeiner Form verwendet wird, um an ihre Aufnahmen zu gelangen.

Ist der Upload via FTP aktiviert, ist es darüber hinaus möglich, sich zu dem FTP-Server zu verbinden und so die Aufnahmen der Kamera abzugreifen.

Rückschlusssicherheit	Schaden
Sehr sicher	Hoch

Aber auch die anderen betrachteten Geräte zeigen teils erschreckende Ergebnisse. Die untersuchte „smarte" Türklingel verwendet keine Verschlüsselung. Das erlaubt einem passiven Angreifer genau zu sehen, ob gerade ein „Klingel"-Ereignis oder ein „Bewegungserkennungs"-Ereignis ausgelöst wurde. Ebenso könnte dieser Umstand genutzt werden, um gefälschte Ereignisse zu produzieren und so Einwohner z.B. zur Tür zu locken.

Das Beleuchtungssystem überträgt die Daten im Allgemeinen nur verschlüsselt via Cloud. Bemerkenswert ist, dass es einen Offline-Modus gibt: Wenn das System keine Verbindung zum Internet herstellen kann und sich ein Smartphone mit App im gleichen Netzwerk befindet, verbindet sich die App direkt unverschlüsselt mit dem System und sendet die Kommandos via http.

15:23-15:27 – Smartphone – Staubsaugen

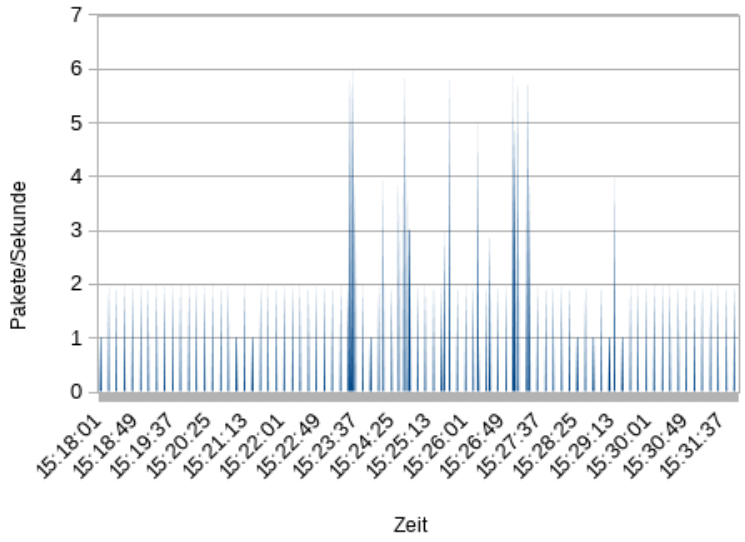


Abbildung 4: Netzwerkgraph, Smartphone

In diesem Graph wurde der Saugroboter vom Smartphone aus kontrolliert. Das Diagramm zeigt auch hier gut den Zeitraum, in dem der Saugroboter aktiv ist und wann der Reinigungsprozess beendet ist.

Rückschlusssicherheit	Schaden
Sehr sicher	Mittel

Bei der Untersuchung der DNS-Anfragen wurden jene markiert, welche mit hoher Wahrscheinlichkeit nur einem bestimmten Gerät zuzuordnen sind. Die DNS-Anfragen wurden im Rahmen der Datensammlung miterfasst. Es reicht hierbei mit einem entsprechenden Tool wie Wireshark oder programmatisch nach DNS-Anfragen, die von einem der Geräte ausgehen, zu filtern.

Hier am Beispiel des oben betrachteten Saugroboters zu sehen:

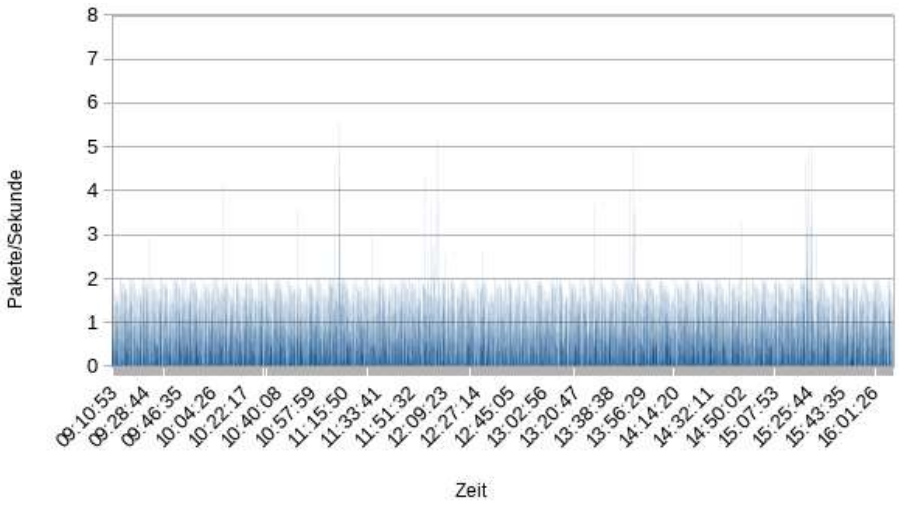


Abbildung 5: Netzwerkgraph, Staubsaugerroboter

Traffic-Muster im Ruhezustand	Der Saugroboter produziert ein konstantes Rauschen, jedoch werden nur sehr wenige Pakete pro Sekunde versendet.
Traffic-Muster bei Verwendung	Während des Staubsaugens produziert der Saugroboter konstant höheren Traffic. So ist klar zu unterscheiden, ob er gerade aktiv ist oder nicht.
DNS-Anfragen	[redacted]api.com. 1.[redacted].pool.ntp.org. 2.[redacted].pool.ntp.org. 3.[redacted].pool.ntp.org. 0.[redacted].pool.ntp.org.
Direkte Verbindung bei Kontrolle mit Smartphone/Sprachassistent?	Nein
Direkte Interaktion mit anderen Geräten im Heimnetzwerk?	Nein
Verbindungen verschlüsselt?	Ja

2.1.8 Resultate

Wenn man alle Resultate aus den Messungen von allen Smart Home-Geräten analysiert, kann gezeigt werden, dass selbst aus dem Vorhandensein und dem Zusammenspiel weniger Smart Home-Geräte bereits viele Informationen über die Bewohner des Smart Homes gewonnen werden können. Auch wenn ein Angreifer dank großteils eingesetzter Übertragungsverschlüsselung nicht mehr alle Details darüber erfahren kann, was sich gerade in dem Smart Home zuträgt, genügt der analysierte Datenverkehr doch, um eine Skizze der Abläufe im Smart Home anzufertigen, die genau genug ist, um zumindest zu beurteilen, ob jemand im Smart Home ist oder nicht.

Es muss beachtet werden, dass bei der Analyse zusätzliche Informationsquellen wie z.B. Aufrufe von Webseiten, Betrachten von Videostreams, Abspielen von Musikstreams etc. nicht mitbetrachtet worden sind. Hiermit sind möglicherweise noch detaillierte Analysen möglich.

Besonders gut konnte der Zustand des Staubsaugerroboters aus seinem Datenverkehr abgelesen werden, aber es war auch möglich, Rückschlüsse aus Sprachbefehlen zu ziehen. Je nachdem, welche weiteren Annahmen ein Angreifer über seine Opfer trifft, ist das bereits eine relativ deutliche Aussage darüber, ob das Smart Home gerade leer steht. Üblicherweise kaufen sich Menschen einen Staubsaugerroboter eher, um diesen die Arbeit machen zu lassen, während sie außer Haus sind.

Setzt ein Gerät nicht auf entsprechende Verschlüsselung (z.B. mindestens TLS 1.2), wie es beispielsweise die Überwachungskamera tat, könnte ein Angreifer das auch nutzen, um Daten zu manipulieren, z.B. um bei einem Einbruch die Spuren zu verwischen. Neben dem Verwischen von Spuren können die Informationen noch in

verschiedene andere Richtungen genutzt werden: Es kann kompromittierendes Material über die Bewohner gesammelt werden, um diese später zu erpressen oder genau ausgeforscht werden, wann sich jemand in einem bestimmten Bereich des Hauses aufhält, oder eben nicht.

Zusammenfassend sind Seitenkanalanalysen möglich, da viele Geräte dagegen kaum Sicherheitsvorkehrungen haben und ein Angreifer immer auch eine gewisse Menge an Informationen aus dem Datenverkehr gewinnen kann. Die Geräte waren im Allgemeinen gegen „normale" Angriffe gut gesichert. Nur der Umstand, dass sie eher mehr als weniger Daten übertragen, bedingt den Informationsgewinn.

3 Normen und Regelwerke

Für ein funktionierendes Internet der Dinge braucht es eine effiziente Standardisierung der eingesetzten Komponenten und Dienste. Gegenwärtig werden die existierenden Standards überprüft, inwieweit sie für Anwendungen im Internet der Dinge angepasst werden können. Während einige Standards lediglich adaptiert werden müssen, sind für andere Themen völlig neue Regelwerke für das Internet of Things zu entwickeln.

Bereits veröffentlicht wurde der dreizehnteilige Internationale Standard ISO/IEC 29341 zum Management von Geräten und deren Protokollen. In Ausarbeitung befinden sich zur Zeit Standards, die Definitionen und Vokabular des Internet of Things (ISO/IEC CD 20924) sowie den Aufbau einer entsprechenden Referenzarchitektur (ISO/IEC CD 30141) thematisieren. Zahlreiche weitere Regelwerke zu Themen wie Frameworks, Use Cases, dem Gebrauch von Object Identifiers und IoT in der Supply Chain sind darüber hinaus in Vorbereitung.

Es ist jedoch noch nicht abzusehen, mit welchen Standards wir in Zukunft den Aufbau von IoT-Infrastrukturen definieren und absichern werden.

3.1 ISO 20924: IoT-Referenzarchitektur

Die ISO/IEC 20924 ist eine in der Draft-Stage befindliche Norm, die sich der Thematik Internet of Things widmet. Diese stellt eine standardisierte IoT-Referenzarchitektur bereit, die ein gemeinsames Vokabular und bewährte Verfahren der Branche verwendet. Es hat einen Top-Down-Ansatz, beginnend mit dem Sammeln der wichtigsten IoT-Merkmale, dem Abstrahieren hin zu einem generischen IoT-Konzeptmodell, welches vom konzeptionellen Modell zu einem systembasierten Referenzmodell auf hoher Ebene führt und sich dann vom Referenzmodell zu fünf Architekturansichten gliedert (Funktionsansicht, Systemansicht, Benutzeransicht, Informationsansicht und Kommunikationsansicht). Diese Norm soll als Basis für die Entwicklung spezifischer IoT-Anwendungen dienen. Zielgruppe sind dabei Ingenieure und technische Manager, die IoT-Anwendungen entwickeln oder entwerfen werden. [8]

3.2 ISO 29341: Standard für Universal Plug and Play

Die ISO/IEC 29341 ist ein internationaler Standard für Universal Plug and Play (UPnP), der hilft verschiedenste Geräte nahtlos sowohl hersteller- als auch technologieübergreifend miteinander zu verbinden. Der Standard beschreibt die Architektur für die Vernetzung von Smart Devices, Audio- und Videogeräten, drahtlosen Geräten und PCs. Er hilft somit den Herstellern die Anforderungen zu erfüllen, damit diese Technologie funktioniert. Der Standard offeriert zudem Spezifikationen zur einfachen Bedienung der Geräte über internetbasierte Kommunikationsstandards (z.B.: TCP/IP, UDP, http, XML, …)

Der Standard besteht aus mehreren Teilen, der erste Teil, ISO/IEC 29341-1, legt die grundlegenden Prinzipien und Basisarchitektur fest. Die weiteren Teile definieren spezifische Anwendungen und Geräte.

3.3 DIN 27072: Mindestanforderungen an IoT-Geräte

Die DIN 27072 stellt eine Vornorm dar. Es handelt sich um eine Spezifikation, die generische Mindestanforderungen an vernetzungsfähige Geräte (IoT-Geräte) festlegt. Ein Basissicherheitsniveau wird adressiert, welches gegen elementare Angriffe auf grundlegende Designschwächen (wie Verwendung von Standardpasswörtern) schützen soll. Geschützt werden soll dabei nicht nur das IoT-Gerät selbst, sondern auch die bereitgestellten Informationen. Dabei liegt der Fokus auf der IT-Sicherheit und es werden keine Aspekte der funktionalen Sicherheit adressiert. Die in der Norm befindlichen Anforderungen richten sich an IoT-Geräte aus dem Consumer-Bereich und es werden Mindestanforderungen an grundlegende IT-Sicherheitseigenschaften für diese Geräte definiert.

3.4 VdTÜV-Merkblatt

Der Verband der TÜV®arbeitet gerade an einem Merkblatt, welches sich einem Conformity Assessment Program für IoT-Geräte widmet. TÜV TRUST IT arbeitet hier intensiv mit dem VdTÜV zusammen, um die entsprechenden Anforderungen und Prüfkriterien zu erstellen. Das Ziel dieses Assessment-Programmes besteht darin, die Sicherheit von Consumer-IoT-Geräten zu erhöhen, sodass diese angemessen vor externen Bedrohungen geschützt sind. Innerhalb eines Lebenszyklus so eines IoT-Gerätes können immer wieder neue Schwachstellen entdeckt und ausgenützt werden. Aus diesem Grund umfasst das IoT-Assessment eine Konformitätsbewertung des Anbieters. Diese soll zusichern, dass der Anbieter in der Lage ist das Produkt zu patchen, sodass dieses wieder in einen sicheren Zustand zurückkehrt. Zertifikate sollen sicherstellen, dass der Anbieter in der Lage ist auf Cyberangriffe zu reagieren, und sich ständig darum bemüht, die Sicherheit des IoT-Produkts über eine Mindestlebensdauer zu gewährleisten.

3.5 TÜV AUSTRIA TRUSTED-IoT-Device-Zertifizierung

Da es aktuell noch kein anerkanntes und allgemeines Verfahren zur Zertifizierung und IT-Sicherheitsüberprüfung von IoT-Geräten gibt, hat TÜV TRUST IT eine eigene TRUSTED-IoT-Device-Zertifizierung erstellt. In dieser Zertifizierung wird das IoT-Gerät, die entsprechende Cloud, die entsprechende App und zughörige Prozesse von den Experten der TÜV TRUST IT im Hinblick auf IT-Sicherheit überprüft und analysiert. Außerdem werden umfassende Sicherheitstests (Penetrationstests) auf das IoT-Gerät und z.T. auch die Backend-Strukturen durchgeführt. Bei einer erfolgreichen Prüfung wird für das Gerät eine Zertifizierung ausgesprochen. Der Hersteller kann dann das TÜV Zertifikat nutzen, um seine Kunden über die IT-Sicherheit seines Produktes zu informieren.

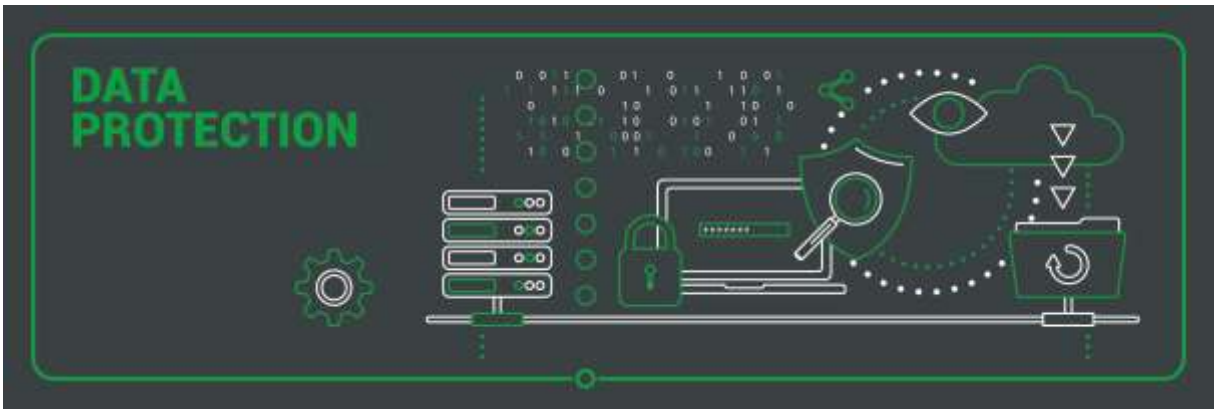
4 Lösungsvorschläge

Aus Kapitel 3 wird ersichtlich, dass seitens Normung/Regelwerken im Bezug IoT-Cybersecurity wenig bzw. kaum Verbindliches zur Verfügung steht. Für den Nutzer braucht es somit konkrete Anweisungen. Der TÜV AUSTRIA hat eine Vielzahl an Hilfestellungen für den Anwender aus Forschungsergebnissen abgeleitet, die Aufschluss darüber geben sollen wie IoT-Geräte zu handhaben sind, um einerseits die Sicherheit zu gewährleisten und sich andererseits gegen Manipulationen von außen zu schützen. Durch Seitenkanäle im Smart Home können eindeutige Rückschlüsse über das Verhalten der Bewohner gezogen werden. Der Schutz der Privatsphäre, sowie der übertragenen Informationen ist ebenso ein wichtiges Thema für Schutzmaßnahmen.

Es genügt ein relativ kurzer Beobachtungszeitraum des Haushaltes, um viele Datenpunkte über die Abläufe im Smart Home zu sammeln. Es zeigt auch, dass mehr Geräte das Informationsnetz immer weiter verdichten werden. Während die Informationen, welche ein Gerät alleine generiert, relativ wenig Gewicht haben, erlaubt die Korrelation der verschiedenen Informationen ein immer klareres Bild der Vorgänge im Smart Home.

Das Problematische an dieser Entwicklung ist, dass die Bewohner des Smart Homes dagegen wenig tun können. Offensichtlich fehlt es hier auch einigen Geräteherstellern an Erfahrung im Umgang mit potenziellen Bedrohungen und IT-Sicherheitslücken oder sie legen aus anderen Gründen, wie z.B. Kostenfaktoren, keinen Wert darauf, die Sicherheit ihrer Produkte vor digitalen Angriffen sicherzustellen. Es ist besonders wichtig, sich vor dem Kauf über Sicherheitsmerkmale der einzelnen Geräte zu informieren, am besten durch unabhängige Quellen und Reviews. Ohne tiefergehendes technisches Verständnis ist es nicht möglich, ein sicheres Gerät von einem unsicheren Gerät zu unterscheiden.

4.1 Schutzmaßnahmen für Endanwender



Endanwender haben verschiedene Möglichkeiten, den Informationsgewinn eines Angreifers im Heimnetzwerk einzudämmen.

Zunächst sollte sich jeder Anwender die Frage stellen, ob er ein bestimmtes Gerät wirklich in einer IoT-Variante braucht. Falls ja, lohnt es sich zu überlegen, ob ein Gerät, welches nur lokale Verbindungen über Bluetooth akzeptiert, genügt.

Anschließend empfiehlt es sich, möglichst viele Informationen über gewünschte Geräte bzw. Gerätetypen zu sammeln. Die smarte Überwachungskamera ist beispielsweise ein eher älteres und billiges Gerät. Es ist sehr wahrscheinlich, dass sich neuere Produkte mit höheren Sicherheitsniveaus finden lassen. Dabei muss teurer nicht sicherer bedeuten.

Die effektivste Maßnahme ist, dass die IoT-Geräte in einem eigenen, vom Rest des Heimnetzwerkes abgetrennten, Netzwerk betrieben werden sollen, das möglichst ohne Internetzugriff aufgesetzt ist. Das Smartphone soll dann gezielt zur Steuerung der IoT-Geräte in dieses Netzwerk eingebunden werden. Das garantiert, dass nur Personen mit Zugriff auf das Netzwerk Informationen über die Geräte erlangen können. Dieses Szenario ist für die meisten Leute jedoch praxisfern, da Geräte wie z.B. der getestete Sprachassistent unbedingt eine Internetverbindung benötigen.

Alle genannten Schutzmaßnahmen sind als Verbesserung der Lage, nicht als vollständige Lösung zu verstehen. Der einzige Weg, die Angriffsfläche möglichst gering zu halten, ist sich genau vor dem Kauf zu informieren und zu überlegen, was man wirklich als IoT-Gerät benötigt.

Der DNS als „geschwätziger Seitenkanal“ wird wohl in einigen Jahren durch die Entwicklung verschlüsselter DNS-Protokolle passé sein. Bis dahin ist es in einem Heimanwender-Szenario unmöglich, diese Lücke zu schließen.

4.2 Tipps für Endanwender

Anhand der vorangegangenen Kapitel wurden zusammenfassend folgende zehn einfach anwendbare Maßnahmen formuliert, die jeder vor dem Kauf bzw. der Inbetriebnahme von IoT-Consumer-Geräten durchführen kann.

1. **Benötige ich die Geräte wirklich als IoT?**
   Im Vorfeld sollte jeder für sich abwägen, ob es Sinn macht das Consumer-Gerät auch tatsächlich mit Smart-Funktionalität zu erwerben, oder ob nicht ein konventionelles Gerät völlig ausreichend ist.
2. **Muss ich das Gerät wirklich an das Smartphone oder das Netzwerk koppeln?**
   Für den Fall, dass das gewünschte Consumer-Gerät nicht ohne IoT-Funktionalität zu erwerben ist (z.B. moderne Smart TVs), so muss dieses nicht zwangsweise oder permanent mit dem Netzwerk verbunden sein.
3. **Gastnetzwerk**
   Es macht Sinn für das IoT-Gerät lediglich ein Gastnetzwerk einzurichten. Angemeldete Geräte nutzen in diesem Fall nur den Internetzugang und haben keinen Zugang zum Heimnetzwerk. Das hat den Vorteil, dass die Nutzung protokolliert und auf bestimmte Internetanwendungen beschränkt werden kann.
4. **Datensparsamkeit – Haken entfernen**
   Bei der Inbetriebnahme des IoT-Gerätes sollte ein Minimum an Dateneingaben erfolgen. Bei den Grundeinstellungen sollten so wenig wie möglich Häkchen gesetzt werden. So wird unnötige Informationsweitergabe vermieden.
5. **Bekannte Hersteller – wo ist die Cloud?**
   Innerhalb der EU unterliegt der Datenverkehr dem Datenschutz (DSGVO). Außerhalb der EU kann dies nicht garantiert werden, da jeweils nationales Recht beziehungsweise Datenschutz greift. Es sollte also darauf geachtet werden, dass die Daten im europäischen Raum gespeichert werden.
6. **Hersteller nach IT-Sicherheit anfragen**
   Sollten Bedenken bezüglich Sicherheit des Consumer-Gerätes vorliegen, kann ein Anruf beim Hersteller nützlich sein um Unklarheiten zu beseitigen.

7. **Achten auf Bewertungen**
   Im Vorfeld des Kaufes ist es ratsam sich Kundenbewertungen durchzulesen. Oft bekommt man damit bereits sehr viel Informationen zu potenziellen Sicherheitslücken.
8. **Regelmäßige Updates**
   IoT-Geräte sollten immer auf dem aktuellsten Stand gehalten, Updates regelmäßig durchgeführt werden.
9. **Zufällige lange Passwörter wählen**
   Je länger und je zufälliger zusammengesetzt ein Passwort ist, desto sicherer ist dieses. Wählen Sie ein langes Passwort, welches keine Bedeutung (z.B. Namen) enthält und welches Sie nur ein einziges Mal verwenden.
10. **Bei wichtigen Funktionen nicht alleine auf ein smartes Gerät vertrauen.**
    Werden bestimmte wichtige Funktionalitäten von einem smarten Gerät übernommen, sollte man zusätzlich die Funktionalität durch eine physikalische Funktion unterstützen. Ein klassisches Beispiel ist ein Smart-Lock, welches man zusätzlich mit einem herkömmlichen Schlüssel absichert.

4.3 Schutzmaßnahmen für Hersteller

Um für die eigenen Geräte ein besseres Schutzniveau zu erlangen, hilft es Herstellerunternehmen und Produktentwicklern insbesondere, sich mit den generellen Gefährdungen und Angriffsvektoren vertraut zu machen. Hierfür kann der Hersteller beispielsweise das Open Web Application Security Project (OWASP), welches jährlich eine Aufstellung der wichtigsten Bedrohungen und Schwachstellen für IoT auflistet, heranziehen und entsprechende Gegenmaßnahmen implementieren [9].

Auf dieser Basis und auf Grundlage der eigenen TÜV AUSTRIA-Prüfkriterien für „TRUSTED-IoT-Devices“ sind nachfolgend einige wirksame Maßnahmen und Verfahren, die Hersteller implementieren können, um ihre Produkte besser vor Angriffen zu schützen, aufgelistet.

1. **Architekturbeschreibung**
   Es sollte eine Beschreibung der (Netzwerk-)Architektur des IoT-Gerätes vorliegen. Darunter fallen beispielsweise verwendete Hardwarekomponenten, betriebene Dienste, Kommunikationsschnittstellen (z.B. App, Cloud). Die Absicherung der Schnittstellen vor unbefugtem Zugriff und Manipulation sollte beschrieben werden.

2. **Benutzer- und Berechtigungsmanagement**
   Ein Rollenkonzept sollte vorhanden sein. Dabei sind sowohl die Systembenutzer auf dem Gerät als auch Anwender zu beschreiben. Bei der Vergabe von Berechtigungen sollte das Least-Privilege-Prinzip (Prinzip, nach dem den Nutzern nur die Rechte zugewiesen werden, die sie benötigen) Anwendung finden.

3. **Systemhärtung**
   Es werden ausreichende Maßnahmen, die zur Härtung des Systems und Reduzierung der Angriffsfläche beitragen, definiert und umgesetzt. Hierbei können beispielsweise Technische Analysten (Pentester) von IT-Sicherheitsunternehmen sinnvolle Beiträge zur Unterstützung leisten.

4. **Kryptographie**
   Es sollten kryptographische Verfahren sowohl zur lokalen Datenhaltung als auch zur Sicherung der Daten auf dem Transportweg implementiert werden. Insbesondere ist darauf zu achten, dass nur kryptographische Verfahren verwendet werden, die nach dem aktuellen Stand der Technik als sicher gelten. Der Umgang mit kryptographischem Schlüsselmaterial und Zertifikaten (Schlüssel- und Zertifikats-Management) muss sicher gestaltet werden.

5. **Patch-Management**
   Es muss ein Prozess etabliert und beschrieben werden, der das Patch-Management aller Komponenten abbildet. Insbesondere ist ein Prozess zu etablieren, der auf die Veröffentlichung von Schwachstellen reagiert und entsprechend der Kritikalität einer Schwachstelle in einem angemessenen Zeitraum Sicherheitsupdates zur Verfügung stellt. Die technische Absicherung des Patch-Prozesses ist zu beachten.

6. **OTA-Updates**
   Hersteller sollten festlegen, wie sie sichere Over-the-Air-Updates für Geräte im Feld gewährleisten können. Dabei ist zu definieren, wie die Updates kryptographisch gesichert werden und wie sichergestellt wird, dass alle Geräte im Feld das Update erhalten.

7. **Entwicklungsprozess**
   Der Entwicklungsprozess zu der in den Geräten verwendeten Software berücksichtigt insbesondere die Aspekte der sicheren Software-Entwicklung (z.B. Threat Modeling, Secure-Software-Development-Lifecycle, Zugriff auf den Quellcode).

8. **Ausgelagerte Software-Entwicklung**
   Ausgelagerte Software-Entwicklung muss denselben definierten Regularien unterliegen wie die interne Entwicklung. Schriftliche Vereinbarungen sollten Sicherheitsanforderungen an Externe definieren.

9. **Technisches Datenschutzkonzept (Logging, Privacy-by-Design)**
   Es sollte eine Dokumentation der von den IoT-Geräten erhobenen, gespeicherten und übermittelten Daten vorliegen. Es muss spezifiziert werden, welche Daten protokolliert werden, wie lange die Daten aufbewahrt und wie sie geschützt werden. Sensible Daten (z.B. Zugangsdaten) dürfen nicht in Log-Nachrichten(-Dateien) geschrieben werden. Es muss eine Begründung zur Erhebung von Daten erfolgen, deren Erhebung nicht aus dem Anwendungskontext des Prüfgegenstands heraus eindeutig ersichtlich ist (Datensparsamkeitsprinzip).

10. **Installations- und Auslieferungszustand**
    Anweisungen zur Inbetriebnahme im Auslieferungszustand müssen einfach und verständlich sein. Hervorzuheben sind dabei Merkmale, die über eine Produktserie identisch sind (z.B. Standard-Passwörter, Pairing-Prozess, Integration in das Netzwerk). Endanwender sollten darauf hingewiesen werden, dass und wie Standard-Passwörter zu ändern sind. Es ist eine angemessene Passwort-Stärke abzuverlangen.

5 Zusammenfassung und Ausblick

Während es auf Basis passiv gesammelter Informationen immer schwer bleibt, eine exakte Antwort über den Zustand des Smart Homes zu geben, hat sich in der Aufzeichnung gezeigt, dass sich viele Ereignisse im Smart Home sehr genau beobachten lassen. Dies hängt am stärksten davon ab, wie „gesprächig" ein Gerät ist.

Die Rolle des Sprachassistenten ist hier speziell interessant. Die Verwendung des Assistenten alleine lässt absolut keine Rückschlüsse darüber zu, wie gerade mit dem Sprachassistenten interagiert wird. Die Frage „wie ist das Wetter heute?" könnte genauso ein Eintrag in eine Online-Notizliste sein. Wird dieser jedoch zusammen mit einem IoT-Gerät verwendet, ist die Korrelation zwischen dem Datenverkehr des Assistenten und dem gesteuerten IoT-Gerät sehr hoch. Üblicherweise vergehen nur Sekunden zwischen einem Datenstrom ausgehend vom Assistenten und z.B. der Reaktion des Beleuchtungssystems.

Generell können die IoT-Geräte gut voneinander unterschieden werden. Selbst ohne davor Vergleichsmaterial gesammelt zu haben, ist es einem Angreifer möglich, auf Grund des Datentransfermusters und der kontaktierten Adressen im Internet (siehe Spezifika der Geräte) zu erraten, was gerade passiert.

Besonders gesprächig zeigt sich der Saugroboter. Der Staubsaugerroboter ist üblicherweise ziemlich „still" im Netzwerk, führt er jedoch einen Reinigungsauftrag durch, sendet er währenddessen konstant Daten in die Cloud. Es kann hier nicht bestimmt werden, was der Roboter mitteilt, da die Daten verschlüsselt übertragen werden, jedoch kann ein Angreifer auf die Minute sagen, wann im Smart Home staubgesaugt wird.

Interaktion mit dem Beleuchtungssystem kann ebenso gut nachverfolgt werden. Allerdings ist auf Grund des verschlüsselten Datenverkehrs nicht zu erkennen, ob Lampen gerade ein- bzw. ausgeschaltet werden oder z.B. die Farbstimmung verändert wird.

Den stärksten Ausschlag zwischen Ruhezustand und Aktivität zeigt die Videotürklingel. Da sie batteriebetrieben ist, wurde sie dahingehend optimiert, möglichst wenig Kommunikation mit dem Netzwerk zu benötigen. Wird geklingelt, oder, falls aktiv, die Bewegungserkennung ausgelöst, produziert das einen deutlichen Ausschlag. Auf diese Art kann klar festgestellt werden, wann sich etwas am Eingang zuträgt.

Eine besondere Rolle nimmt auch die Überwachungskamera ein. Das Gerät nutzt keine Übertragungsverschlüsselung, weder lokal noch für die Live-View-Funktion, welche einen Live-Stream an das Smartphone überträgt. Gelingt es dem Angreifer den Datenverkehr dieses Geräts mitzuschneiden, kann er alles sehen, was die Kamera sieht. Darüber hinaus bietet die Kamera die Möglichkeit, Fotos bei Bewegungserkennung auf einen FTP-Server zu laden, oder per E-Mail zu versenden. Ist diese Option aktiviert, ist es auch als passiver Angreifer ein Leichtes, an die übermittelten Daten zu kommen. Somit kann ein Bereich, der von dieser Kamera überwacht wird, generell als „unsicher" eingestuft werden.

An diesen Beispielen zeigt sich ganz deutlich, dass Hersteller zukünftig mehr noch als bisher dazu aufgefordert werden müssen, bestehende Best-Practices und bewährte Sicherungsmaßnahmen im Rahmen eines Security-by-Design-Ansatzes zu berücksichtigen und in ihren Produkten zu implementieren.

6 Über TÜV AUSTRIA, Know Center und TU Graz

TÜV AUSTRIA Group

TÜV AUSTRIA ist ein internationales Unternehmen mit Niederlassungen in mehr als 20 Ländern und beschäftigt mehr als 1.700 Mitarbeiterinnen und Mitarbeiter.

Das Dienstleistungsportfolio des unabhängigen österreichischen TÜV umfasst die Bereiche Testing, Monitoring, Zertifizierung, Training und Consulting.

Von den Standorten Köln und Wien aus ist TÜV AUSTRIA Group-Member TÜV TRUST IT der neutrale, objektive und unabhängige Partner für Beratungs- und Zertifizierungsleistungen rund um die Themen Informationssicherheit und Datenschutz. Ziel ist es, Unternehmen dabei zu unterstützen, Informationswerte zu schützen, die für den ordnungsgemäßen Geschäftsbetrieb notwendig sind und über Infrastrukturen und -prozesse zur Verfügung gestellt werden. Die Leistungen von TÜV TRUST IT basieren auf anerkannten Standards und bewährten Methoden.

Ansprechpartner zum Thema IoT im Smart Home:

DI Hendrik Dettmer – hendrik.dettmer@tuv-austria.com

TU GRAZ

Die TU Graz ist eine weltweit führende Forschungsinstitution im Bereich der Informationssicherheit. Das Institut für angewandte Informationsverarbeitung und Kommunikationstechnologie der TU Graz beschäftigt mehr als 60 Forscher in diesem Bereich. Die Forscher arbeiten in formalen Methoden, Secure-Crypto-Implementierungen, Secure-E-Government und vertrauenswürdigen Systemen. Zu den Highlights zählen Kryptographie, E-Identity, Trusted Computing, RFID-Sicherheit, sichere Hardwareimplementierungen kryptografischer Algorithmen, Seitenkanalanalyse, Netzwerksicherheit und formale Methoden für Design und Verifizierung. Das Institut ist Teil der Fakultät für Informatik an der Technischen Universität Graz.

Ansprechpartner zum Thema IoT im Smart Home:

Dipl.-Ing. Peter Aufner – peter.aufner@iaik.tugraz.at

Know Center

Das Know Center Graz wurde im Jahr 2000 im Rahmen des COMET K1-Programms gegründet und entwickelte sich zum führenden Forschungszentrum für datengetriebene, innovative Informations- und Kommunikationstechnologien in Österreich. Das Know Center betreibt als assoziierte Forschungseinrichtung und Exzellenzzentrum innerhalb des COMET-Programms Grundlagenforschung und ist an zahlreichen EU-Projekten beteiligt. Das Know Center ist somit immer auf dem neuesten Stand und kann Trends in Wissenschaft und Forschung aktiv mitgestalten.

Ansprechpartner zum Thema IoT im Smart Home:

DI Dr. techn. Robert Ginthör – rginthoer@know-center.at

7 Literaturverzeichnis

Quellen

[1] J. C. Ross, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, 2017.

[2] D. Sokolov, "heise online," 2019. [Online]. Available: https://www.heise.de/newsticker/meldung/Xiaomi-Scooter-laessst-sich-ueber-Bluetooth-kapern-4307588.html. [Accessed 22 Februar 2019].

[3] O. v. Westerhagen, "heise online," [Online]. Available: https://www.heise.de/security/meldung/Kuehlsysteme-mit-schwachem-Standardpasswort-uebers-Internet-manipulierbar-4304161.html. [Accessed 22 Februar 2019].

[4] F. A. Scherschel, "heise online," [Online]. Available: https://www.heise.de/newsticker/meldung/ENOX-Safe-KID-One-Hersteller-sieht-kein-Problem-mit-Spionage-Uhr-4305734.html. [Accessed 22 Februar 2019].

[5] T. Wittenhorst, "heise online," [Online]. Available: https://www.heise.de/newsticker/meldung/Mehr-Hacker-Angriffe-auf-kritische-Infrastruktur-beim-BSI-gemeldet-4311172.html. [Accessed 22 Februar 2019].

[6] J. U. E. R. W. A. Dabrowski, "Grid Shock: Coordinated Load-Changing Attacks on Power Grids," 2017. [Online]. Available: https://www.sba-research.org/wp-content/uploads/publications/201712%20-%20ADabrowski%20-%20Grid%20Shock.pdf. [Accessed 22.02.2019].

[7] K. Lemke and C. Paar, "Ruhr Universität Bochum," [Online]. Available: https://www.emsec.ruhr-uni-bochum.de/media/crypto/veroeffentlichungen/2011/01/29/dach2006_v10.pdf. [Accessed 03 2019].

[8] ISO/IEC, *ISO/IEC CD 30141:20160910(E): Information technology – Internet of Things Reference,* Schweiz, 2019.

[9] "OWASP," [Online]. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.

Abbildungen

Shutterstock (cover photo, P. 2, 4, 8, 11, 13, 16, 22, 24, 25, 26), TÜV AUSTRIA HOLDING AG (Fig. 1, 2, 3, 4, 5)

WhitePaper

TÜV AUSTRIA Group

DI Hendrik Dettmer
TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
Mail: *hendrik.dettmer@tuv-austria.com*

www.tuv.at

TU GRAZ

DI Peter Aufner
Rechbauerstraße 12
8010 Graz
Mail: *peter.aufner@iaik.tugraz.at*

www.iaik.tugraz.at