Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Fachbereich Informatik
Department of Computer Science

Exposé

im Studiengang Bachelor Informatik

Anwendung von BSI TR-03148 auf einen OpenWrt Router

von
Henry Weckermann

Erstprüfer: Prof. Dipl.-Ing. Markus Ullmann
Zweitprüfer: *NN*
Eingereicht am: *TODO*

1. Ausgangspunkt

90% alle deutschen Haushalte verfügen über einen Internetanschluss [1]. Aber ob man von Heimnetzen oder Firmennetzen spricht spielt hier keine Rolle, denn die Verwendung eines Routers haben sie alle gemeinsam. Ein Router ist das Herzstück eines Netzwerks, welcher den Zugang zum Internet erst ermöglicht. Wie so viele andere unscheinbare, kleine Geräte handelt es sich hierbei aber um nichts anderes als einen kleinen Computer. Wie jeder andere Computer auch benötigt dieses Gerät ein Betriebssystem, welches in diesem Umfeld Firmware genannt wird. Diese Firmware wird in den meisten Fällen schon von Werk aus mitgeliefert, produziert und vermarktet von den jeweiligen Herstellern. Die Kunden eines solchen Produktes haben eigentlich keine Möglichkeit die meist proprietäre Firmware der Hersteller nach ihren eigenen Wünschen anzupassen und umzubauen. Darüber hinaus bleiben somit Software-Tests auf Sicherheitsfunktionalität, Stabilität oder andere Features dem Hersteller allein überlassen. Nur durch hohen Reverse Engineering Aufwand lassen sich überhaupt Rückschlüsse auf die inneren Vorgehensweisen 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 arbeiten mit dem Betriebssystem „Internetwork Operating System“ (IOS). Im August des Jahres 2020 listet die „National Vulnerability Database“ (NVD) 860 „Common Vulnerabilities and Exposures“ (CVE), also Sicherheitsbedrohungen, für diese Cisco Firmware [2]. Mit derartigen Zahlen ist es nicht verwunderlich, dass auch Open Source Router Firmware zur Verfügung steht. Ein Vertreter in diesem Bereich ist 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 Natur

dieses Projektes viele der oben genannten negativen Aspekte proprietärer Router Software verbessert, bzw. durch eine alternative Herangehensweise gehandhabt. Eine einfache Anpassbarkeit an die eigenen Vorstellungen, sowie eigene Sicherheitsaudits sind problemlos möglich.

Jedoch muss dieses positive Bild einer solchen Firmware auch mit Vorsicht 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 etablierte Markgrößen setzen?

2. Zielsetzung

In der anzufertigenden 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 bei diesen Open Source Projekt natürlich keinen zuständigen Hersteller gibt, sich das Projekt 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.

In einem weiteren Schritt soll eine Gegenüberstellung bzw. ein Vergleich der Vorgehensweise der BSI Technischen Richtlinie 03148 mit anderen Testverfahren und Herangehensweisen angefertigt werden. Hier sollen insbesondere die Besonderheiten der verschiedenen Verfahren und ihre Bedeutung herausgearbeitet werden. 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 OpenWrts 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 Arbeit 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 Arbeit ein vorher festgelegter Router mit OpenWrt bespielt werden, sowie auf Stabilität der Anwendung geprüft werden. Aufgrund bereits erfolgter Nachforschung bieten sich die folgenden Modelle aufgrund ihrer ausgiebigen Dokumentation in Bezug auf OpenWrt, sowie ihres Preis-/ Leistungsverhältnisses an:

- Linksys WRT1200AC
- ALFA Network AP120C-AC
- Archer C7 AC1750 v5
- Linksys EA8300
- Linksys EA6350 v3
- GL.iNet GL-B1300
- Netgear R6220

Alle Geräte unterstützen die neuste Version von OpenWrt.

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 seien soll.

Nachdem alle in der Prüfspezifikation der BSI TR-03148 definierten Tests, welche nicht im Vorhinein ausgeschlossen wurden, abgeschlossen und dokumentiert sind, soll eine Gegenüberstellung der Testmethodik der Technischen Richtlinie mit anderen Testmethoden der Sicherheitsinformatik angefertigt werden. Hierzu bietet sich ein Vergleich mit der Methodik der kürzlich erschienenen Veröffentlichung des Fraunhofer FKIE, dem „Home Router Security Report 2020“ [8] an. Aber auch ein allgemeiner Vergleich mit Methoden wie statischen Softwaretests, Black- und Whitebox Testen oder Fuzzing ist möglich. Es sollen hier vor Allem Unterschiede und Besonderheiten der jeweiligen Testverfahren aufgezeigt werden und die Wichtigkeit des Zusammenspiels mehrerer Verfahren unterstrichen werden.

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 Vergleichende Gegenüberstellung verschiedener Methodiken zur Feststellung und Überprüfung der Softwaresicherheit von Router Firmware*
  - *2.5.1 Definition der Methodik der TR-03148*

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:

- Einarbeitung des Vergleiches (wenn zeitlich machbar)
- Statische Analyse und Vergleich von OpenWrt mit „FACT“ aufarbeiten und in die Arbeit integrieren (1 Tag)
- Erarbeiten der Kapitel 3, 4 und 5

Woche 11-12:

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

Literatur

[1] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), BSI TR-03148:Secure Broadband Router: Requirements for secure Broadband Routers. [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=3 (accessed: Aug. 11 2020).

[2] P. Herzog, “Open-source security testing methodology manual,” Institute for Security and Open Methodologies (ISECOM), 2003. [Online]. Available: http://cdn.preterhuman.net/texts/other/osstmm.pdf

[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]. Available: http://proquest.tech.safaribooksonline.de/9781593270476

[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]. Available: https://openwrt.org/docs/start (accessed: Aug. 11 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]. Available: https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf (accessed: Aug. 11 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 Informa-tions-und Kommunikationstechnologien: Statistisches Bundesamt.* [Online]. Available: https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/IT-Nutzung/Publikationen/Downloads-IT-Nutzung/private-haushalte-ikt-2150400187004.pdf?__blob=publicationFile (accessed: Aug. 11 2020).

[2] National Institute of Standards and Technology, *Cisco IOS CVE Entries.* [Online]. Available: https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=Cisco+IOS&queryType=phrase&search_type=all (accessed: Aug. 11 2020).

[3] OpenWrt Website, *Documentation of the OpenWrt Project.* [Online]. Available: https://openwrt.org/docs/start (accessed: Aug. 11 2020).

[4] Freifunk Initiative, *OpenWrt.* [Online]. Available: https://wiki.freifunk.net/OpenWrt (accessed: Aug. 11 2020).

[5] Bundesamt für Sicherheit in der Informationstechnik (Hrsg.), *BSI TR-03148:Secure Broadband Router: Requirements for secure Broadband Routers.* [Online]. Available: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=3 (accessed: Aug. 11 2020).

[6] OpenWrt Project, *Statistical Overview.* [Online]. Available: https://downloads.openwrt.org/stats/ (accessed: Aug. 11 2020).

[7] *FACT Core.* [Online]. Available: https://github.com/fkie-cad/FACT_core (accessed: Aug. 11 2020).

[8] Peter Weidenbach, Johannes vom Dorp, *Home Router Security Report 2020.* [Online]. Available: https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf (accessed: Aug. 11 2020).