

Exposé zur Bachelorarbeit zum HackRF One

Felix Dormann

December 4, 2025

Inhaltsverzeichnis

1 Einführung	1
2 Vorgehensweise	3
3 Evaluierung	4

1 Einführung

Mehr und mehr Haushalte nutzen Smart Home Systeme für die Verwaltung unterschiedlichster Funktionen [1]. Smarte Haushaltsgeräte dienen dazu Haushalts-tätigkeiten zu Automatisieren und fernsteuerbar zu machen. Zum Beispiel lässt sich mit einem intelligenten Kühlschrank automatisch eine Einkaufsliste ver-fassen oder mit einem ferngesteuerten Türschloss von der Arbeit aus kontrol-lieren wer an der Tür steht und ob er hinein gelassen werden soll. Mit diesen Eigenschaften eröffnen sich jedoch auch Sicherheitsprobleme; eine dritte Partei könnte das Verhalten des Nutzers überwachen, Geräte fernsteuern und sogar ungestört in den Haushalt eindringen.

Daher sind Prüfungen der Datensicherheit bei solch kritischen Anwendungen besonders wichtig. Ein Netzwerkprotokoll für Smart Home Geräte regelt die Form der Kommunikation zwischen den Geräten. Es bestimmt beispielsweise die Datenrate, Verschlüsselung, Weiterleitung zum Heimnetzwerk sowie die Berech-tigungen der einzelnen Geräte. Da das Ziel dieser Arbeit die Nutzung eines Soft-ware Defined Radio ist, fällt Ethernet als untersuchbares Protokoll raus, obwohl es für Sicherheitskameras und ähnliches sehr beliebt ist. Die populären kabel-losen Protokolle Bluetooth und Wi-Fi haben eine verhältnismäßig hohe Daten-transferrate, was ihnen auch bessere Sicherheitsstandards erlaubt. Dies macht sie weniger anfällig für Angriffe von Studierenden mit begrenzter Erfahrung und Zeit. Aufgrund dieser Einschränkungen wird diese Arbeit besonderes Augen-merk auf Protokolle richten welche für batteriebetriebene Geräte geeignet sind und somit einen sehr geringen Stromverbrauch sowie Datenrate besitzen. Hier

seien Zigbee (sowie dessen Nachfolger Matter), Bluetooth Low Energie (BLE) und Z-Wave erwähnt welche alle die Anforderungen erfüllen.

Das Erkennen von Sicherheitslücken auf smarten Geräten hat zunehmende Geltung, aufgrund der ansteigenden Verbreitung [1] dieser. Eine Umfrage aus 2024 [1] schätzt dass in Deutschland bereits 46% der Haushalte Smart Home Geräte verwendet. Aufgrund der Vertraulichkeit der von diesen Geräten gesammelten Daten ist die Untersuchung auf Sicherheitslücken zunehmend bedeutend. Um Studierenden die Prüfung von Home Automation Systemen auf Fehler und Sicherheitslücken näherzubringen, macht sich das Hack RF One dienlich. Das Hack RF One ist ein Software Defined Radio (SDR), welches die meisten gängigen Funkfrequenzen abdeckt und recht leicht konfigurierbar ist.

SDRs werden bereits für viele Forschungsbereiche genutzt wie zum Beispiel nutzten Jedrzejewski et al[2] ein SDR für Radar Astronomie. In der Ökologie wurden von VonEhr et al. SDR zur Wildzählung genutzt. [3]. Anhand eines SDR konnten Sicherheitsforscher verschiedene Systeme auf Vulnerabilitäten prüfen. Feng et al. nutzten SDR zur Demonstration von GPS Spoofing[4]. Der Einsatz von SDRs in Smart Home Systemen ist bereits von Vitas et al. behandelt worden[5].

Das HackRF One wurde schon auf Nutzbarkeit in Lehrszenarien getestet und ein recht simpler GSM (2G) Sniffer implementiert[6]. Weiterhin nutzten Calderon et al. ein HackRF One zur Untersuchung von Denial-of-Service Attacks in WLAN Netzen[7]. Ein allgemeinerer Nutzen wurde von Wei et al. angestrebt, deren Studie den Nutzen die Erkennung von Radio Signalen verschiedener Modulierungen und Frequenzen demonstrierte[8].

Diese Arbeit wird sich die Forschungsfrage vornehmen:

Ist das HackRF One ein geeignetes Lehrwerkzeug, um angehenden Forschenden der Netzwerksicherheit die Nutzung von SDRs zu ermöglichen?

Konkret wird eine Aufgabe erstellt, welche das *HackRF One SDR von Great Scott Gadgets*[9] sowie die Software *Wireshark*[10] verwendet. Diese soll den Studierenden die Möglichkeiten und Begrenzungen von SDRs am Beispiel des HackRF One beibringen.

Im Smart Home Bereich entwickeln sich Netzwerkprotokolle schnell, da die Heterogenität und damit die Anforderung an diese Protokolle sehr groß ist. Aus diesem Grund ist es essenziell Werkzeuge zur sicherheitstechnischen Untersuchung für etwaige Protokolle und Geräte zur Hand zu haben. SDRs tun sich hier durch ihre große Vielseitigkeit hervor. Da die Verbreitung von Smart Home Systemen in Deutschland stetig zunimmt e.vSmartHomeAnwendungenFastJedem2024, ist die Wichtigkeit genauer Sicherheitsprüfungen nicht zu übersehen, insbesondere bei kritischen Anwendungen wie medizinischer Überwachung von Patienten. Durch wachsende Verbreitung von Smart Home Geräten, wie fern-steuerbaren Wärmepumpen und Smart-Speakern in Privathaushalten, treten zudem Bedenken über die Privatsphäre und Datensicherheit der Verbraucher auf.

Aufgrund des großen Wachstums an Geräten im Smart Home Bereich[?] ist das Testen der angewandten Technologien auf etwaige Sicherheitslöcher eine akute Aufgabe, insbesondere in privaten Haushalten welche möglicherweise geringere Sicherheitsstandards haben. Auch legislative Einflüsse machen eine Aufarbeitung von Smart Home Sicherheit aktuell notwendig. So werden in Deutschland durch das *Gebäudeenergiegesetz* unter anderem Wärmepumpen und Solarthermie-Systeme gefordert und gefördert, welche in der technischen Umsetzung häufig einen an das Internet angebundenen Thermostat benutzen.

Als Hauptstück dieser Arbeit soll eine Machbarkeitsstudie in Form einer spezifischen Anwendung für SDRs im Bereich der Smart Home Sicherheit dienen. Diese spezifische Anwendung wird wie in der Forschungsfrage beschrieben, eine Aufgabe zu Bildungszwecken sein. Eine Schwierigkeit hierbei wird sein, dass die Aufgabe nicht zu oberflächlich an das Thema herangeht und trotzdem einen realistischen Zeitrahmen und Schwierigkeitsgrad für die Lösung der Aufgabe einhält. Im speziellen sollte der Lernerfolg über die Nutzung einfacher Tools wie den GNU Radio Companion (GRC) hinausgehen. Der GRC ist eine graphische Anwendung, welche genutzt werden kann um spezifische Frequenzen zu demodulieren, Frequenzbereiche nach aktiven Sendern abzuhorchen oder aufgenommene Signale abzuschicken. Da diese Funktionalitäten recht weitgreifend sind, muss bei der Aufgabenstellung auf fortgeschrittene Techniken gesetzt werden die sich nicht einfach durch den GRC umsetzen lassen. Hierfür eignen sich unter anderem Entschlüsselung, DoS Attacks und Spoofing. Besonders ersteres ist natürlich ein umfangreiches und vor allem komplexes Forschungsgebiet, weshalb zu anspruchsvolle Anforderungen vermieden werden sollten.

Das Ziel dieser Arbeit soll eine praktische Anwendungsorientierte Aufgabenstellung für Studierende der Informatik sein, welche die Nutzung des HackRF One nahelegt und eine Basis für weitere Untersuchungen der Netzwerksicherheit bietet.

Eine empirische Studie mithilfe verschiedener möglicher Aufgabenstellungen anhand des HackRF One wird durchgeführt. Diese soll zeigen, inwiefern SDRs, wie dem HackRF One einsteigerfreundliche Netzwerksicherheitstools sein können. Als Validierungsmethode wird eine Feldstudie genutzt, in welcher die Aufgabenstellungen von Nutzern bearbeitet werden.

2 Vorgehensweise

Als grundlegende Methode dieser Arbeit steht eine Literaturstudie zum Stand der Forschung an erster Stelle. Auf den Ergebnissen dieser Studie soll dann eine Testphase aufbauen, in welcher verschiedene öffentliche Implementierungen auf das HackRF One übertragen werden. Jedes der getesteten Programme wird hierbei auf Nützlichkeit in Bezug auf Netzwerksicherheit (beziehungsweise Smart Home Sicherheit), Implementierungsaufwand und Umsetzbarkeit für Studierende untersucht.

Nachdem diese verschiedenen Programme und Anwendungen bewertet wurden, werden Aufgabenstellungen zu den am besten geeigneten Anwendungen erstellt. Um festzustellen, ob sich diese Aufgaben für den gegebenen Zeitrahmen sowie den Wissensstand der Studierenden eignen, werden die Aufgaben von einzelnen freiwilligen Studenten getestet und die jeweils benötigte Bearbeitungszeit gemessen, sowie die Rückmeldungen dokumentiert.

In der letzten Phase dieser Arbeit werden alle Rückmeldungen ausgewertet und womöglich finale Aufgabenstellungen aufgestellt, welche als umsetzbar und förderlich angesehen werden.

Als zeitliche Orientierung sollen hierfür folgende Meilensteine dienen:

1. Literaturübersicht/ Methodenübersicht: *4 Wochen*
2. Grundgerüst implementieren (Basisschnittstellen für alle weiteren Programme zum HackRF One ausarbeiten): *3 Wochen*
3. Mehrere Programme aus der Literatur umsetzen: *jeweils 1 Woche*
4. Formulieren der Aufgabenstellungen: *1 Woche*
5. Testlauf mit Studierenden auf Bachelorniveau: *2 Wochen*
6. Analysieren der Rückmeldungen der Studierenden: *1 Woche*
7. Anpassen und finalisieren der Aufgabenstellung: *1 Woche*
8. Fertigstellen der Dokumentation, sowie Auswertung der Ergebnisse als Fazit: *4 Wochen*

Aufgrund der bisher unbekannten Menge an spezifischen Programme welche getestet werden ist ein genauer Zeitpunkt für die Meilensteine noch nicht wägbar. Zudem ist zu erwarten, dass unterschiedliche Programme sehr verschiedene Zeitaufsprünge haben werden, weswegen die ZigBee spezifische Sicherheitssoftware SecBee[11] von CognoSec beispielsweise auf zwei Implementierungen ausgeweitet werden könnte, um die Möglichkeit zu haben alle Werkzeugen des größeren Programms auszuwerten.

3 Evaluierung

Als Grundlage für jegliche weitere Schritte dient eine Literaturstudie, welche die Nutzbarkeit von SDRs (insbesondere dem HackRF One) zur Untersuchung von Smart Home Sicherheit untersucht. Da in Schritt 3 einige Programme aus der aktuellen Forschung umgesetzt werden sollen, werden hierzu nur Programme genutzt welche auf der verfügbaren Hardware anwendbar sind. Da das HackRF One nur Half-Duplex betrieben werden kann, also nur senden oder empfangen kann, fallen mögliche Anwendungen wie eine Mobilfunkzelle weg. Zudem ist unter anderem SecBee auf ein älteres Netzwerkprotokoll (ZigBee 1.0) ausgelegt, und daher für modernere Smart Home Geräte vermutlich unbrauchbar.

Als Finale Evaluierung für soll in dieser Arbeit ein Vergleich mit einem bereits etablierten Werkzeug zur Untersuchung der Netzwerksicherheit dienen. Hierfür wird ein Gerät eingesetzt was jeglichen Netzverkehr des Access Points ausliest. Da diese Geräte sehr verschiedene Protokolle und Medien verwenden, wird ein besonderes Augenmerk auf die Kommunikation weniger ausgewählter Smart Home Geräte gelegt, und deren Gesendete sowie empfangene Kommunikation.

Wie in *Vorgehensweise* besprochen, soll durch einen Testlauf mit mehreren Studierenden entsprechenden Kenntnisstandes evaluiert werden. Hierfür soll das Feedback sowie eine Zeitmessung maßgeblich beitragen. Es wird anhand der Literaturstudie bewertet, ob die Aufgaben auch dem aktuellen Stand der Forschung entsprechen.

Da ?? vor allem auf das Lehren von sicherheitstechnischen Fähigkeiten abzielt, ist hierbei der Erfahrungsgewinn aller Testenden wichtig. Die Teilnehmenden des Testlaufs (5) müssen aus dem Bereich Informatik kommen, mindestens im 5. Fachsemester studieren und zudem noch keinen höheren Abschluss als Bachelor in diesem Bereich haben. Um für vergleichbare Ergebnisse zu sorgen, sollten die Aufgaben in einer offiziellen Räumlichkeit, wie beispielsweise einem Computerlabor durchgeführt werden. Dies garantiert, dass die Rückmeldungen sich auf die Aufgaben und nicht auf das Umfeld beziehen, was die Anpassungen der Aufgabenstellungen eindeutiger macht.

Quellenverzeichnis

- [1] B. e.V, “Smart-Home-Anwendungen in fast jedem zweiten Zuhause | Presseinformation | Bitkom e. V..” <https://www.bitkom.org/Presse/Presseinformation/Smart-Home-Anwendungen-in-fast-jedem-zweiten-Zuhause>, Aug. 2024.
- [2] K. Jedrzejewski, M. Malanowski, K. Kulpa, P. Krysik, and M. Pożoga, “Passive Space Object Observation using LOFAR Radio Telescope and Software-defined Radio Receiver,” in *2022 19th European Radar Conference (EuRAD)*, pp. 1–4, Sept. 2022.
- [3] K. VonEhr, S. Hilaski, B. E. Dunne, and J. Ward, “Software Defined Radio for direction-finding in UAV wildlife tracking,” in *2016 IEEE International Conference on Electro Information Technology (EIT)*, pp. 0464–0469, May 2016.
- [4] W. Feng, J.-M. Friedt, G. Goavec-Merou, and F. Meyer, “Software-Defined Radio Implemented GPS Spoofing and Its Computationally Efficient Detection and Suppression,” *IEEE Aerospace and Electronic Systems Magazine*, vol. 36, pp. 36–52, Mar. 2021.
- [5] I. Vitas, D. Šimunić, and P. Knežević, “Evaluation of Software Defined Radio systems for smart home environments,” in *2015 38th International*

Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), pp. 562–565, May 2015.

- [6] I. Martoyo, P. Setiasabda, H. Y. Kanalebe, H. P. Uranus, and M. Pardede, “Software Defined Radio for Education: Spectrum Analyzer, FM Receiver/Transmitter and GSM Sniffer with HackRF One,” in *2018 2nd Borneo International Conference on Applied Mathematics and Engineering (BICAME)*, (Balikpapan, Indonesia), pp. 188–192, IEEE, Dec. 2018.
- [7] L. Calderon and G. T. Salvador, “Detection and Analysis of Flipper Zero Deauthentication Signals Using HackRF One Software-Defined Radio,” in *2024 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, (Sakhir, Bahrain), pp. 798–804, IEEE, Nov. 2024.
- [8] W. Dai and C. Ji, “Modulation Recognition System of Electromagnetic Interference Signal Based on SDR,” *Telecom*, vol. 5, pp. 928–940, Sept. 2024.
- [9] “HackRF One - Great Scott Gadgets.” <https://greatscottgadgets.com/hackrf/one/>.
- [10] “Wireshark • Go Deep | About.” <https://www.wireshark.org/about.html>.
- [11] T. Zillner, “ZigBee Exploited - The Good, the Bad and the Ugly,”