



**Hochschule
Bonn-Rhein-Sieg**
University of Applied Sciences

Fachbereich Informatik
Department of Computer Science

Exposé

im Studiengang Bachelor Informatik

***Untersuchung der Sicherheit von OpenWrt
anhand der BSI TR-03148 mittels eines OpenWrt
betriebenen Heim-Routers***

von
Henry Weckermann

Erstprüfer: Prof. Dipl.-Ing. Markus Ullmann
Zweitprüfer: Prof. Dr.-Ing. Norbert Jung
Eingereicht am:

1. Ausgangspunkt

Internetrouter bilden häufig die Schnittstelle zwischen privaten Netzen und dem Internet. Dies gilt auch für die 90% der deutschen Haushalte, welche über einen Internetanschluss verfügen [1]. Der Aufbau eines Routers unterscheidet sich in den Grundzügen nicht von anderen eingebetteten Systemen. Das Betriebssystem eines Routers, in diesem Kontext Firmware genannt, ist jedoch oft sehr komplex. Die Firmware ist bereits beim Erwerb der Geräte installiert und wird vom jeweiligen Hersteller entwickelt. Die Kunden eines solchen Produktes haben oft keine Möglichkeit die meist proprietäre Firmware der Hersteller nach ihren Bedürfnissen anzupassen oder um Funktionalität zu erweitern. Darüber hinaus bleiben somit Software-Tests auf Sicherheitsfunktionalität, Stabilität oder andere Features dem Hersteller allein überlassen. Nur durch hohen Reverse Engineering Aufwand lassen sich Rückschlüsse auf die Vorgehensweisen des Gerätes ziehen oder eventuelle Sicherheitslücken entdecken. Dies ist in der heutigen Zeit, welche immer wieder von schwerwiegenden Sicherheitslücken in solchen Geräten geprägt ist, ein großes Problem.

Einer der weltweit größten Hersteller proprietärer Router und deren Software ist Cisco Systems. Router dieses Unternehmens werden mit der Firmware „Internetwork Operating System“ (IOS) betrieben. Im August des Jahres 2020 listete die „National Vulnerability Database“ (NVD) 860 „Common Vulnerabilities and Exposures“ (CVE), also Sicherheitsbedrohungen, für diese Cisco Firmware [2]. Eine Alternative zu den proprietären Firmwares der Router Hersteller bietet ein Open Source Projekt wie OpenWrt (abgeleitet von: Open Wireless Router).

Bei OpenWrt handelt es sich um eine kostenlose, frei verfügbare Linux Distribution für eingebettete Systeme, besonders Router [3]. Es verfügt über einen eigenen Paket-Manager, mit Hilfe dessen es möglich ist einen sehr großen Umfang an Funktionalität nachträglich zu installieren. Weiterhin bietet es ein eigenes Dateisystem, welches dem „extended filesystem“ (ext) ähnlich ist. Wie bereits aus den genannten Punkten ersichtlich wird, werden durch die Herangehensweise dieses Projektes viele der oben genannten negativen Aspekte proprietärer Router Software verbessert. Der Quellcode von OpenWrt lässt sich mit wenig Aufwand ändern oder selbstständig auf Fehler überprüfen,

bevor dieser für ein Gerät kompiliert werden kann. Ebenfalls ermöglicht der offene Quellcode IT-Sicherheitsaudits privater und öffentlicher Instanzen.

Allerdings müssen auch die negativen Aspekte eines solchen öffentlichen Unterfangens betrachtet werden. Die Mitarbeit an einem solchen Projekt ist rein freiwillig und eine Qualitätssicherung muss nicht unbedingt stattfinden. Dennoch wird eine von OpenWrt abstammende Software von der Freifunk Initiative genutzt [4]. Diese stellt ein freies Funknetz zur Verfügung, welches vor allem Anonymität und Schutz vor Überwachung bieten soll.

So soll es das Ziel dieser Arbeit sein, einen Einblick in einige Aspekte der Sicherheitslage von OpenWrt zu gewinnen. Kann OpenWrt die Versprechen an Sicherheit und Betriebsumfang halten, oder sollte man doch auf vorinstallierte proprietäre Firmware setzen?

2. Zielsetzung

In der anzufertigenden wissenschaftlichen Arbeit soll als Ausgangspunkt einer Sicherheitsanalyse von Router Firmware die BSI TR-03148: Secure Broadband Router [5] auf einen OpenWrt fähigen Router angewendet bzw. überprüft werden. Hierbei sollen einige Aspekte der Sicherheit von OpenWrt anhand dieser Technischen Richtlinie geprüft werden. Die Technische Richtlinie beschreibt sehr umfängliche Tests und Anforderungen an Router Firmware, welche von Herstellern eingehalten werden sollten, um grundsätzlich die Sicherheit des Gerätes und der darauf betriebenen Software feststellen zu können. Ein positiver Nebeneffekt ist, dass die meisten Anforderungen auch noch im Nachhinein in einer Firmware angepasst werden können, ohne die gesamte Software Architektur ändern zu müssen. Die Anforderungen sind mit Absicht allgemein gehalten, um sie auf ein möglichst weites Spektrum von Geräten anwenden zu können. So also auch auf das Open Source Projekt OpenWrt. Da es natürlich keinen zuständigen Hersteller gibt, sich OpenWrt aber großer Beliebtheit erfreut [6], ist eine Überprüfung anhand der Technischen Richtlinie des BSI von Interesse. Die Erfüllung der Technischen Richtlinie 03148 bietet zudem eine weitere Möglichkeit für Endanwender. Falls ein noch funktionierendes Gerät nicht mehr durch Updates vom Hersteller unterstützt wird, könnte es durch das Betreiben mit OpenWrt weiter sicher genutzt werden, statt einem Neukauf weichen zu müssen.

Zunächst sollen die zugehörigen Tests der BSI TR-03148 möglichst vollumfänglich an einem, im Vorhinein festgelegten, OpenWrt fähigen Router durchgeführt und der Test Spezifikation folgend dokumentiert werden. Funktionalität wie ein integriertes Virtual Private Network (VPN) oder Voice over IP (VoIP) sollen dabei nicht in den Anforderungsbereich fallen. Wenn es der Testfall anbietet so soll ein automatischer Test entwickelt werden, welcher in Zukunft die Durchführung beschleunigen kann.

Nach Abschluss aller Tests könnte in einem letzten Schritt ein Software Tool wie das vom Fraunhofer Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) entwickelte Open Source Software Projekt „FACT“ [7] verwendet werden, um auch einige Varianten der aktuellen „stable release“ Version von OpenWrt damit zu analysieren und die Ergebnisse denen des „Home Router Security Report 2020“ gegenüberzustellen.

Nachdem alle Tests abgeschlossen wurden, sollen die Ergebnisse zusammengetragen, ausgewertet und in Kontext gesetzt werden. Basierend auf den Anhaltspunkten, die aus den Tests gewonnen wurden, muss eine Sicherheitsbewertung von OpenWrt's stable release Version für den ausgewählten Router erarbeitet werden. Darüber hinaus müssen Wege und Vorschläge entwickelt werden, die fehlgeschlagenen Tests zu bestehen, um die Sicherheit zu erhöhen.

Diese wissenschaftliche Untersuchung setzt sich nicht das Ziel die vollständige Sicherheit aller Aspekte der Software OpenWrt nachzuweisen, auch wenn dies natürlich wünschenswert wäre. Es muss immer betont werden, dass viele potenziell wichtige Aspekte einer sicheren Software nicht in Betracht gezogen werden. Vielmehr soll eine Grundlage bzw. ein möglicher Einstiegspunkt für weitere Forschung an Methoden und Abläufen zum Testen von Open Source (Router) Software geschaffen werden.

3. Vorgehensweise und Umsetzung

Zunächst muss für eine erfolgreiche Durchführung der Untersuchung ein vorher festgelegter Router mit OpenWrt bespielt werden, sowie auf Stabilität der Anwendung geprüft werden. Das Modell soll vor allem aufgrund einer ausgiebigen Dokumentation in Bezug auf OpenWrt, sowie des Preis-/Leistungsverhältnisses bestimmt werden. Darüber hinaus muss die aktuellste Version von OpenWrt unterstützt werden und es müssen genügend RAM und Speicherplatz verfügbar sein.

Die Durchführung der Untersuchung anhand der BSI TR-03148 soll den Anforderungen konform anhand der dazugehörigen Tabellenkalkulationsdatei durchgeführt werden. Dazu wird zunächst das sog. "Conformance Statement" ausgefüllt, in welchem Angaben zur Beschaffenheit des Gerätes und der Firmware, sowie Dokumentation und Bedienungsanleitung gemacht werden. Ebenso werden hier die Fähigkeiten des Gerätes aufgeführt und festgehalten. Es werden alle privaten und öffentlichen Schnittstellen des Gerätes, alle statischen kryptographischen Schlüssel, alle Funktionalitäten und Konfigurationen festgehalten. Aus diesen Angaben lässt sich entscheiden, ob die TR-03148 überhaupt auf den ausgewählten Router anwendbar ist. Ebenso sind diese Angaben von großem Interesse für einige der Testfälle. Wenn dieser Schritt abgeschlossen ist, werden die festgelegten Testfälle der TR-03148 schrittweise durchgeführt. Dafür muss zunächst festgestellt werden, ob der Testfall anwendbar ist, woraufhin der Test durchgeführt wird und die Ergebnisse, sowie alle sonstigen Notizen in der Datei festgehalten werden. Erstellte Bildschirmfotos oder weitere Referenzen für den Testfall werden in einer einheitlichen und übersichtlichen Weise gespeichert, sodass diese später einfach nachzuvollziehen sind. Für die Reihenfolge des Vorgehens soll sich an den bereits gemachten Angaben von „MUST“ und „SHOULD“ orientiert werden, sodass zunächst die MUST-Anforderungen bearbeitet werden. Wenn der Testfall es anbietet, soll zur Durchführung desselben ein automatischer Test entworfen werden, welcher Wiederholungen erleichtert und der Reproduzierbarkeit des Ergebnisses dienlich sein soll.

Wenn es sich im zeitlichen Rahmen der Bachelor-Arbeit umsetzen ließe, so wäre auch eine direkte Gegenüberstellung der Ergebnisse des „Home Router Security Reports 2020“ mit ausgewählten OpenWrt Firmware Varianten eine

Möglichkeit das Thema noch weiter auszuführen und einen tieferen Einblick in die Sicherheitslage von OpenWrt zu gewinnen. Der „Home Router Security Report 2020“ [8] des Fraunhofer FKIE beschreibt die Nutzung der Open Source Software „FACT“ [7], welche ebenfalls vom FKIE entwickelt wird. Dazu wurden 127 [8, p. 3] verschiedene Firmware Versionen verschiedener Router Hersteller durch das Tool analysiert und die Ergebnisse ausgewertet. Ausgewertet wurden unter anderem, ob es für die betrachtete Version bereits bestehende Critical Vulnerability and Exposure (CVE) Einträge gibt, ob kryptographisches Material oder Benutzerkonten gefunden werden konnten oder ob Linux-Härtungsmaßnahmen eingesetzt werden. Da die Ergebnisse mit dem gleichen Programm gesammelt und analysiert werden, wäre ein Vergleich leicht umsetzbar.

Abschließend müssen alle Ergebnisse zusammengetragen und ein Urteil über die Sicherheit von OpenWrt formuliert werden. Es soll jedoch nicht nur die Sicherheitslage von OpenWrt im Vordergrund stehen, sondern auch eine differenzierte Bewertung der verwendeten Methoden zur Analyse von OpenWrt. Eine wissenschaftliche Diskussion der Ergebnisse, Limitationen des durchgeführten Vorgehens, sowie Vorschläge und Ideen für zukünftig notwendige Forschungsarbeit wird sich anschließen.

4. Gliederungsentwurf für die Abschlussarbeit

Abbildungsverzeichnis

Abkürzungsverzeichnis

1 Einführung

- 1.1 Was ist OpenWrt?
- 1.2 Relevanz und Verwendung von OpenWrt im Jahr 2020
- 1.3 Verwendung von OpenWrt im Kontext weitverbreiteter Mainstream-Produkte
- 1.4 Bisherige Forschung zur Sicherheit von OpenWrt
- 1.5 Router Firmware und Analyseverfahren
- 1.6 Beschreibung der BSI TR-03148: Secure Broadband Router
- 1.7 Zielsetzung dieser Arbeit

2 Methoden

- 2.1 Übersicht und Begründung der verwendeten Methoden
- 2.2 Aufbau und Beschreibung der Arbeitsumgebung
- 2.3 Durchführung der Testfälle der BSI TR-03148
 - 2.3.1 Anfertigung des Conformance Statements
 - 2.3.2 Ausarbeitung der Test Documentation
 - I. Modul A - Private Network
 - II. Modul B – Public Network
 - III. Modul C – Functionalities
 - IV. Modul D – Configuration and Information
 - V. Modul E – Firmware Updates
 - ...
 - XII. Nicht anwendbare Testfälle und Komplikationen
- 2.4 Nötige Änderungen zum vollständigen Bestehen der Technischen Richtlinie
- 2.5 Statischer Software Test von OpenWrt mit „FACT“
 - 2.5.1 Installation und Testumgebung
 - 2.5.2 Erstellung des Corpus
 - 2.5.3 Durchgeführte Tests und Metriken

2.5.4 Graphische Auswertung der Ergebnisse

2.5.5 Graphische und textuelle Gegenüberstellungen mit
Ergebnissen von Produkten des Verbrauchemarktes

3 Ergebnisse

3.1 Ergebnisse der Technischen Richtlinie

3.2 Ergebnisse der statischen Auswertung mit „FACT“

4 Diskussion

4.1 Zusammenfassung der Ergebnisse

4.2 Limitationen

4.3 Implikationen

5 Fazit

Literaturverzeichnis

Anhang

Eidesstattliche Erklärung

5. Zeit- /Arbeitsplanung

Woche 1:

- Installation und Einrichtung von OpenWrt auf einem ausgewählten Router
- Testen der Stabilität, um einen reibungslosen Ablauf zu garantieren
- Anfertigung eines richtig formatierten „Templates“ der Bachelorarbeit
- Anlegen einer geeigneten Ordner-Struktur zur korrekten Ablage von gesammelten Testergebnissen
- Eine automatische Datensicherung und Versionierung anlegen
- Reihenfolge der Testfälle festlegen

Woche 2-9:

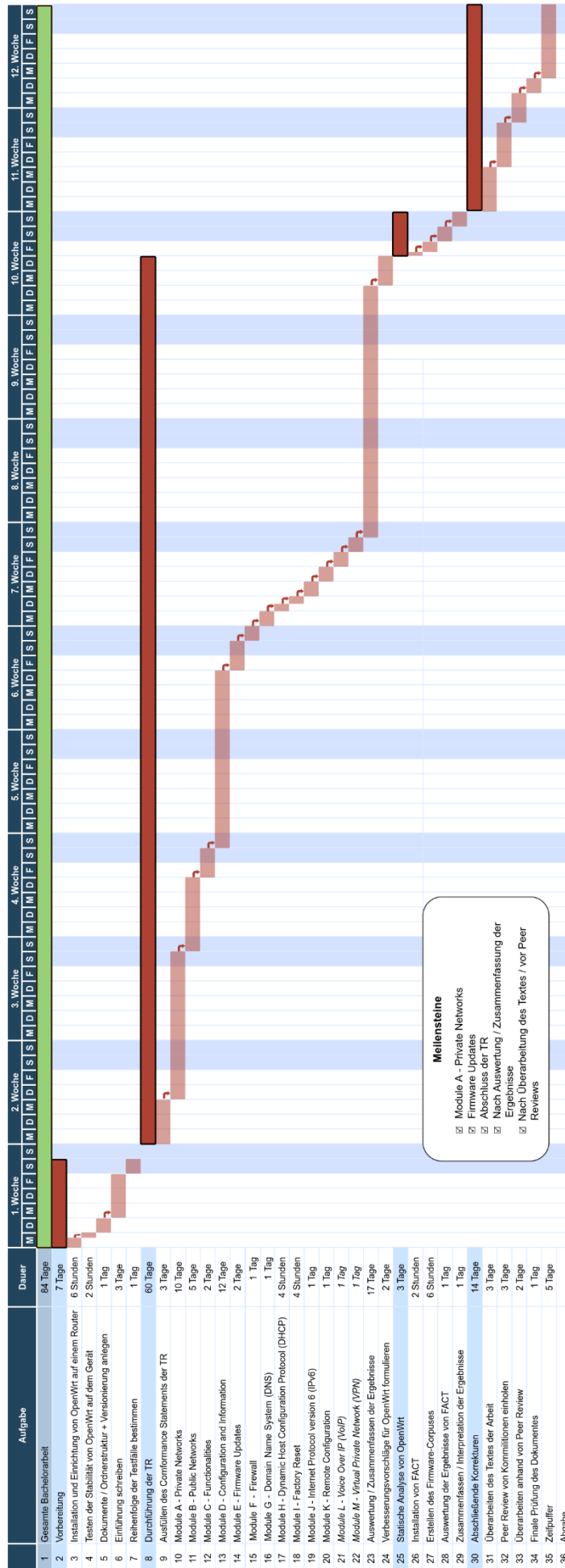
- Formulierung des Abschnittes „Einführung“, sowie der Abschnitte 2.1 und 2.2
- Ausfüllen und erarbeiten des „Conformance Statements“
- Durchführung und Dokumentation der Testfälle der TR-03148
- Simultane schriftliche Aufbereitung der Ergebnisse

Woche 10-11:

- Statische Analyse und Vergleich von OpenWrt mit „FACT“ aufarbeiten und in die Arbeit integrieren
- Erarbeiten der Kapitel 3, 4 und 5

Woche 11-12:

- „Peer review“ einiger Kommilitonen einholen
- Überarbeitung anhand dieser Kritikpunkte



Literatur

- [1] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), BSI TR-03148:Secure Broadband Router: Requirements for secure Broadband Routers. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=3 (Letzter Zugriff: 11. August 2020).
- [2] P. Herzog, "Open-source security testing methodology manual," Institute for Security and Open Methodologies (ISECOM), 2003. [Online]. Verfügbar unter: <http://cdn.preterhuman.net/texts/other/osstmm.pdf> (Letzter Zugriff: 11. August 2020).
- [3] T. Howlett, Open source security tools: Prentice Hall, 2004.
- [4] C. M. Kozierok, The TCP/IP guide: A comprehensive, illustrated Internet protocols reference, 1st ed. San Francisco: No Starch Press, 2005. [Online]. Verfügbar unter: <http://proquest.tech.safaribooksonline.de/9781593270476> (Letzter Zugriff: 11. August 2020).
- [5] G. Lawton, "Open source security: opportunity or oxymoron?," Computer, vol. 35, no. 3, pp. 18–21, 2002.
- [6] OpenWrt Website, Documentation of the OpenWrt Project. [Online]. Verfügbar unter: <https://openwrt.org/docs/start> (Letzter Zugriff: 11. August 2020).
- [7] C. Payne, "On the security of open source software," Information systems journal, vol. 12, no. 1, pp. 61–78, 2002.
- [8] Peter Weidenbach, Johannes vom Dorp, Home Router Security Report 2020. [Online]. Verfügbar unter: https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf (Letzter Zugriff: 11. August 2020).
- [9] T. Wrightson, Wireless network security: A beginner's guide [set up and maintain secure wireless networks; find out how hackers break in and how to stop them; avoid attacks and prevent vulnerabilities. New York, NY: McGraw-Hill, 2012.

Quellenverzeichnis

- [1] Destatis, *Private Haushalte in der Informationsgesellschaft: Nutzung von Informations- und Kommunikationstechnologien: Statistisches Bundesamt*. [Online]. Verfügbar unter: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/IT-Nutzung/Publicationen/Downloads-IT-Nutzung/private-haushalte-ikt-2150400187004.pdf?__blob=publicationFile (Letzter Zugriff: 11. August 2020).
- [2] National Institute of Standards and Technology, *Cisco IOS CVE Entries*. [Online]. Verfügbar unter: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Cisco+IOS&queryType=phrase&search_type=all (Letzter Zugriff: 11. August 2020).
- [3] OpenWrt Website, *Documentation of the OpenWrt Project*. [Online]. Verfügbar unter: <https://openwrt.org/docs/start> (Letzter Zugriff: Aug. 11 2020).
- [4] Freifunk Initiative, *OpenWrt*. [Online]. Verfügbar unter: <https://wiki.freifunk.net/OpenWrt> (Letzter Zugriff: 11. August 2020).
- [5] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), *BSI TR-03148: Secure Broadband Router: Requirements for secure Broadband Routers*. [Online]. Verfügbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publicationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=3 (Letzter Zugriff: 11. August 2020).
- [6] OpenWrt Project, *Statistical Overview*. [Online]. Verfügbar unter: <https://downloads.openwrt.org/stats/> (Letzter Zugriff: 11. August 2020).
- [7] FACT Core. [Online]. Verfügbar unter: https://github.com/fkie-cad/FACT_core (Letzter Zugriff: 11. August 2020).
- [8] Peter Weidenbach, Johannes vom Dorp, *Home Router Security Report 2020*. [Online]. Verfügbar unter: https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf (Letzter Zugriff: 11. August 2020).