Hochschule Rhein-Waal
Fakultät: Kommunikation und Umwelt
Studiengang: Verwaltungsinformatik
Modul: Workshop 2: Wissenschaftliches Schreiben

Aufgabe 4
Hausarbeit

Linus Wolf - 28611

11. Mai 2025

Inhaltsverzeichnis

Abbildungsverzeichnis iii

Abkürzungsverzeichnis iv

1 Einleitung 1

2 Netzwerkverbindungen von Internet of Things (IoT)-Geräten 2

2.1 Mash-Netzwerk 2

2.2 Zigbee 3

3 Angriffsszenarien 4

3.1 Ausnutzung von Fehlern in der Sicherheit von IoT-Geräten 4

3.2 Spoofing 4

3.3 Seitenkanalattacke 5

4 Gründe für Angriffe auf IoT-Geräte 6

4.1 Botnetze 6

4.2 Einfallstore in Netzwerke 6

4.3 Ausspähen von menschlicher Anwesenheit 7

4.4 Spurenloser Einbruch 8

5 Fazit 9

Literaturverzeichnis 10

Abbildungsverzeichnis

1 Prognose zur weltweite Anzahl von IoT-Verbindungen 1

2 Architektur eines Mesh-Netzwerkes 3

3 Heatmap von Joggern in geheimer US Basis 7

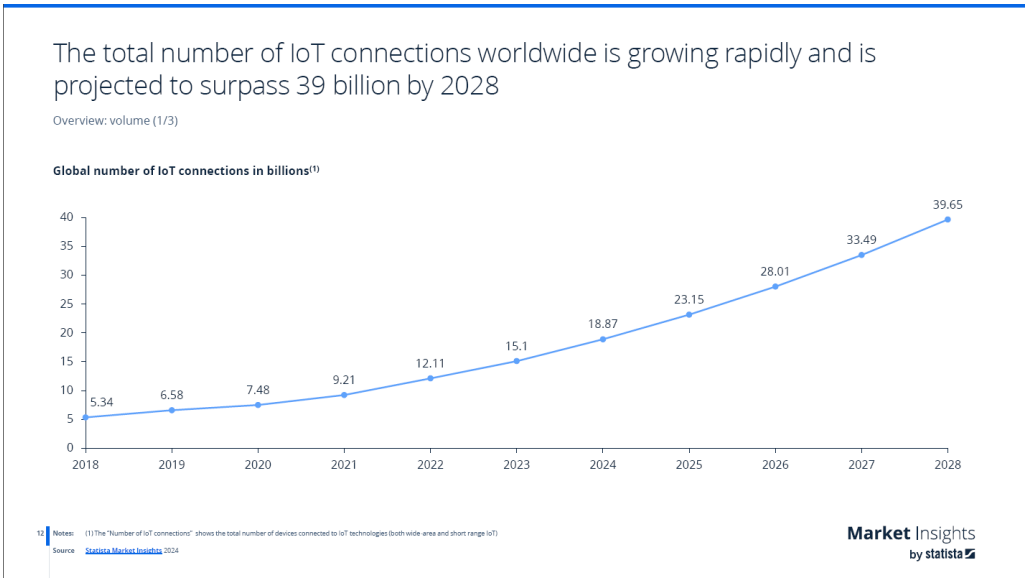
Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
IEEE	Institute of Electrical and Electronics Engineers.
IoT	Internet of Things
LAN	Local Area Network
MAC	Medium Access Control
MBSS	Mesh Basic Service Set
PAN	Personal Area Network
RFID	Radio Frequency Identification
RZF NRW	Rechenzentrum der Finanzverwaltung des Landes NRW

1 Einleitung

Laut Statista gab es 2025 weltweit 23,15 Millarden Verbindungen von Geräten im IoT. Für 2028 werden 39,65 Millarden Verbindungen prognostiziert. Es besteht die Möglichkeit, dass sich Behörden mit dem Thema IoT im Allgemeinen und Smart Home Geräte im Besonderen auseinander setzen müssen. In dieser Arbeit geht es um die technischen Grundlagen, Angriffsmethoden und Gefahren zur Forschungsfrage: Gibt es in den Liegenschaften des Rechenzentrum der Finanzverwaltung des Landes NRW (RZF NRW) IoT-Signale und wie soll zukünftig auf Gefahren im Zusammenhang mit dem IoT hingewiesen werden?

Abbildung 1: Prognose zur weltweite Anzahl von IoT-Verbindungen



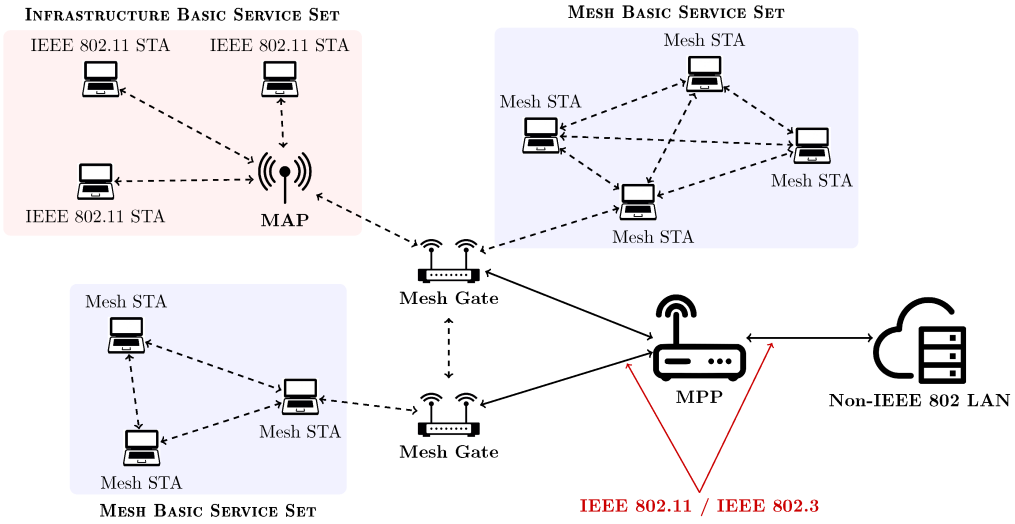
2 Netzwerkverbindungen von IoT-Geräten

Zwei der am meistgenutzten Verbindungen zwischen IoT-Geräten sind Mesh-Netzwerke und Zigbee, die hier kurz beschrieben werden solle.

2.1 Mash-Netzwerk

Der Institute of Electrical and Electronics Engineers. (IEEE) 802.11-Standard, welcher für „Standard für Informationstechnologie - Telekommunikation und Informationsaustausch zwischen Systemen - Lokale und Metropolen-Netzwerke - Spezifische Anforderungen Teil 11: Wireless LAN Medium Access Control (MAC) und Physical Layer Spezifikationen“ steht, hat für die Verwendung von Mesh-Netzwerken eine eigene Bezeichnung: IEEE 802.11s. Hierbei kommt es zu den oben genannten Titel der Zusatz „Änderung 10: Mesh-Netzwerk“. Beim IEEE 802.11s wird ein neues Routing-Verfahren eingesetzt, welches auf der MAC-Schicht anstatt auf der Netzwerkschicht, wie beim ‚traditionellen‘ IEEE 802.11, durchgeführt wird. Dabei behält der IEEE 802.11s-Standard die physischen Schichten wie bei dem „traditionellen“ Standard. Um ein effizientes Routing zu haben, müssen die Knoten genaue Kenntnisse über die drahtlosen Verbindungen haben, die sie mit ihren direkten Nachbarn verbinden. Dies führt zu nahtlosem Routing für Protokolle höherer Schichten. In einem IEEE 802.11s-Mesh-Netzwerk, auch als Mesh Basic Service Set (MBSS) bezeichnet, gibt es verschiedene logische Komponenten, wie in Abbildung 2 dargestellt. Die wichtigsten sind die Mesh-Stationen, die an der Bildung des MBSS teilnehmen und in dem jeder Knoten die gleiche Komplexität hat und keine hierarchische Struktur vorliegt. Die Mesh Stationen nehmen außerdem an der Pfadauswahl und -weiterleitung teil, wodurch ein sehr einfaches selbstorganisiertes Netzwerk entsteht.

Abbildung 2: Architektur eines Mesh-Netzwerkes



Im Falle der Integration mit anderen Netzwerktypen, wie dem ‚traditionellen' IEEE 802.11 oder wenn der MBSS auf externe Netzwerke zugreifen muss, sind andere logische Komponenten erforderlich. Die Geräte, welche den Zugang zum Mesh-Netzwerk für ‚traditionelle' IEEE 802.11-Stationen gewährleisten, werden als Mesh APs bezeichnet. Darüber hinaus werden zur Kommunikation zwischen dem Mesh Netzwerk und einem nicht-IEEE 802.11 Local Area Network (LAN), wie beispielsweise einem kabelgebundenen LAN, weitere logische Komponenten verwendet, nämlich die Mesh Portal Points, die die Kommunikation mit externen Entitäten ermöglichen (Cilfone 2019, S. 4–6).

2.2 Zigbee

ZigBee ist ein drahtloses Netzwerkprotokoll, das für niedrige Datenraten und niedrigen Stromverbrauch optimiert ist und hauptsächlich für die Automatisierung von Hausgeräten und anderen Geräten im IoT verwendet wird. Es wurde von der ZigBee Alliance entwickelt und basiert auf dem IEEE 802.15.4-Standard für Personal Area Network (PAN). Eines der wichtigsten Merkmale von ZigBee ist seine Fähigkeit, eine große Anzahl von Geräten mit geringem Stromverbrauch zu verbinden. Es ist auch sehr skalierbar und kann Netzwerke mit Hunderten von Geräten unterstützen. Die Sicherheit ist in ZigBee gut implementiert und es bietet auch eine hohe Zuverlässigkeit und geringe Latenzzeiten. ZigBee wird hauptsächlich in Anwendungen verwendet, in denen niedrige Datenraten und geringer Stromverbrauch erforderlich sind, wie beispielsweise in der Steuerung von Beleuchtung, Heizung und Klimatisierung, in Sicherheitssystemen und in der Überwachung von Umweltbedingungen. Es wird auch in vielen anderen Anwendungen im Bereich des Internet der Dinge verwendet, wie beispielsweise in der Industrieautomatisierung und in Gesundheitsüberwachungssystemen (Gessler und Krause 2015, S. 195).

3 Angriffsszenarien

3.1 Ausnutzung von Fehlern in der Sicherheit von IoT-Geräten

Kein System ist von Grund auf perfekt. Mit der Zeit werden Systeme entsprechend geupdated und Sicherheitslücken werden geschlossen. Smart Home Geräte wie Kühlschränke, Glühbirnen oder ähnliches werden jedoch häufig von sicherheitsunkundigen Personen genutzt, nach dem Kauf an Strom und Internet angeschlossen und danach nicht weiter beachtet. Dadurch bleiben Sicherheitslücken bestehen, die sich schon bei der Produktion in den Geräten befunden haben. Solche Sicherheitslücken können dann von Hackern ausgenutzt werden. In den gleichen Bereich fallen auch standardmäßig gesetzte Passwörter, die in Handbüchern stehen, bei allen Geräten gleich sind und nicht geändert werden. Die Ransomwares WannaCry und NotPetya verursachten im Jahre 2017 Milliarden an Schäden, indem sie eine Schwachstelle in der Implementierung des Server Message Block Protokols von Microsoft ausnutzten (Chantzis 2021, S. 5). Zum Zeitpunkt des Angriffs war der Fehler bereits bekannt und es stand seit 2 Monaten ein Hotfix von Microsoft zur Verfügung.

3.2 Spoofing

Beim Spoofing agieren Angreifer, als wären sie Teil des Netzwerkes oder als wären sie jemand anderes. Dies ermöglicht dem Angreifer sich zwischen zwei kommunizierende Geräte zu platzieren, die Übertragungen beider Seiten abzufangen und diese durch seine eigenen Übertragungen zu ersetzen. Diese Form wird Man-In-The-Middle-Angriff genannt. Alternativ kann der Angreifer sehr viele Anfragen an einen Netzwerkteilnehmer schicken, wobei er die Daten des anfragenden Geräts fälscht. Die Antworten werden dann an diese gefälschte Adresse geschickt, mit dem Ziel diese Adresse mit den Antworten zu überlasten. Hier spricht man von einer Denial-of-Service-Attacke, oder wenn mehrere Geräte genutzt werden, um ein Ziel zu mit Antworten zu überfrachten, von einer Distributed-Denial-of-Service-Attacke.

3.3 Seitenkanalattacke

Nach Abrishami handelt es sich bei Seitenkanalattacken um nicht invasive Angriffe, da die Geräte dabei nicht zerstört oder verändert werden. Durch Beobachtung, Messungen, Abfangen von Funkdaten mit oder ohne Senden von Daten an das Gerät lassen sich Rückschlüsse auf interne Komponenten oder Berechnung durchführen. Unterschieden werden dabei sieben verschiedene Möglichkeiten der Seitenkanalattacke (Abrishamchi, Mohammad Ali Nassiri et al. 2017).

Eine davon ist die Netzwerkverkehranalyse. Dabei werden die Pakete, die in einem Netzwerk von Geräten verschickt und empfangen werden, analysiert. Sender- und Empfänger-MAC-Adresse sind in jedem Paket nach IEEE 802.3 Standard im Klartext vorhanden und auslesbar. Dadurch lässt sich ermitteln welche Geräte untereinander kommunizieren. Durch die Größe der Pakete, Anzahl oder Zeitpunkte lassen sich weitere Details ermitteln.

Zum Beispiel sendet ein Gerät, das auf Sprachbefehle wartet, regelmäßig Daten an einen Server, um die aufgenommenen Geräusche zu analysieren. Bei erhöhter Kommunikation des Geräts und Antworten des Servers liegt daher der Verdacht nah, dass gesprochen wird und sich mindestens eine Person im Raum befindet. Khan et. al. waren 2009 bei verschlüsselter Kommunikation in der Lage aus 10 Personen mit 70-75% Wahrscheinlichkeit die sprechende Person zu identifizieren (Khan, L. A. et al. 2010, S. 70).

4 Gründe für Angriffe auf IoT-Geräte

Gründe für das Angreifen von Teilen des IoT sind unterschiedlich und abhängig ob die Ziele bewusst ausgewählt werden, z.B. im Rahmen von Firmenspiongage, oder es sich um zufällige Ziele handelt, um ein Botnetzwerk aufzubauen.

4.1 Botnetze

Kleinere Gegenstände aus dem IoT haben bauartbedingt nicht die gleiche Rechenkapazität wie ein Desktop-PC oder ein Laptop/Tablet. Dies wäre auch völlig überdimensioniert. Da die Programme auf solchen Geräten gleichzeitig recht einfach sind und wenig Leistung erfordern ist jedoch freie Rechenkapazität vorhanden. Durch das Einbinden von solchen Kleinstrechnern in das Botnet kann über die reine Anzahl solcher Geräte ein profitables Botnetz entstehen. Im Bericht des Bundesamt für Sicherheit in der Informationstechnik (BSI) aus dem Jahre 2015 steht, dass im Durchschnitt pro Tag 60.000 neue Systeme pro Tag allein in Deutschland infiziert werden. Nicht alle werden in Botnetze eingebunden oder bleiben übernommen, aber es besteht Potential (Bundesamt für Sicherheit in der Informationstechnik 2015, S. 30). Mit der steigenden Anzahl an IoT-Geräten seit 2015 ist auch damit zu rechnen, dass sich diese Zahl vergrößert hat. Laut Putman haben Botnetze die Möglichkeit sechsstellige Summen oder noch höhere Beträge zu erwirtschaften (Putman 2018).

4.2 Einfallstore in Netzwerke

Beim Angriff auf Systeme gehen Hacker meist sehr gezielt und methodisch vor. Entsprechend greifen sie nicht zuerst die am stärksten gesicherten Teile eines Netzwerkes am, um in ein System einzudringen. Sondern sie versuchen sich zuerst an den weniger gesicherten Geräten, um Zugriff zu erlangen. Sobald ein Hacker Zugang zu einem schwächer gesicherten Gerät oder einer schwächer gesicherten Komponente erhalten hat, kann er sich von dort aus weiter ausbreiten und das System schrittweise infiltrieren. Entweder indem Informationen abgegriffen werden können, die die Attacke auf eine andere Komponente erlauben. Eine andere Möglichkeit besteht darin, das schwächere Gerät oder die schwächere Komponente als Basis zu verwenden, um die

eigene Identität zu verschleiern und sich als eine andere Person oder ein anderes Gerät auszugeben. Hierbei kann der Hacker andere Teile des Systems manipulieren oder steuern, ohne erkannt zu werden.

4.3 Ausspähen von menschlicher Anwesenheit

Durch die Ausnutzung von Angriffen, die auf die Anwesenheit von Personen in Gebäuden hindeuten (siehe Seitenkanalattacken) können Objekte ausgekundschaftet werden, bzw. bestimmte Bereiche auf Anwesenheit überwacht werden.

Abbildung 3: Heatmap von Joggern in geheimer US Basis

Eine weitere Möglichkeit der Nutzung von solchen Erkenntnissen ist die Erstellung von Bewegungsprofilen von Personen. Hier sticht insbesondere die Verfolgung sogenannter Wearables (Smartwatches, Fitnesstracker o.ä.) hervor. Meist sind diese mit einem Mobiltelefon verbunden, tauschen regelmäßig Daten aus oder laden sie auf Webseiten hoch. Auf diese Weise wurde im November des Jahres 2017 eine geheime Afghanistan-Basis der US Armee enttarnt, als vom dem sozialem Fitnessnetzwerk Strava eine Heatmap mit 3 Billionen GPS-Punkten veröffentlicht wurde. Ein extrem heller Spot in einem ansonsten dunklem Gebiet in der Helmand Provinz in Afghanistan ließ dabei auf Anwesenheit schließen und die Heatmap war detailliert genug,

um sogar das Layout der Basis in Erfahrung zu bringen. Kartendienste wie Google Maps zeigten an der gleichen Stelle keinerlei Aktivitäten (Hern 2018-01-28).

4.4 Spurenloser Einbruch

Zugangssysteme mittels Radio Frequency Identification (RFID)-Tags, -Karten oder dem Mobiltelefon, sowie biometrische Systeme haben auch in Privathaushalten Einzug erhalten und ersetzen den klassischen Schlüssel an der Haustür. Sind diese Systeme mit einer Basisstation verbunden, ist diese im Normalfall an das Internet angebunden und kann über bereits erwähnte Wege angegriffen werden, um so Zutritt zu erlangen. Es besteht aber auch die Möglichkeit mittels RFID-Lesern den Inhalt des Zugangstokens auszulesen. Dazu genügt es oft schon den Leser für 1 bis 2 Sekunden in der Nähe des RFID-Tags zu bringen. Anschließend können mittels verschiedener Programme oder eines Brute-Force-Angriffs den Inhalt der Sector Keys [1] ausgelesen werden und so eine funktionierende Kopie des Zugangstokens repliziert werden. Mit diesem kann dann die Tür normal geöffnet werden, ohne das Einbruchsspuren zurück bleiben. Eventuell vorhandene Alarmsysteme können zudem häufig mit einem Störsender überlagert werden, indem ein weißes Rauschen auf den verwendeten Frequenzen gesendet wird.

Ein entsprechender Angriff inklusive verwendeter Soft- und Hardware wird in *Practical IoT hacking: The definitive guide to attacking the internet of things* auf den Seiten 372-379 ausführlich dargelegt.

[1] Sector Keys sind Verschlüsselungsdaten, die den Zugriff auf bestimmte Sektoren des RFID-Chips erlauben

5 Fazit

Die vorliegende Arbeit hat sich mit den technischen Vorraussetzungen von IoT-Geräten in behördlichen Infrastrukturen beschäftigt. Dabei wurde deutlich, dass mit der zunehmenden Verbreitung von IoT-Technologien neue sicherheitsrelevante Herausforderungen entstehen, denen Rechnung getragen werden muss.

Ein zentrales Ergebnis der Analyse ist, dass insbesondere schlecht gesicherte oder veraltete IoT-Geräte als Einfallstor für Angriffe dienen können. Angriffsszenarien wie Spoofing, Seitenkanalattacken oder das Auslesen von RFID-Tags zeigen, dass der Zugriff auf sensible Bereiche teilweise mit einfachsten Mitteln möglich ist – oft ohne Spuren zu hinterlassen. Auch die Nutzung kompromittierter Geräte in Botnetzen stellt ein erhebliches Risiko dar. Die beschriebenen technischen Grundlagen zeigen wie die Kommunikationsstrukturen der IoT-Geräte beschaffen sind.

Die Ergebnisse unterstreichen die Notwendigkeit, Sensibilisierung und Schulung von Mitarbeitenden in Bezug auf IoT-Sicherheit auszubauen sowie konkrete technische Maßnahmen – wie das Monitoring von Funkverbindungen und das konsequente Patchen von Geräten – umzusetzen. Für Behörden wie das RZF NRW könnte dies bedeuten, dass zukünftig eigene Richtlinien und Frühwarnsysteme für IoT-Risiken etabliert werden müssen.

Literaturverzeichnis

Abrishamchi, Mohammad Ali Nassiri et al. (2017). „Side channel attacks on smart home systems: A short overview“. In: *Proceedings IECON 2017 - 43nd Annual Conference of the IEEE Industrial Electronics Society*. Piscataway, NJ: IEEE, S. 8144–8149. ISBN: 978-1-5386-1127-2. DOI: 10.1109/IECON.2017.8217429.

Bundesamt für Sicherheit in der Informationstechnik (2015). *Die Lage der IT-Sicherheit in Deutschland 2015*. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2015.html (besucht am 18. 04. 2025).

Chantzis, Fotios et al. (2021). *Practical IoT hacking: The definitive guide to attacking the internet of things*. San Francisco: No Starch Press. ISBN: 9781718500907.

Cilfone, Antonio et al. (2019). „Wireless Mesh Networking: An IoT-Oriented Perspective Survey on Relevant Technologies“. In: *Future Internet* 11.4. ISSN: 1999-5903. DOI: 10.3390/fi11040099.

Gessler, Ralf und Thomas Krause (2015). *Wireless-Netzwerke für den Nahbereich: Eingebettete Funksysteme: Vergleich von standardisierten und proprietären Verfahren*. 2., aktualisierte u. erw. Aufl. 2015. Wiesbaden: Springer Fachmedien Wiesbaden. ISBN: 978-3-8348-2075-4. DOI: 10.1007/978-3-8348-2075-4.

Hern, Alex (2018-01-28). „Fitness tracking app Strava gives away location of secret US army bases“. In: *The Guardian* 2018. URL: https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (besucht am 18. 04. 2025).

Khan, L. A. et al. (2010). „Speaker recognition from encrypted VoIP communications“. In: *Digital Investigation* 7.1-2, S. 65–73. ISSN: 17422876. DOI: 10.1016/j.diin.2009.10.001.

Putman, C.G.J. et al. (2018). *Business Model of a Botnet*. DOI: 10.1109/PDP2018.2018.00077. URL: https://arxiv.org/pdf/1804.10848.