Hochschule
Bonn-Rhein-Sieg
University of Applied Sciences

Fachbereich Informatik
Computer Science Department

Bundesamt
für Sicherheit in der
Informationstechnik

Abschlussarbeit

im Bachelorstudiengang Informatik

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

von Henry Weckermann

Erstbetreuer:	**Prof. Markus Ullmann**
Zweitbetreuer:	**Prof. Dr. Norbert Jung**
Betreuer im BSI:	**Florian Bierhoff**
Eingereicht am:	**25.01.2021**

Erklärung

Hiermit erkläre ich an Eides Statt, dass ich die vorliegende Arbeit selbstständig und ohne Benutzung anderer als der angegebenen Hilfsmittel angefertigt habe. Die aus fremden Quellen direkt oder indirekt übernommenen Gedanken sind als solche kenntlich gemacht. Die Arbeit wurde bisher in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt bzw. nicht veröffentlicht.

Bonn, den 25.01.2021

Henry Weckermann

Abstract

In an increasingly digitalized world, the network router often forms the border between the home network and the internet. An increasing number of attacks on these very home networks for the spread of ransomware and botnets is observed worldwide [1, p. 11-15]. This makes it more important for manufacturers and customers to evaluate the security of their products. The goal of this thesis was to evaluate the open-source router operating system OpenWrt using the “Technical Guideline 03148 - Secure Broadband Routers“ of the German Federal Office for Information Security. Furthermore, solutions for shortcomings of OpenWrt were worked out in cases were OpenWrt could not comply with the guideline. To address another possibility for security verification the source code of various open source router operating systems were statically analyzed. Finally, the results of this analysis were compared with the results of the “Home Router Security Report 2020“.

To support the premise that OpenWrt is compliant with the Technical Guideline, all applicable test cases were tested against the published test criteria. Furthermore, the source codes of seven contemporary open source router firmware images were statically analyzed using the “Firmware Analysis and Comparison Tool“ so that the results were comparable to the “Home Router Security Report 2020“. The results showed that OpenWrt fails to comply in 22% of the test cases, but the predicted effort to correct these weaknesses is low. The static code analysis showed that the open source firmware, while not without shortcomings, is superior to the proprietary firmware which was analyzed in the “Home Router Security Report“.

The results showed that, with some adjustments, OpenWrt can present a safer alternative to proprietary pre-installed router firmware and that open source firmware performs comparatively well when using static code analysis. Ultimately, a repetition of the static code analysis with a larger set of open-source firmware is desirable in order to establish a higher degree of comparability.

Zusammenfassung

In einer zunehmend digitalisierten Welt bildet der Netzwerk-Router häufig die Grenze zwischen dem Heimnetzwerk und dem Internet. Weltweit wird eine zunehmende Anzahl an Angriffen auf eben diese Heimnetze für die Verbreitung von Ransomware und Bot-Netzen beobachtet [1, p. 11-15]. Umso wichtiger sind Mittel und Wege für Hersteller und Kunden die Sicherheit ihrer Produkte zu evaluieren. Das Ziel dieser Arbeit war es das quelloffene Router-Betriebssystem OpenWrt mittels der „Technischen Richtlinie 03148 - Sichere Breitband Router“ des deutschen Bundesamtes für Sicherheit in der Informationstechnik (BSI) zu prüfen. Ferner sollten Lösungen für eventuelle Defizite erarbeitet werden, falls OpenWrt den Anforderungen der TR nicht entsprechen kann. Anschließend wurde der Quellcode verschiedener quelloffener Router-Betriebssysteme statisch analysiert, um eine weitere Möglichkeit der Sicherheitsüberprüfung zu thematisieren. Die Ergebnisse dieser Analyse wurden abschließend mit den Ergebnissen des „Home Router Security Reports 2020“ verglichen.

Um die Annahme zu stützen, dass OpenWrt TR-konform ist, wurden alle anwendbaren Testfälle anhand der veröffentlichten Prüfkriterien getestet. Weiterhin wurde der Quellcode von sieben quelloffenen Router Firmware-Abbildern statisch mit dem „Firmware Analysis and Comparison Tool“ analysiert, sodass die Ergebnisse mit dem „Home Router Security Report 2020“ vergleichbar waren. Die Ergebnisse zeigten, dass OpenWrt 22% der Technischen Richtlinie nicht besteht, der Aufwand aber gering ist, diese Defizite auszubessern. Die statische Code-Analyse zeigte, dass die quelloffene Firmware zwar nicht ohne Mängel ist, jedoch im Vergleich der proprietären Firmware überlegen ist.

Die Ergebnisse zeigen, dass OpenWrt mit einigen Anpassungen eine sichere Alternative zu proprietärer vorinstallierter Firmware bilden kann und die quelloffene Firmware bei einer statischen Code-Analyse vergleichsweise gut abschneidet. Letztlich ist eine Wiederholung der statischen Code-Analyse mit einem größeren Korpus erstrebenswert, um eine höhere Vergleichbarkeit herzustellen.

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CCC	Chaos Computer Club
CNA	CVE Numbering Authorities
CPE	Common Platform Enumeration
CSRF	Cross-Site-Request-Forgery
CSS	Cascading Style Sheets
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
(D)DoS	(Distributed) Denial of Service
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DUT	Device under Test.
EOL	End Of Life
FACT	Firmware Analysis and Comparison Tool
FIRST	Forum of Incident Response and Security Teams
FKIE	Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie
GOT	Global Offset Table
GPL	GNU General Public License
ICS	Implementation Conformance Statement
IDE	Integrated Development Environment
IoT	Internet of Things
IP	Internet Protocol
ISP	Internet Service Provider
LAN	Local Area Network
LuCI	OpenWrt web user interface
NAT	Network Address Translation
NTP	Network Time Protokoll
NX-Bit	No eXecute Bit
OpenWrt	Open Wireless Router
OWASP	Open Web Application Security Project
PIE	Position-Independent Executables
RATS	Rough Auditing Tool for Security
RELRO	RELocation Read-Only
SCP	Secure Copy
SDK	Software Developer Kit
SE	Secure Element
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SOHO	Small Office, Home Office
TEE	Trusted Execution Environment
TFTP	Trivial File Transfer Protocol
VoIP	Voice over IP
VPN	Virtual Private Network
VPS	Virtual Private Server
WAN	Wide Area Network
WPA	Wi-Fi Protected Access
WPS	Wi-Fi Protected Setup

Inhaltsverzeichnis

Kapitel 1

Einleitung

1.1 Ausgangspunkt

Das Internet wird ein zunehmend wichtigerer Teil des menschlichen Lebens. Öffentliche Hotspots, internetfähige Alltags-Geräte (Internet of Things (IoT) Geräte) und mobiles Arbeiten von Zuhause sind nur einige Beispiele für technologische Neuerungen, welche ohne das Internet nicht möglich wären. Die rund 38 Mio. Netzanbindungen an DSL-, Kabel-, oder Glasfaser-Anschlüsse in Deutschland werden in Heimnetzen und Kleinunternehmen überwiegend durch Netzwerk-Router realisiert [2]. In vielen Fällen bildet der Router die direkte Schnittstelle zwischen dem Internet und dem privaten Netzwerk. So stellt dieser durch Paketfilter und eine Firewall meist auch die einzige zentrale Sicherheitskomponente zum Schutz des Netzwerkes bereit. Ein erfolgreicher Angriff auf den Router bietet einem Angreifer unzählige Möglichkeiten, in das Netz einzugreifen und so immensen Schaden anzurichten. Neben bekannten Zielen wie private Daten und Passwörtern kann der Router auch als Teil eines Bot-Netzwerks für Distributed Denial-of-Service (DDoS) verwendet werden oder als Einfallstor auf weitere Geräte des Netzwerkes [3]. In Korrelation mit den stark steigenden Fällen von Cyberkriminalität im privaten und wirtschaftlichen Umfeld zeigt dies wie wichtig ein von Werk aus geschützter Router mit einer sicheren Konfiguration ist [1].

Handelsübliche Router, wie sie in Privathaushalten und Small Office, Home Office (SOHO) Umgebungen eingesetzt werden sind bereits mit einem proprietären Betriebssystem bespielt. Die Sicherheit dieser meist proprietären Distribution kann nur mit großem Aufwand von Endnutzern verifiziert werden und Sicherheitsupdates nur vom Hersteller veröffentlicht werden. Hersteller können in der zunehmend kürzer werdenden Zeit zwischen neuen Iterationen von Malware meist nicht in angemessener Zeit reagieren, um Sicherheitsupdates zur Verfügung zu stellen. Quelloffene Router Firmware wie OpenWrt, DD-Wrt, Tomato oder LibreCMC bieten eine Alternative zu den vorinstallierten, proprietären Betriebssystemen der Router [4, 5, 6, 7]. Diese Projekte können vollständig eingesehen, modifiziert und kompiliert werden, sodass die Sicherheit des Produktes einfacher evaluiert werden kann. Ebenfalls können aufgrund der hohen Anzahl an Mitwirkenden Sicherheits- und Funktions-

updates schneller entwickelt und veröffentlicht werden. Umfangreiche Überprüfungen dieser Projekte, wie z.B. anhand der BSI TR-03148: Sichere Broadband Router, werden allerdings aufgrund des hohen Zeit- bzw. Kostenaufwands selten durchgeführt, sodass diese Zertifizierung nicht erlangen können [8]. Eine solche Zertifizierung könnte ungeschulten Endnutzern auch diese quelloffenen Router-Betriebssysteme als Alternativen näherbringen und somit zu einem höheren Sicherheitsniveau in privater und SOHO Netzwerkinfrastruktur führen.

1.2 Verwandte Arbeiten

Während der Einsatz von OpenWrt im privaten und professionellen Umfeld beliebt zu sein scheint (vgl. Abschnitt 2.4) und auch einige Forschungsarbeiten mit OpenWrt verwirklicht wurden, sind derzeit keine aktuellen Arbeiten zur Sicherheit von OpenWrt verfügbar. Ortega et al. (2009) veröffentlichte eine Arbeit über eine quelloffene Methode zum Verhindern von sogenannten ARP Poisoning Attacken. Sie nutzten in diesem Kontext OpenWrt lediglich als vielseitig unterstützte Testplattform [9]. Palazzi et al. (2010) nutzten den Funktionsumfang und die Anpassbarkeit der Firmware, um einen verbesserten Datendurchsatz in Heimnetzen mit verschiedenen WLAN-Geräten zu erreichen [10]. Keine der derzeitigen Veröffentlichungen beschäftigt sich mit der Sicherheit von OpenWrt als Betriebssystem. Einzig Andrew McDonnell (2014) veröffentlichte in seinem Blog zwei Einträge über eine Sicherheitsanalyse von OpenWrt mittels des Tools checksec.sh (`https://github.com/slimm609/checksec.sh`) und entwarf eine verbesserte Version, in welcher bedeutend mehr Maßnahmen zur Verhinderung von Exploits aktiviert waren [11]. Die Ergebnisse der Veröffentlichung basierten jedoch auf Version 14.07 (Barrier Breaker) von OpenWrt, welche stark veraltet ist [12].

Die Forschung an Komponenten, die OpenWrt ausmachen, ist jedoch keinesfalls so eingeschränkt wie zuvor aufgezeigt. Der Linux Kernel, welcher einen grundlegenden Teil des OpenWrt Betriebssystems ausmacht, ist seit seiner Veröffentlichung 1991 ein andauerndes Gebiet der Forschung und Entwicklung, so auch in der IT-Sicherheit [13, 14, 15, 16]. Ebenso definiert sich OpenWrt über seine ca. 3800 zusätzlichen quelloffenen Pakete. Viele dieser Software-Erweiterungen existieren schon seit Jahrzehnten und ihre Integrität und Vertraulichkeit sind von den unzähligen Nutzern auf verschiedensten Plattformen anerkannt [17, 18, 19]. Abschließend kann man festhalten, dass es zwar durchaus Forschung an Komponenten, welche auch in OpenWrt genutzt werden, gibt, jedoch OpenWrt selbst noch nicht im Mittelpunkt der Forschung stand und die Sicherheitslage des Projektes weitestgehend ungeklärt bleibt.

1.3 Zielsetzung

Ziel dieser Arbeit war es, die Technische Richtlinie 03148 des BSI an Version 19.7.04 von OpenWrt durchzuführen und das Router-Betriebssystem auf Konformität zu prüfen. Hierbei wurde ein TP-Link Archer C7 Router genutzt. Es wurden die grundsätzlichen Sicherheitsmerkmale von OpenWrt mittels der Technischen Richtlinie evaluiert (siehe Abschnitt 3.3). Dabei wurde nur die Funktionalität des Betriebssystems geprüft, welche nach der Installation auf dem Gerät bereitgestellt wurde. Funktionen, welche vom Nutzer zusätzlich installiert und eingerichtet werden mussten, wurden nicht betrachtet. Wenn es der Testfall angeboten hat wurde ein automatischer Test entwickelt, sodass eine wiederholte Durchführung beschleunigt werden kann. Ebenso wurde die Anwendbarkeit der Technischen Richtlinie auf quelloffene Netzwerk-Betriebssysteme ermessen. Darüber hinaus wurden statische Softwaretests einiger quelloffener Router-Betriebssysteme mittels des „Firmware Analysis and Comparison Tools“ als weitere Metrik genutzt, um einen differenzierteren Einblick in die Sicherheitslage solcher Projekte zu gewähren (siehe Abschnitt 3.4). Die Ergebnisse dieser Analyse wurden darauffolgend mit den Ergebnissen des „Home Router Security Report 2020“ des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) verglichen (siehe Abschnitt 4.3). Abschließend wurde sich kritisch mit den Ergebnissen, sowie der technischen Richtlinie, auseinandergesetzt (vgl. Abschnitt 5). Die in dieser wissenschaftlichen Untersuchung genutzte Vorgehensweise kann nicht die vollständige Sicherheit aller Aspekte der Software OpenWrt nachzuweisen. 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. Die Ergebnisse der Arbeit können sowohl der Entwicklung von OpenWrt als auch Endnutzern weitere Einblicke in die Sicherheit des Projektes liefern und somit langfristig die Resilienz der Heimnetz-Infrastruktur stärken.

Kapitel 2

Grundlagen

2.1 Netzwerkrouter

Ein Netzwerkrouter (auch als Router bezeichnet) ist ein essentieller Bestandteil der meisten Computer-Netzwerke und kann auf Schicht 3 des OSI-Referenzmodelles (vgl. Abbildung 2.1) Netzwerkpakete zwischen mehreren Netzwerken weiterleiten [20, p. 48]. Eine häufige Verwendung von Routern ist die Anbindung eines privaten Netzwerkes an das Internet. Da Router auf Schicht 3 des OSI-Modells arbeiten, nutzen sie das IP-Protokoll um Netzwerkpakete weiterzuleiten [20, p. 48]. Eine wichtige Aufgabe des Routers ist unter anderem die sog. „Network Address Translation (NAT)“. Diese Technik wird eingesetzt, um den Netzwerkverkehr aller Systeme im privaten Netzwerk durch den Router in das öffentliche Netz (Internet) zu transportieren und dort an die korrekte IP-Adresse zuzustellen [21]. Im Gegensatz zu Netzwerk-Bridges (auch „Netzwerk-Switches“ genannt) sind Router flexibler, da sie mit logischen Adressen (IP-Adressen) arbeiten [22, p. 714]. Bridges hingegen arbeiten auf der Sicherungsebene (Schicht 2) des OSI-Modells. Dadurch können sie nicht verwendet werden, um ein anderes Sub-Netz zu adressieren. Daraus folgt ebenso, dass Netzwerk-Bridges nicht für die Verbindung eines privaten Netzwerks mit dem Internet geeignet sind [20, p. 48].

Neben den bereits genannten Aufgaben eines Routers liefern die meisten modernen Heimrouter zusätzliche Funktionen. So verfügen moderne Heimrouter meist auch über die Möglichkeiten einer Firewall. Durch diese können ein- und ausgehende Pakete gefiltert werden, oder Angriffe auf das Netzwerk erkannt werden [23, p. 588]. Ebenfalls bieten viele Router einen „Dynamic Host Configuration Protocol (DHCP)“-Server an. Dieses Protokoll ermöglicht die automatische Zuweisung einer Netzwerkkonfiguration an Clients [22, p. 222]. Darüber hinaus findet man häufig auch einen „Network Time Protocol (NTP)“-Server, welcher genutzt werden kann, um über den Router Zeitinformationen zu beziehen [22, p. 577]. Zusätzlich verfügen einige Heimrouter über die Möglichkeit das „Voice over IP (VoIP)“ Protokoll zu nutzen, welches Telefonie über das Internet ermöglicht [22, p. 911]. Einige Modelle unterstützen auch „Virtual Private Networks“(VPN) . Dabei handelt es sich um eine sichere Verbindung von zwei privaten Netzwerken über ein öffentliches Netzwerk,

also dem Internet. Die Daten sind auf dem Weg vollständig verschlüsselt, sodass abgefangene Pakete keinen Aufschluss über den Inhalt geben. In diesem Zusammenhang wird auch von einem „Tunnel“gesprochen, da die einzigen Zugangspunkte an den jeweiligen Enden sind [20, p. 50].

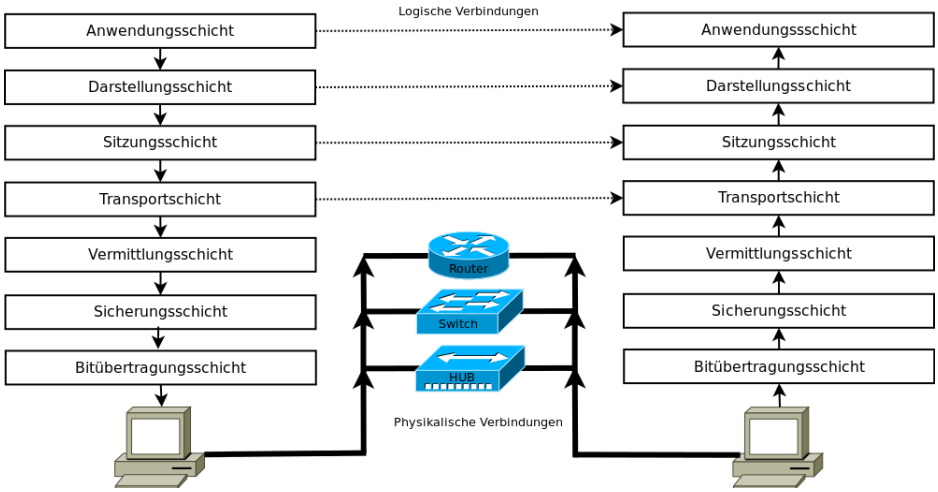


Abbildung 2.1: Abbildung des OSI-Referenzmodells [24].

2.2 Angriffe auf Netzwerkroutern

Router sind ein immer beliebteres Angriffsziel für Cyberkriminelle [25]. Der Netzwerkrouter stellt oft die direkte Schnittstelle zwischen dem Internet und einem privaten Netzwerk dar. Die Übernahme von Routern bietet Angreifern daher viele Monetarisierungsmöglichkeiten. Router bieten ein geeignetes Einfallstor in ein privates Netz, da Angreifer über einen kompromittierten Router Zugriff auf weitere Geräte des privaten Netzes erhalten können. Der Router und die ggf. weiteren infizierten Geräte können nun z.B. für die Verbreitung von Ransomware eingesetzt werden, oder selbst Opfer eines Ransomware-Angriffs sein. Bei diesem Angriff wird der Zugriff auf die Daten des Geräts von einem Angreifer verhindert, bis das Opfer den geforderten Betrag bezahlt. Ein kompromittierter Router kann auch als Teil eines Bot-Netzes eingebunden und für die Zwecke des Angreifers missbraucht werden. Darüber hinaus kann das Gerät auch genutzt werden, um den Datenverkehr des Angreifers über die IP-Adresse des Routers zu leiten, sodass die Spuren des Angreifers verwischt werden und die IP des infizierten Routers augenscheinlich illegale Aktivitäten durchführt [25].

2.2.1 Bruteforce Angriffe

Bei einem Bruteforce Angriff versucht ein Angreifer nicht eine bestimmte Software- oder Hardwarelücke auszunutzen, sondern stattdessen durch eine erschöpfende Suche des Schlüsselraumes das korrekte Passwort zu finden. Es können natürlich auch Kombinationen von Nutzername und Passwort gesucht werden, um sich auf einem Gerät anmelden zu können. Für diese Suche werden oft Passwortlisten oder Listen mit häufigen Kombinationen von Nutzername und Passwort eingesetzt. Es ist jedoch auch möglich automatisch einen voreingestellten Passwortraum, z.B. acht Zeichen mit einer Kombination aus Buchstaben und Zahlen, zu bilden und alle möglichen Kombinationen zu testen [26]. Indem der Angreifer die Antwort des angegriffenen Servers oder Systems evaluiert, kann er einen Erfolg feststellen. Aus dem Vorgehen wird ersichtlich, dass dieser Angriffsvektor unter Umständen sehr zeitintensiv ist, wenn ein sicheres Passwort gewählt wurde (vgl. Tabelle 2.1). Wie Hilt et al. (2020) zeigten, gewinnen Bruteforce Angriffe auf Router jedoch stetig an Beliebtheit. Aufgrund von einfachen oder bekannten Standardpasswörtern ist es Angreifern möglich, schnell durch einen Bruteforce-Angriff Zugriff auf einen Router zu erhalten und diesen für eigene Zwecke zu nutzen [25, p. 5].

Zeichenraum	**4 Zeichen**	**5 Zeichen**	**6 Zeichen**	**7 Zeichen**	**8 Zeichen**	**9 Zeichen**	**10 Zeichen**
26 [a-z]	<1 Sekunde	<1 Sekunde	<1 Sekunde	8 Sekunden	4 Minuten	2 Stunden	2 Tage
52 [A-Z; a-z]	<1 Sekunde	<1 Sekunde	20 Sekunden	17 Minuten	15 Stunden	33 Tage	5 Jahre
62 [A-Z; a-z; 0-9]	<1 Sekunde	<1 Sekunde	58 Sekunden	1 Stunde	3 Tage	158 Tage	27 Jahre
96 (mit Sonderzeichen)	<1 Sekunde	8 Sekunden	13 Minuten	21 Stunden	84 Tage	22 Jahre	2108 Jahre

Tabelle 2.1: Benötigte Rechenzeit zum Finden eines Passwortes durch einen Bruteforce Angriff für verschiedene Zeichenräume und Zeichenanzahl bei der Berechnung von 1 Milliarden Schlüsseln pro Sekunde.

2.2.2 Cross-Site-Request-Forgery

Neben dem Bruteforce Angriff auf den Webserver ist auch Cross-Site-Request-Forgery (CSRF) ein Angriffsvektor, welcher bei Routern zum Einsatz kommen kann [27]. Wenn keine adäquaten Schutzmaßnahmen vom Server getroffen werden, kann ein Angreifer über eine präparierte Website oder einen Phishing Link schädlichen Code auf Webseiten ausführen, auf denen der Nutzer bereits authentifiziert ist. Dieser Code versetzt den Angreifer in die Lage, Befehle auf der Webseite oder dem Webserver auszuführen, auf welchem der Nutzer angemeldet ist [28]. Es könnte zum Beispiel ein neuer Benutzeraccount durch den Angreifer angelegt werden oder Einstellungen und Sicherheitsparameter an den Angreifer gesendet werden (siehe Abbildung 2.2). So könnte ein Angreifer eine gültige Session eines Nutzers übernehmen, wenn dieser beim Webserver seines Routers angemeldet ist. Von dort könnte er Zugangsdaten entwenden und verändern oder einen persistenten Einstiegspunkt in das Netzwerk ermöglichen. Ebenso könnte ein präpariertes Firmware-Abbild aufgespielt

werden. Es ist auch ein zweistufiges Verfahren bekannt, bei dem der Nutzer zunächst durch den Angreifer an seinem Gerät angemeldet wird, da das Opfer meist nicht an seinem Gerät angemeldet ist. Danach verläuft der CSRF-Angriff wie beschrieben. Dieses zweistufige Vorgehen ist möglich, da viele Endnutzer das Passwort ihres Gerätes nicht ändern und die voreingestellten Passwörter oft nach einem bekannten Muster generiert werden [27].

Eine häufig verwendete Sicherheitsmaßnahme gegen CSRF Angriffe ist ein Anti-CSRF Cookie (auch Token genannt). Dieser wird im „HTTP-request-header“, im „http-POST-body“ oder als verstecktes Feld in einem „HTTP-FORM-Objekt“ deklariert und besteht aus zwei zufällig generierten Zeichenketten, sodass der Nutzer und der Server jeweils einen Cookie gespeichert haben. Der Cookie des Nutzers wird für jede http-Methode benötigt, welche nach dem Setzen des Cookies aufgerufen wird. Dazu wird neben dem normalen Session Cookie auch geprüft, ob der korrekte Anti-CSRF Cookie übermittelt wurde. Dies geschieht auf Seiten des Servers mittels des zweiten Teils des CSRF-Tokens [29]. Wenn der Angreifer diesen Wert nicht berechnen kann, so kann er keine erfolgreiche domänenübergreifende Anfrage stellen. Um ein höheres Sicherheitsniveau zu erreichen sollte der CSRF-Cookie an die Session des Nutzers gebunden sein [27].

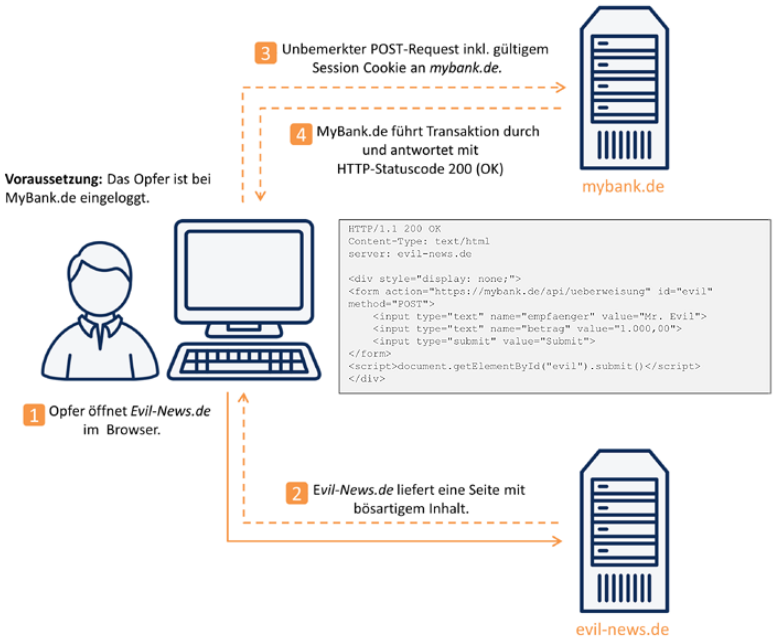


Abbildung 2.2: Ein möglicher Ablauf eines Cross-Site-Request-Forgery Angriffs. Der Nutzer ist bei MyBank.de angemeldet und öffnet Evil-News.de. Diese Seite liefert Schadcode an den Browser des Opfers aus. Der Code tätigt eine Überweisung mittels eines POST Requests und dem gültigen Cookie des Nutzers. Da es keine Abwehrmaßnahmen gibt tätigt der Bankserver die Überweisung an den Angreifer [30].

2.2.3 DNS Rebinding Attacke

Bei dieser Art von Angriff wird die vom Browser durchgesetzte „Same Origin Policy“ umgangen, um arbiträre Anfragen an das lokale Netzwerk des Opfers zu stellen. Abbildung 2.3 zeigt, wie die Herkunft („Origin“) eines Web Dokumentes definiert ist.

Abbildung 2.3: Origin (dt. Herkunft) eines Web-Dokumentes [31]

Zwei Dokumente haben also die gleiche Herkunft („same origin“), wenn sie identische „scheme“, „host“ und „port“ Komponenten haben. Die „Same Origin Policy“ setzt durch, dass Skripte, oder auch Cascading Style Sheets (CSS), nur auf Daten von anderen Webseiten zugreifen können, wenn diese sich dieselbe Herkunft teilen. Wenn diese Richtlinie nicht implementiert wäre, dann wäre eine bösartige Webseite zum Beispiel in der Lage auf ein Bankkonto zuzugreifen, auf dem ein Opfer ebenfalls eingeloggt ist. Dort könnten Daten wie die Transaktionshistorie ausgelesen oder weitere Aktionen ausgeführt werden.

Bei einem DNS Rebinding Angriff ruft das Opfer zunächst eine kompromittierte, oder bösartige, Website auf. Für diesen Aufruf wird ein DNS-Server beauftragt mit der IP-Adresse des angefragten Web-Servers zu antworten. Der vom Angreifer kontrollierte DNS-Server antwortet mit einem DNS A Record, welcher auf die Angreifer-Webseite verweist und den Browser des Opfers anweist, die DNS-Daten nur für eine geringe Zeit im Cache zu behalten. Ein Skript, welches auf der Webseite des Angreifers platziert wurde, wartet nun darauf, dass die DNS-Daten aus dem Cache verfallen, sodass der Browser eine neue Anfrage stellen muss. Diesmal antwortet der DNS-Server allerdings nicht mit der eigenen IP-Adresse, sondern mit einer IP-Adresse im lokalen Netzwerk des Opfers. Nun kann das Skript Anfragen an diesen lokalen Dienst stellen, z.B. Daten exfiltrieren oder weitere Angriffe starten (siehe Abbildung 2.4).

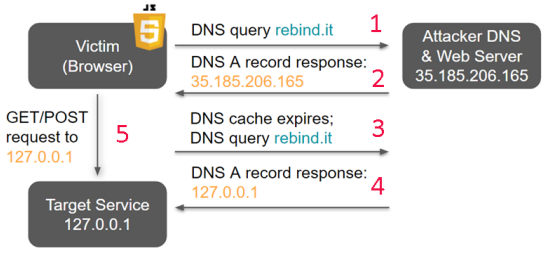


Abbildung 2.4: Ablauf eines DNS Rebinding Angriffs mittels des des Webtools der NCC Group (`http://rebind.it:8080/manager.html` [31]

2.2.4 Denial of Service Angriff

Bei einem „Denial of Service (DoS)“ Angriff generiert ein Angreifer unzählige Anfragen oder eine sehr große Menge Daten auf einem anderen System, um die Netzwerk- oder Rechenkapazitäten des Opfers auszuschöpfen. Während eines solchen Angriffes wird der Zugriff auf die Webseite, den Dienst oder den Rechner für legitime Nutzer verhindert [32] [22, p. 217]. Es handelt sich also um einen Angriff auf das Schutzziel der Verfügbarkeit.

> “More simply, a DoS attack is when an attacker uses a single machine’s resources to exhaust those of another machine, in order to prevent it from functioning normally [32].“

Es handelt sich also bei DoS um ein System, welches ein anderes oder mehrere andere Systeme angreift. Diese Art von Angriff kann entweder durch eine Sicherheitslücke in einem gegebenen System ausgeführt werden, oder über eine Überlastung des Netzwerkes mit Anfragen. Daher teilt man DoS-Attacken meist in drei Kategorien ein [33]:

- Bandbreitensättigung
- Ressourcensättigung
- Herbeiführung von System- und Anwendungsabstürzen

Bandbreitensättigung beschreibt das Vorgehen einen Webdienst oder Webserver mit einer großen Menge an Anfragen zu belasten, sodass legitime Nutzer den Dienst nicht, oder nur sehr langsam, nutzen können. Ressourcensättigung ist das Äquivalent für ein gesamtes Rechnersystem. Hier wird eine Sicherheitslücke oder ein Programmierfehler genutzt, um durch einen Prozess eine sehr hohe Auslastung des Systems zu erzeugen, sodass dieses nicht mehr reagiert. Die letzte Art beschreibt das Herbeiführen von Abstürzen. Auf diese Weise kann der Zugriff auf ein Webdienst oder System vollständig unterbrochen werden. Darüber hinaus ist es so möglich, gezielt Elemente eines Netzwerkes wie eine Firewall auszuschalten, sodass ein weiterführender Angriff möglich ist [1].

Die meisten Webserver können jedoch Überlastungsversuchen von einem einzelnen System widerstehen. Daher nutzen Angreifer meist mehrere Systeme, welche ein Ziel überlasten sollen. Dies bezeichnet man als „Distributed Denial of Service“(DDoS) Angriff [22, p. 210]. Für diesen Zweck werden in den meisten Fällen viele Systeme unter ein Kommando gestellt, sodass der Angriff koordiniert ablaufen kann. Dies wird als „Botnetz“ bezeichnet. Den Teilnehmern eines solchen Botnetzes ist oft gar nicht bekannt, dass ihre Geräte durch speziell präparierte Malware infiziert und zu einem Botnetz hinzugefügt wurden [25]. Der Einsatz von infizierten IoT-Geräten wird ebenfalls immer beliebter, da diese oft sehr schlecht abgesichert sind und die Nutzer zumeist das Standardpasswort nicht ändern [34].

Mögliche Motive für DoS und DDoS sind finanzielle Ziele, politische Motivation („Hacktivismus“), zielgerichtete Angriffe auf kritische IT-Infrastruktur oder vertrauliche Daten („Advanced Persistent Threats“) sowie Cyberkrieg [32, p. 12] [1]. DoS und DDoS Angriffe auf Router sind durch die Schnittstellenfunktion des Routers relativ einfach möglich. Die Abwehr solcher Attacken auf Router ist jedoch in den meisten Fällen durch Software und einige Firewall-Regeln automatisch möglich. So kann z.B. die erlaubte Datenrate dynamisch vom Router eingestellt werden, wenn bestimmte Muster in den Anfragen erkannt werden, welche auf einen (D)DoS Angriff hindeuten [33].

2.3 Was ist OpenWrt?

OpenWrt (Open Wireless RouTer) ist ein quelloffenes Netzwerk-Betriebssystem für Router, welches auf GNU/Linux basiert und durch eine GNU General Public License (GPL) lizensiert ist [4]. Die Installation umfasst einen Bootloader, einen Linux-Kernel, ein eigenes Dateisystem und ausgewählte Anwendungen. Es kann auf Routern, Switches und Wireless Access Points eingesetzt werden, um die vorinstallierte Firmware vollständig zu ersetzen [35]. Es bietet neben standardmäßiger Router-Funktionalität einen eigenen Paketmanager, über welchen ca. 3800 (Stand 01.11.20) weitere Pakete installiert werden können [36]. Dies bietet viele weitere Einsatzmöglichkeiten und Funktionen, welche vom Hersteller nicht oder unzureichend unterstützt werden. Ebenfalls beinhaltet die Installation von OpenWrt den SSH-Dienst BusyBox und das Web-Interface LuCI, sodass dem Nutzer über den root-Benutzeraccount vollständiger Zugriff auf das Gerät gewährt wird. Nach derzeitigem Stand werden über 1700 Geräte von ca. 270 Herstellern von OpenWrt unterstützt [37]. Diese Anzahl Geräte kann unter anderem deshalb unterstützt werden, da OpenWrt nur minimale Ressourcen auf dem Endgerät benötigt. Nach eigenen Angaben kann die derzeitige Version auf Geräten installiert werden, welche 4MB Flash Speicher und 32MB RAM besitzen. Ab der nächsten „Major Release“ Version (20.XX) werden 8MB Flash und 64MB RAM vorausgesetzt [37]. Diese Voraussetzungen sind jedoch bei den meisten Geräten der letzten Jahre gegeben. OpenWrt zeichnet sich ebenfalls dadurch aus, dass es sich nicht nur um eine statische Firmware handelt, sondern ebenfalls um ein komplettes Framework zur Entwicklung und Erstellung von angepassten Firmware Versionen. OpenWrt zeichnet sich auch dadurch aus, dass Geräte solange unterstützt werden, wie sie die minimalen Systemanforderungen erfüllen. Dies steht im Gegensatz zu den meisten proprietären Betriebssystemen, welche nur einige Jahre Funktions- und Sicherheitsupdates erhalten und nach ihrem sog. „End of Life“ (EOL) nicht mehr sicher betrieben werden können und ausgetauscht werden müssen. Auch wenn in der Entwicklungsgeschichte von OpenWrt viel für die Benutzerfreundlichkeit des Betriebssystems getan wurde, ist es nicht unbedingt für Laien geeignet. Trotz des

Managements über die Weboberfläche erweist sich die Einrichtung ohne Grundkenntnisse als anspruchsvoll.

Die Entwicklung von OpenWrt begann 2004, nachdem der amerikanische Hersteller Linksys zuvor einen Router auf den Markt brachte, dessen Firmware zu Teilen ebenfalls unter der GPL Lizenz stand und somit öffentlich verfügbar sein musste. Die erste Veröffentlichung von OpenWrt erfolgte im Januar 2006 mit Version 0.9 (White Russian). Seitdem wurde das Projekt stetig weiterentwickelt (siehe Abbildung 2.5). 2016 spaltete sich eine Gruppe Mitwirkender aufgrund interner Diskrepanzen ab und gründete das LEDE Projekt. Jedoch wurde LEDE bereits 2018 wieder in OpenWrt integriert, sodass beide Projekte nun wieder zusammen unter einem Namen entwickelt werden. Die derzeit aktuelle Version ist 19.07.5, welche am 09.12.2020 veröffentlicht wurde (vergleiche Anhang B.1) [12].

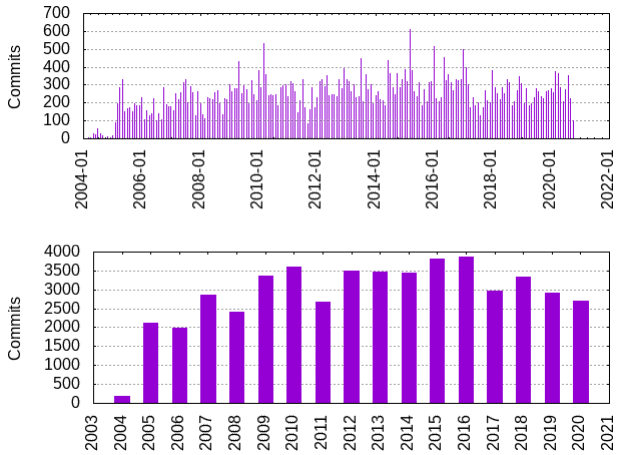


Abbildung 2.5: Die git Commits pro Monat (oben) und pro Jahr von 2004 bis 2020 (unten) des OpenWrt git Repositories. Seit 2005 werden jedes Jahr mindestens 2000 Commits gemacht. Die Grafik wurde mit dem Programm GitStats erstellt (http://gitstats.sourceforge.net).

2.4 Relevanz und Verwendung von OpenWrt

Die Webseite des OpenWrt Projektes verzeichnete im Jahre 2020 bis einschließlich November 1.261.500 Besucher, sowie 52,4 Millionen Seitenaufrufe. Insgesamt wurden bis November 2020 bereits 16,44TB Daten abgerufen [38]. Die zum Zeitpunkt des Seitenaufrufes aktuelle Version von OpenWrt (19.07.4) wurde dabei allein im November 1981 Mal heruntergeladen. Ebenfalls wurde Version 18.06.8 noch 935 Mal angefragt. Zusammen wurden ca. 10000 Firmware-Abbilder im November 2020 heruntergeladen [38]. Wie die Daten zeigen ist OpenWrt keinesfalls ein kleines Projekt mit nur wenigen Interessierten, sondern

eine nachgefragte Alternative für Heimrouter, Unternehmen und Entwickler. Es lässt sich nur schwer abschätzen wie die Verteilung zwischen dem privaten und wirtschaftlichen Einsatz der Firmware genau ist, jedoch ist eine mehrheitliche Nutzung im privaten Umfeld zu vermuten, da die Downloadzahlen eine Tendenz zu Geräten mit einer günstigeren MIPS-Architektur, anstelle von professionellen Geräten, zeigen (siehe Abbildung 2.7). OpenWrt ist dennoch nicht nur für Heimrouter relevant, sondern zeichnet sich auch in seinem Nutzen für Unternehmen und Entwickler aus. Es bietet Unternehmen die Möglichkeit ein Netz zu betreiben, welches sie vollständig mit quelloffener Software realisieren und steuern können. Ebenfalls bietet es Dienstleistungsunternehmen einen Weg, hochgradig maßgeschneiderte Netzstrukturen für ihre Kunden zu entwerfen, welche quelloffen und leicht anpassbar sind. So können neue oder geänderten Funktionen über ein Paket bereitgestellt und verteilt werden.

Month	Unique visitors	Number of visits	Pages	Hits	Bandwidth
Jan 2020	132,873	197,956	1,127,395	4,665,469	1.67 TB
Feb 2020	110,371	163,646	1,002,759	4,104,171	1.61 TB
Mar 2020	122,633	183,308	1,002,048	5,175,434	1.66 TB
Apr 2020	129,317	189,456	988,607	4,377,669	1.68 TB
May 2020	118,101	173,179	925,788	5,681,240	1.84 TB
Jun 2020	134,365	184,142	790,987	3,189,593	1.17 TB
Jul 2020	97,788	140,153	712,274	7,458,245	1.59 TB
Aug 2020	100,393	143,850	661,420	3,240,342	1.39 TB
Sep 2020	101,636	145,296	767,185	3,216,887	1.21 TB
Oct 2020	124,108	177,852	790,254	3,692,070	1.35 TB
Nov 2020	89,915	127,187	655,436	7,628,492	1.28 TB
Dec 2020	0	0	0	0	0
Total	1,261,500	1,826,025	9,424,153	52,429,612	16.44 TB

Abbildung 2.6: Übersicht über verschiedene Statistiken der OpenWrt Webseite für das Jahr 2020. (Erstellt: 30.11.2020)

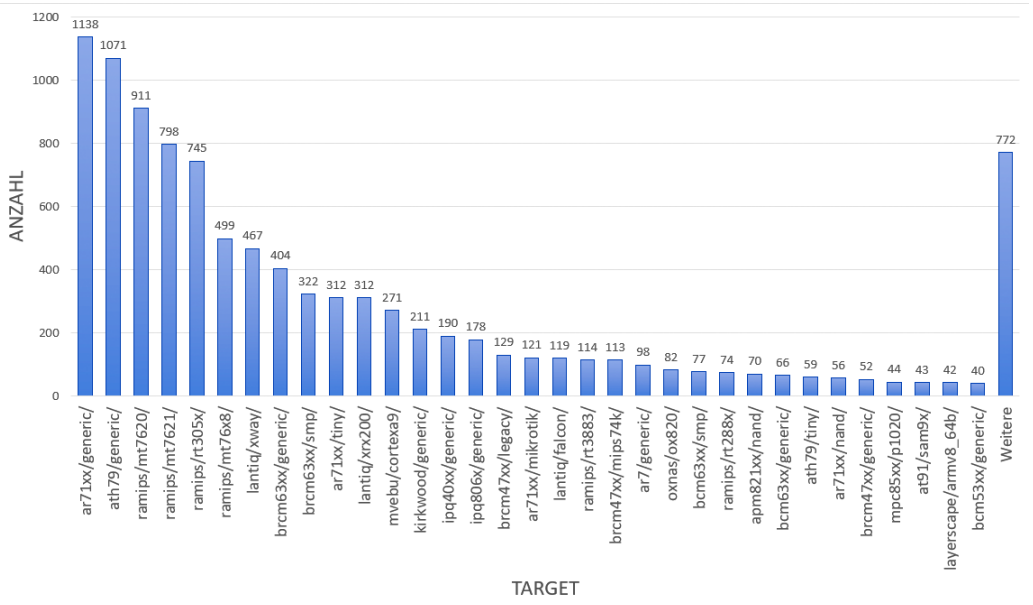


Abbildung 2.7: Anzahl der heruntergeladenen Firmware pro Target im November 2020. Es zeichnet sich ein deutlicher Trend zu günstigeren MIPS-Geräten ab.

2.5 Möglichkeiten zur Evaluation von Router Firmware

2.5.1 Beschreibung der Technischen Richtlinie 03148 - Sichere Breitband Router

Bei der Technischen Richtlinie „Sichere Breitband Router“ (BSI TR-03148) des Bundesamtes für Sicherheit in der Informationstechnik handelt es sich um eine Sammlung von grundlegenden Sicherheitsanforderungen für Breitband Router [8, p. 3]. Der Schwerpunkt der Richtlinie liegt hierbei vor allem auf Heimroutern, sowie auf Geräten, welche im SOHO Umfeld eingesetzt werden. Das Dokument wird durch die Dokumente „BSI TR-03148 Implementation Conformance Statement (ICS)“ sowie „BSI-TR-03148-P ICS and Test Documentation” ergänzt. In diesen Dokumenten sind Testfälle und Dokumentation zur Durchführung einer Prüfung festgehalten. Die Test Spezifikation der Technische Richtlinie definiert 101 „Test Requirements", welche insgesamt 164 „Test Procedures" beschreiben. Die „Test Requirements“ sind dabei in logische Module unterteilt. Ein „Test Requirement“ wird als fehlgeschlagen gewertet, wenn ein zugehöriges „Test Procedure“ nicht bestanden wird. Nach Angaben des BSI richtet sich die Technische Richtlinie vor allem an Hersteller von Routern, sie kann jedoch auch für Endnutzer relevant sein, wenn diese einen neuen Router anschaffen möchten und sich daher über den Stand der Technik informieren wollen [39]. Es werden Anforderungen für ein Mindestmaß an verpflichtenden und einigen optionalen IT-Sicherheitsmaßnahmen definiert, um ein grundlegendes Niveau für die Sicherheit dieser Geräte zu schaffen [8, p. 11]. Die angestrebte Zertifizierung von Geräten würde ebenso die Sicherheit der Geräte für den Verbraucher transparenter machen.

Das Dokument entstand aus einer Zusammenarbeit des BSIs mit verschiedenen Herstellern von Routern, Telekommunikationsanbietern, Behörden, dem Innen- und Wirtschaftsministerium, sowie unter anderem mit Vertretern des OpenWrt Projektes und des Chaos Computer Clubs (CCC) [40]. Diese trugen ihre Ideen und Vorstellungen zur Sicherheit von Routern zusammen und suchten Lösungen für Interessenkonflikte. Nach Veröffentlichung der Richtlinie im Jahre 2018 wurde diese allerdings unter anderem von Vertretern des OpenWrt Projektes sowie vom CCC kritisiert. Nach Meinung dieser Interessengruppe sind die definierten Maßnahmen in der Technischen Richtlinie nicht ausreichend, um tatsächliche Angriffe auf Router zu verhindern [41].

Der Aufbau der Technischen Richtlinie, des „Conformance Statements“ und der Test Spezifikation ist für das Verständnis der Arbeit unabdingbar. Die Technische Richtlinie selbst beginnt mit einer Beschreibung für welche Geräte die TR genutzt werden soll. Darauf folgt eine Beschreibung des Rahmens, welcher durch die TR vorgegeben wird. So wird festgelegt, dass Router mit einem Betriebssystem betrachtet werden sollen, welche die Schnittstelle zum Internet darstellen und dem Nutzer das Management seines eigenen privaten Netzes ermöglichen. Weiterführend wird festgelegt, dass die Sicherheit von zusätzlichen

angeschlossenen Geräten und nicht essenziellen zusätzlichen Funktionsmerkmalen nicht betrachtet wird. Anschließend werden drei Zustände definiert, in dem sich ein Gerät während des Testens befinden kann: „factory settings“, „initialized (after initialization)“ und „(end user) customized“ (vgl. Abschnitt 3.3.2). Bevor die einzelnen logischen Themenmodule der TR erläutert werden, wird zunächst das Bedrohungsmodell definiert (siehe Grafik 2.8). Hierzu werden zwei verschiedene Angreifer festgelegt. Angreifer A greift den Router über das Internet, also die „Wide Area Network“ (WAN) Schnittstelle des Routers an, während Angreifer B einen Angriff über das „Local Area Network“ (LAN) und „Wireless-Lan“ (WLAN) Interface versucht. An dieser Stelle wird auch ein erweiterter kombinierter Angriff betrachtet. Darauffolgend werden die Module der Technischen Richtlinie beschrieben, welche die Anforderungen in logische Einheiten bündeln. Es werden die folgenden Module beschrieben:

Module A	-	Private Network (privates Netzwerk)
Module B	-	Public Network (öffentliches Netzwerk)
Module C	-	Functionalities (Funktionen)
Module D	-	Configuration and Information (Konfiguration und Informationen)
Module E	-	Firmware Updates
Module F	-	Firewall
Module G	-	Domain Name System (DNS)
Module H	-	Dynamic Host Configuration Protocol (DHCP)
Module I	-	Factory Reset (Zurücksetzen des Gerätes)
Module J	-	Internet Protocol version 6 (IPv6)
Module K	-	Remote Configuration (Fernwartung)
Module L	-	Voice over IP (VoIP)
Module M	-	Virtual Private Network (VPN)

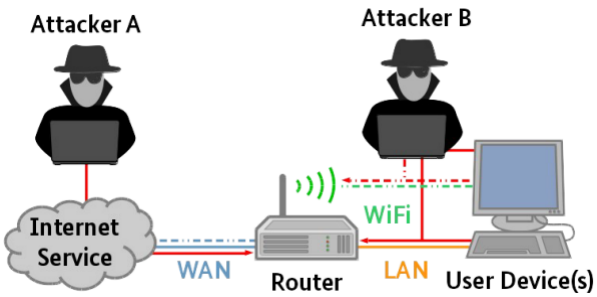


Abbildung 2.8: Das von der Technischen Richtlinie betrachtete Bedrohungsmodell [39]

Bevor die eigentlichen Tests, welche in der TR beschrieben sind, durchgeführt werden können, muss zunächst ein sogenanntes „Implementation Conformance Statement“ ausgefüllt werden. In diesem werden maßgebende Informationen über das zu testende Gerät festgehalten. Bei einer Durchführung der Technischen Richtlinie im Kontext einer Zertifizierung würde dieses „Conformance Statement“ zunächst vom Hersteller bzw. Auftraggeber ausgefüllt und eingereicht. Die angegebenen Informationen unterstützen den Tester, sind

aber auch selbst Teil der Testprozedur. Zu diesen Informationen gehören neben dem Namen und der betrachteten Software-Version auch eine Übersicht über die zur Verfügung stehende Dokumentation des Gerätes. Hierzu wird auch technische Dokumentation gezählt, welche normalerweise nicht für Endnutzer und Verbraucher zur Verfügung steht. Des Weiteren werden Informationen zu allen Modulen zusammengetragen, welche bei der Durchführung der „Test Procedures“ von Relevanz sind.

Der Aufbau der Test Spezifikation orientiert sich ebenfalls an den einzelnen Modulen. Nach einer Einleitung wird zunächst das „Device Under Testing“(DUT) beschrieben sowie Ansprüche an die Fähigkeiten und die Ausstattung des Testers. Darauf steht erneut das komplette „Conformance Statement“ zur Verfügung. Im Anschluss darauf werden die Testfälle, sowie die Kriterien zum Bestehen der Testfälle definiert. Die Ergebnisse können in der Test Dokumentation, welche als Tabellenkalkulationsdatei ausgefüllt wurde, dokumentiert werden. Die Testdokumentation definiert die folgenden Kategorien: Eine durchlaufende Nummerierung und eine Angabe, ob es ein „muss“ oder „soll“ Kriterium ist, eine Beschreibung des Testfalls und die Angabe des Testers, ob der Testfall anwendbar ist oder nicht. Ebenso steht „N/A“ (not applicable) als Option zur Verfügung. Darauf folgen Felder für die jeweiligen Ergebnisse der Tests einer jeden Testreihe, gefolgt von der Möglichkeit für Notizen, Referenzen, benutze Tools, Zugriffsmethoden und einer Referenz für weitere Daten wie Bilder (siehe Tabelle 2.2).

TR	**MUST or SHOULD**	**Description of TR**	**Applicability of Test Requirements**											
			Yes	No	N/A	1. TP	2. TP	3. TP	4. TP	5. TP	Notes	Used Tools	Used Configuration Access Method	Test data reference
Module A - Private Network														
TR.A.1	MUST	...	X			Pass	Fail	Inc.	N/A			nmap	web-interface	1.png
. . .														
Module B - Public Network														
. . .														
Module C - Functionalities														
. . .														

Tabelle 2.2: Aufbau der Test Dokumentation als Tabellenkalkulationsdatei.

2.5.2 Statische Softwaretests

Bei einem statischen Softwaretest wird die Software nicht während der Laufzeit (vgl. dynamischer Softwaretest) getestet, sondern der eigentliche Quellcode oder der dekompilierte Bytecode analysiert. Statische Softwaretests gehören also zur Gruppe der sog. „non-execution-based“-Methoden. Dynamische Softwaretests bezeichnet man hingegen als „execution-based“, da die Software ausgeführt werden muss. Zu den statischen Softwaretests gehören unter anderem das Software-Review oder auch werkzeuggestütze automatische Verfahren. Wie die meisten Softwaretestverfahren gehören statische Softwaretests zu den falsifizierenden Verfahren und können somit lediglich die Anwesenheit von Fehlern bestimmen [42, 43].

Bei einem Software-Review wird der Quellcode, die Dokumentation oder jedes weitere Dokument eines Softwareentwicklungsprozesses von einem oder mehreren Prüfern inspiziert und ausgewertet. Dabei sollte nach einen festgelegten Plan vorgegangen werden. Darüber hinaus müssen auch psychologische Effekte in Betracht gezogen werden, sodass der Entwickler des geprüften Dokumentes sich nicht persönlich kritisiert sieht [42].

Werkzeuggestützte statische Softwaretests kommen in vielen Formen vor. So führen die meisten integrierten Entwicklungsumgebungen (IDE) und Compiler bereits eine statische Analyse durch. Sie zeigen z.B. Abweichungen von voreingestellten Code-Stilen an, sodass ein Entwickler darin unterstützt wird, einheitlichen und strukturierten Code zu schreiben. Ebenso werden sog. „Code Smells“ in einigen IDEs angezeigt. Es handelt sich hierbei um ein Code-Konstrukt oder Code-Abschnitt, welcher es nahelegt, diesen zu refaktorisieren. Dazu gehören zum Beispiel Duplikate im Quellcode oder zu lange und komplexe Methoden. Viele moderne IDEs zeigen noch viele Metriken zur Verbesserung des Quellcodes an [42, 44]. Es existieren jedoch auch Programme, mit denen gezielt eine statische Analyse durchgeführt werden kann. Ein Beispiel hierfür ist das Programm „Lint“. Es ist eines der ersten Programme für statische Softwaretests und prüfte kritische Stellen, wie nicht initialisierte Variablen, da dies von frühen Compilern nicht unterstützt wurde [45]. Ein weiteres bekanntes Beispiel ist das „Rough Auditing Tool for Security“(RATS) Programm. Es unterstützt mehrere Programmiersprachen und prüft viele verschiedene Fehler [46]. Jedoch müssen die Ergebnisse dieser Programme aufgrund einer erhöhten Falsch-Positiven-Rate von einem Menschen kontrolliert werden.

Firmware Analysis and Comparison Tool

Das „Firmware Analysis and Comparison Tool“ (FACT) ist ein quelloffenes Programm zur statischen Analyse von Firmware, welches vom Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie entwickelt wurde. Es ist in der Lage arbiträre Firmware (Router, Webcams, UEFI, etc.) zu entpacken und mehrere Analysen durchzuführen.

Nachdem mehrere Firmware-Abbilder extrahiert und analysiert wurden, kann FACT ebenfalls genutzt werden, um diese miteinander zu vergleichen. Eine Benutzeroberfläche wird dabei durch ein Web-Interface bereitgestellt, während die eigentliche Funktionalität über Plug-Ins organisiert ist, sodass eigens entwickelte Komponenten einfach hinzugefügt werden können. FACT automatisiert somit den normalerweise aufwendigen Prozess der Firmware-Analyse [47]. In der Standardinstallation stellt FACT die folgenden Plug-Ins für die Analyse zur Verfügung:

- Identifikation der Software
  - Betriebssystem erkennen
  - Welche Programme sind installiert?
  - Welche Programmversionen kommen zum Einsatz?
  - Welche Routinen werden beim Systemstart gestartet?
  - Können bekannte Schwachstellen gefunden werden?
- Benutzerkonten finden. Vor allem hartkodierte Passwörter
- Kryptographisches Material identifizieren
  - Private Schlüssel
  - Zertifikate
- CPU-Architektur bestimmen (Für Emulation und Disassembler)
- QEMU Unterstützung evaluieren (Für Debugging und Fuzzing)
- Bekannte Fehler in der Implementierung
- Exploit Mitigationen auswerten
- zusätzliche Plug-Ins

Härtungsmaßnahmen

FACT ist in der Lage einige bekannte Härtungsmaßnahmen (auch als Exploit Mitigationen bezeichnet) für elf-Binärdateien in einem Firmware-Abbild zu analysieren. So kann angezeigt werden welche Binärdateien mit diesen Maßnahmen erzeugt wurden und welche nicht. Diese Härtungsmaßnahmen sind vor allem Wege zur Mitigation von Speicherkorruption, entweder durch einen Angreifer oder durch Systemfehler. FACT kann folgende Mitigationen auswerten:

- **Stack Canary**: Es handelt sich hierbei um eine zufällig gewählte Byte-Sequenz, welche vor die „return“-Adresse auf den Stack geschrieben wird, um Overflows zu erkennen. Diese zufällige Sequenz wird aus einer statisch adressierbaren Speicherregion außerhalb des Stacks geholt [48]. Wenn es zu einem Buffer-Overflow kommt, würde diese

Sequenz überschrieben und diese kann somit nicht vor dem Zurückkehren (return) verifiziert werden, sodass der Overflow erfolgreich erkannt wird [49]. Wenn die Werte nicht übereinstimmen, dann wird eine Kernel-Panik ausgelöst und der Prozess terminiert.

- **FORTIFY_SOURCE** ist eine zusätzliche Option der GCC Compiler Collection. Wenn diese Option beim Kompiliervorgang von Dateien ausgewählt wird, werden verschiedene Funktionen zur Manipulation von Zeichenketten und Speicher (memcpy, memset, strcpy, strcat, sprintf, gets, ...) während der Ausführung auf Pufferüberläufe (buffer overflow) geprüft. Dies schützt meistens nicht vor gezieltem Ausnutzen dieser Funktionen aber vor der Korruption des Heaps und Stacks durch Systemfehler [50].

- **Non-Executable Bit (NX)**: Dieses besondere Bit markiert Bereiche des Speichers als reine Datenspeicherbereiche. Dadurch wird sichergestellt, dass in diesen Bereichen, in denen kein Code ausgeführt werden sollte, auch kein Code ausgeführt werden kann. Diese Separierung findet sich sonst nur in Harvard-Architekturen [51, p. 11].

- **Position-Independent Executable (PIE)** (positionsunabhängiges ausführbares Programm) bezeichnet eine Technik, bei welcher Programm-Code an einer zufälligen Speicheradresse geladen wird. Hierbei wird nicht mit absoluten, sondern relativen Speicheradressen gearbeitet. Dies erschwert zwar Angriffe, da ein Angreifer zunächst die absolute Speicheradresse finden muss, jedoch verlangsamt diese Technik unter Umständen auch die Ausführung des Codes [52].

- **RELocation Read-Only (RELRO)** schützt den “Global Offset Table” (GOT) gegen Manipulationen während der Laufzeit. Der Global Offset Table beinhaltet die Speicheradressen von gemeinsam genutzten Softwarebibliotheken oder globalen Variablen, sodass diese von einem Programm genutzt werden können. Wenn die RELRO Option beim Kompiliervorgang ausgewählt wurde, dann wird nach dem Start des Programms ein reiner Lesezugriff auf den GOT festgelegt [51, p. 12].

Common Vulnerabilities and Exposures

Das „Common Vulnerabilities and Exposures“(CVE) System wurde 1999 geschaffen, um ein weltweit einheitliches System zur Beschreibung von Firmware oder Software Schwachstellen zu etablieren [53]. Sogenannte „CVE Numbering Authorities“(CNAs) vergeben pro Sicherheitslücke eine spezifische Identifikationsnummer. Nachdem eine Beschreibung und Referenzen formuliert wurden, wird der Eintrag in die CVE-Datenbank aufgenommen und kann weltweit eingesehen werden. Durch das festgelegte Format von CVE-Einträgen ist auch

die automatische Verarbeitung von Einträgen möglich. Dies kann für die automatische Notifikation eines Betroffenen genutzt werden, wenn eine sicherheitsrelevante Schwachstelle gemeldet wird. Das CVE Projekt wird von dem US-Amerikanischen Unternehmen „MITRE“ unterhalten [54].

Da CVE-Einträge keinen Aufschluss über die schwere der Sicherheitslücke geben, wurde 2005 vom „Forum of Incident Response and Security Teams“(FIRST) ein Bewertungssystem für CVE-Einträge entwickelt. Dieses als „Common Vulnerability Scoring System“(CVSS) bezeichnete System ist heute der Industriestandard [54]. Das CVSS-Bewertungssystem ermöglicht es, die Erarbeitung von Lösungen für Sicherheitslücken zu priorisieren. Jeder CVE-Eintrag erhält durch eine Reihe von Metriken, welche den Anspruch und die Auswirkung einer gegebenen Sicherheitslücke in Betracht ziehen, eine CVSS Bewertung zwischen null und zehn. Eine Bewertung von zehn ist dabei die schwerwiegendste Stufe [55]. 2007 wurde die zweite Version, CVSS2 (auch CVSS v2), veröffentlicht und 2015 wurde CVSS3 (CVSS v3) herausgegeben [55, 56]. Die neuste Version beinhaltet überarbeitete Metriken sowie ein neues Einstufungssystem mit zwei neuen Stufen (vgl. Tabelle 2.3). Die Bewertungen sind nicht mit einander vergleichbar [56]. Da vor allem ältere Sicherheitslücken keine CVSS3 Bewertung haben, wird im weiteren Verlauf dieser Arbeit das CVSS2 System verwendet.

Rating	CVSS2 Score	CVSS3 Score
None	-	0.0
Low	0.0 - 3.9	0.1 - 3.9
Medium	4.0 - 6.9	4.0 - 6.9
High	7.0 - 10.0	7.0 - 8.9
Critical	-	9.0 - 10.0

Tabelle 2.3: Unterschiede in der Bewertungsskala von CVSS2 und CVSS3 [55, 56]

Kapitel 3

Methodik

3.1 Übersicht und Begründung der verwendeten Methodik

Die Methodik der Arbeit ist in großen Teilen durch die Technische Richtlinie vorgegeben. Die Testfälle wurden aufgrund ihrer Gruppierung in thematische Module in chronologischer Reihenfolge erarbeitet (siehe Abschnitt 2.5.1). Einzig solche Testfälle, welche spezifizierten, dass sie erst zum Ende der Testphase durchgeführt werden sollten, wurden nach hinten gestellt. Da es in erster Linie um die Technische Richtlinie 03148 gehen sollte, wurden weitere Tests, wie ein statischer Test mit dem „Firmware Analysis and Comparison Tool“ (siehe Abschnitt 2.5.2), erst nach Vollendung der Technischen Richtlinie begonnen [47].

Die Testfälle der Technischen Richtlinie wurden, soweit möglich, mit den Programmen durchgeführt, welche in der TR selbst spezifiziert wurden. Die Ergebnisse einer Literaturrecherche zeigten, dass die aufgeführte Software für die Überprüfung der Testanforderungen geeignet ist und die Ergebnisse dieser Programme seit vielen Jahren weitestgehend als korrekt akzeptiert sind. Hierzu zählt vor allem das Programm nmap, welches aufgrund von verschiedenen Testrechnern in den Versionen 7.80, 7.90 und 7.91 verwendet wurde [57]. Die Änderungshistorie von nmap gibt allerdings keinen Anlass zur Annahme, dass dies die Ergebnisse invalidiert [58]. Ebenso wurde airmon-ng / airodump-ng in der Version 1.6 zum Prüfen verwendet. Dieses Softwarepaket ist ebenfalls seit vielen Jahren angesehen und findet in wissenschaftlichen Arbeiten Verwendung [59, 60]. Zur Aufzeichnung von Netzwerkpaketen wurde Wireshark 3.4.2 verwendet, welches neben der Kommandozeilenanwendung tcpdump häufig Verwendung findet [61, 62]. Im Rahmen der Tests wurde des Weiteren auf einige zweckspezifische Skripte in den Programmiersprachen Python und Bash zurückgegriffen. Bei der Entwicklung wurde Wert auf einfache Ausführbarkeit, sowie eine geringe Zahl an externen Abhängigkeiten, gelegt, um eine wiederholbare Ausführbarkeit auch in der Zukunft zu gewährleisten. Wireshark und nmap wurden, neben den bereits genannten Gründen, aufgrund der wiederholten expliziten Nennung in der Technischen Richtlinie gewählt. Die verwendeten Programme des Aircrack-ng Softwarepaketes wurden genutzt, da diese auch in den bereits durchgeführten Prüfungen von Geräten durch die TR zum Ein-

satz kamen. Eine Alternative zu nmap bietet das Programm „MASSCAN“ oder „Angry IP Scanner“ [63, 64]. Jedoch ermöglichen beide Programme nicht den Funktionsumfang von nmap. Vergleichbare Funktionalität zu den Programmen aus dem aircrack-ng Paket hat das „netsniff-ng toolkit“ [65]. Neben tcpdump stellt auch „Ethercap“ eine geeignete Alternative zu Wireshark dar. So können Netzwerkmitschnitte ebenfalls im „pcap“ Format gespeichert werden, welches auch Wireshark nutzt [66].

Als Router wurde ein TP-Link Archer C7 (AC1750) Dualband-Gigabit-WLAN-Router (v5) verwendet. Dieses Modell wurde aufgrund der Beliebtheit im OpenWrt-Umfeld, der Verfügbarkeit, der aktuellen Ausstattung und dem Preis-Leistungs-Verhältnis gewählt. Die Statistiken der OpenWrt-Webseite haben gezeigt, dass die zu dem Gerät gehörige Version die am dritthäufigsten heruntergeladene OpenWrt-Firmware im November des Jahres 2020 ist (vgl. Tabelle 3.1). Bei dem Xiaomi Mi R3P und dem D-Team Newifi D2 Router, welche öfter abgefragt wurden, handelt es sich zwar um günstigere Geräte, allerdings haben diese nur eine eingeschränkte Verfügbarkeit in Deutschland. Die vom gewählten TP-Link unterstützten Funktionen sind darüber hinaus vergleichbar mit vielen Endgeräten, welche im privaten und SOHO Umfeld eingesetzt werden.

Firmware image	Hits	Bandwidth
/releases/19.07.4/targets/ramips/mt7621/openwrt-19.07.4-ramips-mt7621-xiaomi_mir3p-initramfs-kernel.bin	2598	528.26 MB
/releases/19.07.4/targets/ramips/mt7621/openwrt-19.07.4-ramips-mt7621-d-team_newifi-d2-squashfs-sysupgrade.bin	1289	3.90 GB
↪ /releases/19.07.4/targets/ath79/generic/openwrt-19.07.4-ath79-generic-tplink_archer-c7-v5-squashfs-factory.bin	1255	4.91 GB
/releases/19.07.4/targets/ath79/generic/openwrt-19.07.4-ath79-generic-tplink_archer-c6-v2-squashfs-factory.bin	1129	4.27 GB

Tabelle 3.1: Auszug aus den Downloadzahlen pro Firmware vom 30.11.2020.

3.2 Aufbau und Beschreibung der Testumgebung

Der genutzte Testaufbau soll einen reibungslosen Ablauf der Testfälle erlauben sowie einfach reproduzierbar sein. Der Internetanschluss wurde durch den Internet Service Provider (ISP) bn:t Blatzheim Networks Telecom GmbH zur Verfügung gestellt. Der Glasfaseranschluss des ISP terminiert in einer FRITZ!Box 5530 Fiber, welche das Subnetz 192.168.178.0/24 bereitstellt. Der WAN Port des mit OpenWrt 19.7.04 bespielten TP-Link Archer C7 v.5 Dualband-Gigabit-WLAN-Router, wurde mit dieser FRITZ!Box verbunden, sodass der OpenWrt-Router das Subnetz 192.168.1.0/24 zur Verfügung stellen konnte. Die Erstinstallation von OpenWrt auf dem TP-Link Router erfolgte über die zur Verfügung stehende Anleitung [67]. Zunächst wurde das Firmware-Abbild heruntergeladen, daraufhin wurden die Hash-Werte mit den veröffentlichten und signierten Hash-Werten abgeglichen. Nachdem sichergestellt wurde, dass diese übereinstimmten, konnte die Datei über das Web-Interface des TP-Link Routers aufgespielt werden. Die OpenWrt Installationsdatei wurde hierzu über

die Firmware-Update Funktion hochgeladen und automatisch vom Gerät installiert. Das Gerät startet daraufhin persistent mit OpenWrt anstelle des Betriebssystems von TP-Link. Alternativ besteht die Möglichkeit das Firmware-Abbild von OpenWrt über die „Trivial File Transfer Protocol“ (TFTP) Funktionalität des Routers aufzuspielen.

Ein Testcomputer wurde über das LAN Interface angeschlossen, ein weiterer Laptop per WLAN und LAN verbunden (siehe Abbildung 3.1). Der Testcomputer wurde wahlweise mit Windows 10 Version 20H2 (Build 19042.685) oder Ubuntu 20.04 LTS betrieben. Auf dem Laptop kam Kali Linux 2020.2 zum Einsatz. Dieser Aufbau gibt dem Tester eine flexible Arbeitsumgebung, in welcher die Tests ungestört durchgeführt werden können. Durch die Abtrennung des Netzes in das 192.168.1.0/24 Subnetz durch den OpenWrt Router sind Geräte des allgemeinen Heimnetzes von Portscans und Netzwerkpaketmitschnitten ausgeschlossen. Dadurch können Tests performanter durchgeführt werden, während andere Teilnehmer des Netzes ungestört weiterarbeiten können. Ebenso bietet der beschriebene Aufbau einfach die Möglichkeit weitere Geräte, welche für Tests benötigt werden, hinzuzufügen. Die verwendeten Linux-Distributionen, Ubuntu 20.4 LTS und Kali Linux, bieten die Möglichkeit die notwendigen Programme reibungslos zu betreiben.

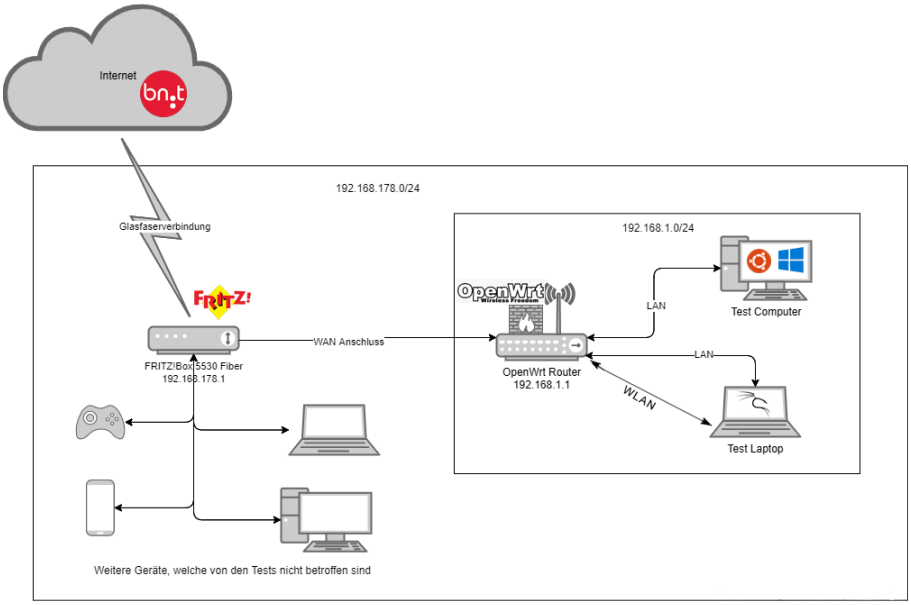


Abbildung 3.1: Aufbau der eingesetzten Testumgebung. Es handelt sich hierbei um einen sog. „double NAT“ Aufbau, d.h. der OpenWrt-Router hat keinen nativen Internetanschluss sondern bezieht die Internetverbindung über einen vorgelagerten Router. Die Tests wurden im Subnetz 192.168.1.0/24 durchgeführt.

Dieser sogenannte „double NAT“ (Network Address Translation) Aufbau (vergleiche Abbildung 3.2) stellt praktisch keinen Nachteil dar [68]. Obwohl der direkte Anschluss des OpenWrt-fähigen Routers präferiert eingesetzt werden sollte, können alle Tests ohne Integritätsverlust durchgeführt werden. Die Tests bezüglich des WAN Anschlusses kön-

nen über die IP-Adresse des OpenWrt Routers durchgeführt werden, welche durch die FRITZ!Box vergeben wurde. Weiterhin wurde der „Domain Name System Resolver“ (DNS Resolver) der FRITZ!Box auf die IP-Adresse des OpenWrt Routers geändert, um die Tests bzgl. des DNS-Protokolls und der Implementierung nicht zu verfälschen. Alle verfügbaren Firewall- und Filter-Einstellungen der FRITZ!Box wurden ebenfalls während der Tests deaktiviert.

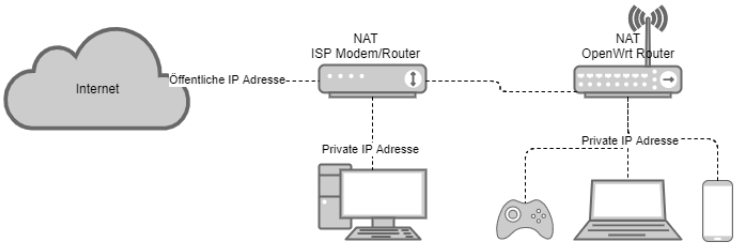


Abbildung 3.2: Beispiel einer allgemeinen „double NAT“ Umgebung. Die Darstellung basiert auf: https://kb.netgear.com/30186/What-is-Double-NAT (abgerufen: 13.12.2020)

3.3 Durchführung der Testfälle

3.3.1 Conformance Statement

Im Falle dieser Arbeit wurde das „Conformance Statement“ (vgl. Abschnitt 2.5.1) als Teil der Richtlinie betrachtet und mit den in der Online-Dokumentation von OpenWrt beschriebenen Informationen ausgefüllt. Darüber hinaus konnte der Quellcode Aufschluss über in der Dokumentation ungeklärte Fragestellungen geben. Die Informationen zu Modul A zeigen, dass OpenWrt eine vergleichsweise geringe Anzahl an Diensten im Ausgangs- sowie initialisierten Zustand anbietet. Lediglich der Web-Server uHTTPd auf Port 80, der SSH Server auf Port 22 und der von dnsmasq zur Verfügung gestellte DNS-Dienst auf Port 53 sind aktiv. Funktionen wie das Session Initiation Protocol (SIP) für Voice-over-IP-Telefonie (vgl. Abschnitt 2.1) oder Protokolle zur externen, automatischen Konfiguration des Geräts, welche oft bei handelsüblichen Routern verwendet werden, fehlen vollends. Ebenso gibt die Dokumentation an, dass das veraltete und als unsicher geltende Wi-Fi Protected Setup (WPS) Verfahren ohne die Installation von zusätzlicher Software nicht verwendet werden kann [69]. Dies ist auf vielen aktuellen Geräten in den Standardeinstellungen aktiviert. Aus dieser eingeschränkten Menge an Diensten wird ersichtlich, dass das Gerät nur über die Netz-Schnittstelle oder per SSH eingerichtet und bedient werden kann. Jedoch steht dem Nutzer standardmäßig der sogenannte „root“ Benutzer zur Verfügung, sodass uneingeschränkter Zugriff auf alle Funktionen und Einstellungen des Gerätes gewährleistet ist. Eine weitere Besonderheit zeigt sich in

auch in der Vorkonfiguration des WLAN-Netzes von OpenWrt. Dies ist zunächst deaktiviert und wird standardmäßig ohne Passwort initialisiert. Begründen kann man dies damit, dass OpenWrt nicht mit gerätespezifischer Dokumentation ausgeliefert werden kann wie sonst üblich. Ein Schriftstück mit einzigartigem Passwort für das Gerät, sowie das voreingestellte WLAN, kann nicht erstellt werden. So muss jedes Passwort, welches für ein OpenWrt Gerät verwendet wird, vom Benutzer selbst erstellt werden. Dies kann sowohl positive als auch negative Implikationen für die Sicherheit des Gerätes haben. Zum einen verhindert dieses Vorgehen, dass ein Hersteller ein unsicheres Passwort festlegt, welches ein unerfahrener Nutzer nicht ändert. Ebenso könnte der Hersteller ein bestimmtes Muster oder Master-Passwort verwenden. Wenn dieses veröffentlicht wird, so sind alle Geräte auf denen das Passwort nicht geändert wurde in Gefahr. Zum anderen könnte der Nutzer ein unsicheres Passwort vergeben, wenn er damit konfrontiert wird. Wenn vom System keine festen Ansprüche an dieses Passwort gesetzt werden, so würde ein schwaches Passwort die Sicherheit des Gerätes ebenso kompromittieren (siehe Abschnitt 2.2.1).

Schon im zweiten Abschnitt des „Conformance Statement“, welcher sich auf das öffentliche Netz bezieht, wird erkenntlich, dass auch auf Seiten des Internets nur eine minimale Anzahl an Diensten verwendet wird. Die Dokumentation von OpenWrt spezifiziert keinen Dienst, welcher auf dem WAN-Interface angeboten wird. Ein vergleichbarer Trend kann auch bei den angebotenen Funktionen des Geräts beobachtet werden. Lediglich sehr grundlegende Funktionen wie DHCP, SSH, secure copy (SCP), IPv6 Unterstützung und eine Firewall werden angeboten. Die eigens für OpenWrt entwickelte, quelloffene Packet-Management Software „opkg“, über welche zusätzliche Funktionalität installiert werden kann, bildet jedoch eine Ausnahme. Der geringe Umfang an Funktionen lässt sich in zweierlei Hinsicht begründen. Durch den Packet Manager opkg kann gewünschte Funktionalität leicht vom Benutzer selbst installiert und eingerichtet werden, ohne schon im Vorhinein Speicherplatz für Funktionen zu nutzen, welche unter Umständen nicht verwendet werden. Darüber hinaus kann OpenWrt so auch auf Geräten mit limitiertem persistenten Speicher oder Arbeitsspeicher installiert werden. So kann zum Beispiel das Web-Interface von der Installation ausgeschlossen sein, wenn ein Gerät nicht über genügend Speicher verfügt. Dadurch ist eine minimale Installation auf Geräten mit 4MB Flashspeicher und 32MB RAM möglich (vgl. Abschnit 2.3).

Ein Defizit von OpenWrt lässt sich jedoch bereits im „Conformance Statement“ finden. Es besteht keine Möglichkeit sicherheitsrelevante Updates automatisch einzuspielen. Über den Paket Manager bereitgestellte Funktionen könnten zwar mittels sog. CronJobs aktualisiert werden, dies würde jedoch nur periodisch nach Einstellung des Nutzers geschehen. Dies bietet keine Sicherheit, wenn die Periode zu groß gewählt wurde. Sicherheitslücken im Linux Kernel können jedoch nur über vollständige Firmware-Upgrades behoben werden

und erfordern das aktive Eingreifen des Nutzers. Dies setzt das Engagement und fachliche Verständnis des Nutzers voraus, über den aktuellen Stand informiert zu bleiben und eine Aktualisierung zeitnah durchzuführen. Jedoch gibt die Dokumentation an, dass die Überprüfung des Firmware-Upgrades von OpenWrt auf Integrität und Authentizität nicht automatisiert ist. Für einige Abbilder stehen digitale Signaturen zur Verfügung, welche vom integrierten Tool fwtool beim Aufspielen des Updates geprüft werden. Falls dieser Option allerdings nicht zur Verfügung steht, stehen dem Nutzer zur Unterstützung beim Upgrade-Prozess dann die eingebetteten Metadaten bereit, welche ausschließlich sicherstellen, dass es sich überhaupt um ein unterstütztes Gerät handelt. Gleichermaßen sind die berechneten Hash-Werte verfügbar, welche durch den Benutzer mit den signierten Werten des Download-Servers abgeglichen werden können [70].

Die folgenden Module des „Conformance Statements“ zeigen gleichwohl eine weitere Besonderheit von OpenWrt. Die für Firewall, DNS und DHCP verwendeten Implementierungen sind vollständig quelloffen und werden schon seit vielen Jahren entwickelt. Die Firewall wird durch ein für OpenWrt gestaltetes Programm firewall3 bereitgestellt. Es handelt sich hier um eine einfache Möglichkeit netfilter/iptable Regeln zu gestalten. Iptables ist Bestandteil des Kernels und wird schon seit Version 2.4 mitgeliefert [71]. Der DHCP und DNS-Dienst werden von dnsmasq ermöglicht. Dies ist ebenfalls ein weit verbreitetes Programm, welches bereits 2001 veröffentlicht wurde und seitdem kontinuierlich weiterentwickelt wurde [72]. Da OpenWrt keine Fernwartungs-, VoIP- oder VPN-Funktionalität bereitstellt, ohne die entsprechenden Pakete über den Paketmanager zu installieren, werden diese im weiteren Verlauf nicht betrachtet und dieses Ergebnis im „Conformance Statement“ vermerkt.

3.3.2 Test Documentation

Die Testdokumentation wurde in Form der bereitgestellten Tabellenkalkulationsdatei ausgefüllt (vgl. Abschnitt 2.5.1 und Tabelle 2.2). Alternativ können die Ergebnisse auch in einer Textdatei festgehalten werden. Die Anforderungen mit Kriterien zum Bestehen des Testes finden sich in der veröffentlichten „Test Specification“. Die in der Richtlinie spezifizierten Zustände (vgl. Absatz 2.5.1 des DUT wurden vor Beginn der Test nach Rücksprache mit dem BSI wie folgt festgelegt: Das Gerät ist im Auslieferungszustand (factory state), wenn es initial in Betrieb genommen wurde und nach jedem vollständigen Zurücksetzen. Der erste Start nach einem solchen Zurücksetzen des Geräts versetzt dieses in den Auslieferungszustand. Der initialisierte Zustand (initialized state) ist erreicht, wenn das Gerät im Auslieferungszustand gestartet und ein Passwort für das Root-Konto vergeben wurde. Dies ist vom Nutzer selbst vorzunehmen und nicht verpflichtend. Für alle Testfälle, die den initialisier-

ten Zustand oder den kundenspezifischen (customized state) Zustand voraussetzen, wurde diese Aktion durchgeführt. Das Gerät befindet sich im kundenspezifischen Zustand, wenn zusätzliche Einstellungen vom Nutzer aktiviert oder angepasst wurden (vgl. Abbildung 3.3). Die spezifizierten Kriterien für den Übergang zwischen den verschiedenen Zuständen sind spezifisch für das in dieser Arbeit betrachtete Gerät und müssen für jedes weitere Gerät selbst definiert werden.

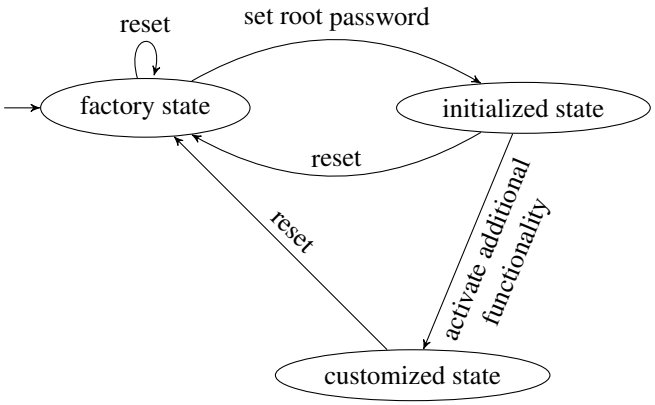


Abbildung 3.3: Darstellung der Zustände des Geräts sowie Übergangskriterien.

Modul A – Private Network

Wie in TP.A.1 nachgewiesen, unterstützt die betrachtete Version von OpenWrt zwei Arten, das Gerät in Betrieb zu nehmen. Zum einen stellt das Gerät einen SSH Zugang zur Verfügung, zum anderen den Web-Server, welches das Web-Interface „LuCI“ bereitstellt. Zur Prüfung des verlangten vollständigen Internetzugangs im initialisierten Zustand (TR.A.1) wurde die DNS-Funktionalität des bei Windows 10 standardmäßig installierten Kommandozeilenprogramm nslookup verwendet. Um zu testen, ob eine FTP-Verbindung (File Transfer Protocol) über den OpenWrt Router aufgebaut werden kann wurde das Windows-Kommandozeilenprogramm "ftp"verwendet. Hierzu wurde der FTP-Downloadserver von DD-WRT genutzt (ftp.dd-wrt.com), da dieser ohne Benutzerkonto genutzt werden kann. HTTP, sowie HTTPS-Unterstützung können mittels des Programms „curl“ nachgewiesen werden. Hierbei handelt es sich um ein quelloffenes Programm, welches neben HTTP und HTTPS viele verschiedene Protokolle unterstützt und zur Übertragung von Daten über diese Protokolle gedacht ist [73]. Das „Simple Mail Transfer Protocol“ (SMTP) kann ebenfalls mit Hilfe von curl getestet werden. Die geforderte IPv4 und IPv6 Konnektivität kann mit den Kommandozeilenapplikationen ping bzw. ping6 geprüft werden. Zur Sicherstellung der SSH-Verbindung kann zum Beispiel der kostenlose öffentliche Server von „SDF Public Access UNIX System, Inc“ genutzt werden (ssh.sdf.org). Ein eigens bereitgestellter SSH-

Server kommt ebenfalls in Frage. Die Unterstützung für das Telnet Protokoll muss unter Windows zunächst aktiviert werden, es ist jedoch auf vielen Linux Distributionen sofort verfügbar. Ein Test kann über die URL „towel.blinkenlights.nl“ durchgeführt werden. Die verwendeten Programme stehen unter den meisten aktuellen Betriebssystemen standardmäßig zur Verfügung und die spezifizierten Server sind weltweit kostenlos zu erreichen. Ebenfalls kann angenommen werden, dass die angegebenen URLs längerfristig zu erreichen sind, da sie schon seit vielen Jahren ihre Dienste anbieten.

Ein wichtiger Aspekt der Technischen Richtlinie wird ebenfalls durch TR.A.2 bis TR.A.5 spezifiziert. Diese „Test Requirements" behandeln die durch das Gerät zur Verfügung gestellten Dienste. Es wird vorausgesetzt, dass die angebotenen Dienste durch den Hersteller dokumentiert und auf eine wohldefinierte, minimale Menge beschränkt sind. Die Überprüfung kann mit Hilfe des Tools nmap (siehe Abschnitt 3.1) durchgeführt werden. Nmap ist ein quelloffener Portscanner, welcher ursprünglich von Gordon Lyon entwickelt wurde [57]. Es wird genutzt, um offene Ports und die darauf lauschenden Dienste zu identifizieren. Die TCP Ports des DUT wurden mit dem Kommando

```
$ nmap -sS -sC -sV -p- -Pn -oN <Dateiname.txt> 192.168.1.1
... oder ...
$ nmap -sSCV -p- -Pn -oN <Dateiname.txt> 192.168.1.1
```

Listing 3.1: Verwendetes nmap-Kommando zum Scannen aller **TCP**-Ports des OpenWrt Routers.

überprüft. Ebenfalls kann der Option „-T4“ hinzugefügt werden, um ggf. die Geschwindigkeit durch eine engere Taktung der Anfragen zu erhöhen. UDP Dienste wurden wie folgt getestet:

```
$ nmap -n -sUV --version-intensity 0 -p- --max-retries 1 -v -oN <Dateiname.txt>
    192.168.1.1
```

Listing 3.2: Verwendetes nmap-Kommando zum Scannen aller **UDP**-Ports des OpenWrt Routers.

Die optionale Erweiterung „-v“ erhöht die Verbosität und liefert bei den zeitintensiven UDP-Scans Informationen über den Fortschrittsgrad. Eine genaue Übersicht über die Funktion der gewählten Kommandos liefert Abbildung 3.4. Die beiden verwendeten Kommandos bzw. leichte Abwandlungen von diesen wurden vor allem aufgrund ihrer detaillierten Ausgabe sowie Performanz gewählt.

```
HOST DISCOVERY:
    -Pn: Treat all hosts as online -- skip host discovery
    -n: Never do DNS resolution [default: sometimes]

SCAN TECHNIQUES:
    -sS: TCP SYN
    -sU: UDP Scan

PORT SPECIFICATION AND SCAN ORDER:
    -p <port ranges>: Only scan specified ports
        Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
        Use -p- to scan all ports

SERVICE/VERSION DETECTION:
    -sV: Probe open ports to determine service/version info
    --version-intensity <level>: Set from 0 (light) to 9 (try all probes)

SCRIPT SCAN:
    -sC: equivalent to --script=default

TIMING AND PERFORMANCE:
    Options which take <time> are in seconds, or append 'ms' (milliseconds),
    's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
    -T<0-5>: Set timing template (higher is faster)
    --max-retries <tries>: Caps number of port scan probe retransmissions.

OUTPUT:
    -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
        and Grepable format, respectively, to the given filename.
    -v: Increase verbosity level (use -vv or more for greater effect)
```

Abbildung 3.4: Auszug aus der Dokumentation des Programms nmap. Die hier dargestellten Optionen des Programmes beziehen sich auf die im Verlauf der Arbeit eingesetzten Optionen. Quelle: https://svn.nmap.org/nmap/docs/nmap.usage.txt (Abgerufen am 02.01.2020)

Zur Prüfung der WLAN-Schnittstelle wurde auf die Programmsuite aircrack-ng zurückgegriffen. Es handelt sich hierbei um eine frei verfügbare Sammlung von Programmen zur Analyse der Sicherheit von Wi-Fi Netzwerken [74]. Zunächst wird das Programm airmon-ng eingesetzt, um die WLAN-Karte in den sogenannten Monitor-Modus zu versetzen:

```
$ airmon-ng start wlan0
```

Listing 3.3: Kommando um die WLAN-Karte in den Monitormodus zu versetzen. Der Name der verwendeten Karte ist wlan0.

Daraufhin kann airodump-ng verwendet werden, um Informationen zu allen verfügbaren WLAN-Netzen bereitzustellen:

```
$ airodump-ng wlan0mon
```

Listing 3.4: Kommando um airodump-ng mit der soeben in den Monitormodus versetzen WLAN-Karte zu starten.

Vor allem die Spalte „ENC“, welche für „encryption“ steht, ist von Bedeutung. Sie zeigt an, dass das Gerät durch Wi-Fi Protected Access 2 (WPA2) geschützt ist. Dies unterstützt die Annahme, dass das Gerät WPA2 nach dem IEEE802.11i Standard bereitstellt.

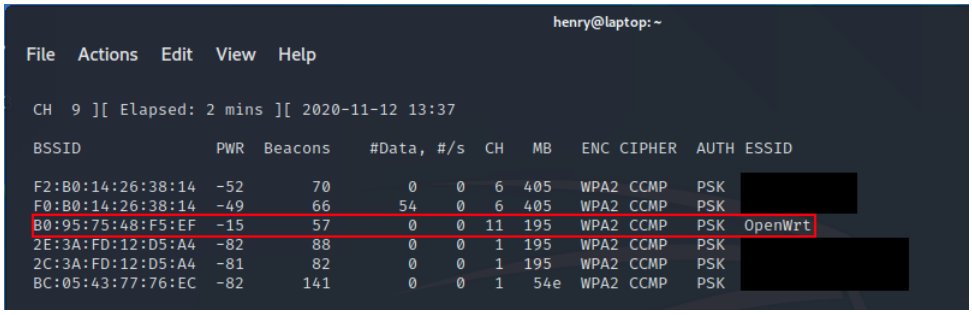


Abbildung 3.5: Die Ausgabe des Programms airodump-ng. Man kann sehen, dass OpenWrt mit WPA2 CCMP verschlüsselt ist und ein Password (Spalte PSK) benötigt.

Modul B - Public Network

Die Teststrategie, welche für Modul B – Public Network eingesetzt wurde, ist nahe an der Vorgehensweise von Modul A – Private Network orientiert. Jedoch wird nun die IP des OpenWrt Geräts im Kontext des Subnetzes 192.168.178.0/24 verwendet (siehe Abbildung 3.1). So wird nicht die LAN-Schnittstelle des Gerätes angesprochen, sondern die WAN-Schnittstelle, also die öffentliche IP-Adresse des Gerätes ist.

```
$ # Fuer TCP:
$ nmap -sSCV -p- -Pn -oN <Dateiname.txt> 192.168.178.115
$ # Fuer UDP:
$ nmap -n -sUV --version-intensity 0 -p- --max-retries 1 -v -oN <Dateiname.txt>
    192.168.178.115
```

Listing 3.5: nmap Kommandos zum Scannen der WAN-Schnittstelle von OpenWrt. Das erste Kommando scannt TCP, das zweite UDP. Die angegebene IP-Adresse ist die des OpenWrt Routers.

Auch die VoIP Funktionalität kann effektiv mit nmap getestet werden. Zusätzlich zu einem vollständigen Scan des Geräts wurden auch die standardmäßig für VoIP verwendeten Ports 5060 und 5061 separat gescannt.

```
$ # TCP Port 5060, 5061 testen
$ nmap -sSCV -p 5060,5061 -Pn -oN <Dateiname.txt> 192.168.178.115
$ # UDP Port 5060, 5061 testen
$ nmap -n -sUV --version-intensity 0 -p 5060,5061 --max-retries 1 -v -oN
    <Dateiname.txt> 192.168.178.115
```

Listing 3.6: Kommandos zum gezielten Scan der Ports 5060, 5061 mit nmap.

Jedoch sollte eine vollständige Prüfung aller Ports in jedem Falle durchgeführt werden, da diese Ports nicht zwingend genutzt werden müssen.

Modul C - Functionalities

Das „Test Requirement" TR.C.2 beschreibt die Anforderung, dass dem Endnutzer keinerlei Funktionalität verheimlicht werden darf. Dies ist eine durchaus schwierig zu prüfende Anforderung, welche erst zum Ende des Tests durchgeführt werden sollte. Im Falle von OpenWrt und dem somit vollständig verfügbaren Quellcode, sowie dem vollumfänglichen root Zugriff auf das Gerät per SSH ist dies vereinfacht, jedoch aufgrund des Funktionsumfangs immer noch eine Herausforderung. Es muss sich hier auf die Eindrücke und Erfahrungen des Testers zum Ende der Testphase verlassen werden. Darüber hinaus verweist die Technische Richtlinie ebenfalls auf eine Recherche in Foren und Blogs.

Modul D – Configuration and Information

Für die meisten modernen Heimrouter ist die Konfiguration durch ein Web-Interface die benutzerfreundlichste Methode, so auch für OpenWrt. Die Sicherung der Datenintegrität und Vertraulichkeit auf dem Transportweg wird heutzutage durch HTTPS erreicht. Diese Transportwegverschlüsselung verhindert, dass eine böswillige dritte Partei die übertragenen Daten auslesen oder verändern kann (siehe Abschnitt 2.2. Es ist also naheliegend, die Anforderung an eine durch HTTPS gesicherte Verbindung zum Webserver in der Technischen Richtlinie zu finden. Zur Überprüfung des „Test Requirement" TR.D.3 bietet sich ein Skript wie testssl.sh an, welches von Dr. Wetter IT-Consulting frei zur Verfügung gestellt wird [75]. Dieses Skript zeigt detaillierte Informationen zu allen vom Webserver unterstützten Protokollversionen sowie Verschlüsselungsmethoden an. Des Weiteren kann auch ein Paketaufzeichnungs- und Analyse-Software wie Wireshark eingesetzt werden, um die unverschlüsselten Pakete zu betrachten. Wenn HTTPS aktiv ist, sollten keine unverschlüsselten Daten in den Paketen gefunden werden können. Es ist ebenfalls möglich, Informationen zu HTTPS und dem dazugehörigen Zertifikat in den meisten modernen Browsern in der Nähe der URL-Leiste zu finden.

Nichtsdestoweniger müssen auch andere Angriffsvektoren auf Heimrouter betrachtet bzw. getestet werden. So muss das Einloggen auf dem Gerät gegen Bruteforce Angriffe (vgl. Abschnitt 2.2.1) geschützt sein. Eine Schutzmaßnahme kann ein Fehlerzähler sein, welcher die fehlgeschlagenen Versuche protokolliert und das Aufschalten auf das Gerät nach einer gewissen Anzahl an Versuchen unterbindet oder verlangsamt. Ebenso könnte die Eingabe auf Muster geprüft werden, um automatische Login-Versuche zu erkennen. Die Prüfung dieses „Test Requirements" wurde durch ein Skript in der Programmiersprache Python umgesetzt. Durch den Aufruf

```
$ python3 OpenWrt_Bruteforce_Check.py web
```

Listing 3.7: OpenWrt Webserver mit Python Skript auf Resistenz gegen Bruteforce Angriffe testen. (Das Programm ist auf dem Datenträger verfügbar)

wird der Web-Server getestet. Alternativ kann durch

```
$ python3 OpenWrt_Bruteforce_Check.py ssh
```

Listing 3.8: OpenWrt SSH-Server mit Python Skript auf Resistenz gegen Bruteforce Angriffe testen.

der SSH Server getestet werden. Vor der Nutzung können der korrekte Benutzername, sowie das korrekte Password, die Anzahl der Versuche, die IP des Geräts, sowie der SSH-Port festgelegt werden. Für den Test des SSH-Servers wurden 100 Versuche eingestellt, wobei die Zeit für die Antwort des Servers gemessen wird. Das Python Modul „SSHLibrary“ wird genutzt, um die Verbindungen mit dem SSH-Server zu handhaben. Zunächst wird geprüft, ob der spezifizierte Server erreichbar ist. Daraufhin werden die spezifizierten Login Versuche durchgeführt und die Zeit bis zur Antwort des Servers gemessen. Die Antwort des Servers bei falschen Daten ist der Abbruch der Session durch eine SSHLibrary Exception. Nachdem die Daten gesammelt wurden, wird eine lineare Regression auf den Daten durchgeführt, um einen Trend in den Antwortzeiten kenntlich zu machen. Wenn ein linearer Anstieg zu erkennen ist, dann werden die Versuche verlangsamt, wenn die Regressionslinie jedoch zur X-Achse parallel ist, so werden die Versuche in konstanter Zeit durchgeführt. Neben der grafischen Darstellung der Antwortzeiten, sowie der Regressionslinie, werden dem Nutzer der Mittelwert, der Median, der Regressionskoeffizient und der Standardfehler angezeigt. Nachdem die Analyse durchgeführt wurde, werden die korrekten Login Daten verwendet, um eine neue Verbindung herzustellen. Wenn das OpenWrt SSH-Banner korrekt angezeigt wird, lässt der SSH-Server trotz der vorherigen fehlgeschlagenen Versuche noch weitere zu, ohne erkennbare Entschleunigung. Der Test des Webservers wurde durch die POST Anfrage

```
http://192.168.1.1/cgibin/luci/admin/status?luci_username={USERNAME}
                                          &luci_password={PASSWORD}
```

realisiert. Wenn ein falscher Benutzername, oder ein falsches Passwort verwendet wird, so antwortet der Webserver mit dem Statuscode 403. Nach der ersten Überprüfung der Verbindung wurden erneut 100 Versuche eingestellt. Dieser Wert wurde gewählt, um eine möglichst große Stichprobengröße zu erzielen und den unter Umständen implementierten Grenzwert für Login-Versuche zu überschreiten. Der weitere Ablauf der Analyse verläuft wie bereits beschrieben. Nach der Auswertung der Daten werden die korrekten Login-Daten an den Server geschickt. Ein einfacher regulärer Ausdruck überprüft, ob ein erfolgreicher Login möglich war, und es wird dem Benutzer anschließend angeboten, eine eingeloggte Session im Browser zu öffnen.

Zur Überprüfung der Anforderung TR.D.12 wird zunächst festgestellt, ob es einen Anti-CSRF Cookie (vgl. Abschnitt 2.2.2) gibt. Zunächst kann der Speicher des Webbrowsers angezeigt werden, um zu prüfen, ob überhaupt ein Cookie eingesetzt wird. Daraufhin wird die Web-Proxy Funktionalität von Burp Suite genutzt, um den Ablauf des Logins und der Erstellung einer gültigen Session zu beobachten. Dabei handelt es sich um ein Programm, welches die Anfragen des Nutzers und des Servers entgegen nimmt und stellvertretend an den jeweils anderen vermittelt. Die Besonderheit bei Burp Suite ist dabei, dass die Anfragen zunächst abgefangen werden und der Inhalt für den Nutzer dargestellt wird. Auf diese Weise lässt sich die gesamte Kommunikation zwischen einem Client und einem Server beobachten (vgl. Abbildung 3.6). Alternativ zu Burp Suite kann auch der „Zed Attack Proxy“ (ZAP) des „Open Web Application Security Project“ (OWASP) eingesetzt werden [76]. Alle nachfolgenden http-Methoden sollten nach Initialisierung des Cookies diesen als Sicherheitsmerkmal mit versenden. Der Quellcode von OpenWrt gibt darüber hinaus weiteren Aufschluss über die Implementierung der Anti-CSRF Tokens. Die Datei „dispatcher.lua“ des LuCI Interfaces, welche die Erstellung und Validierung der Benutzer-Sitzungen handhabt, zeigt in diesem Falle eindeutig, dass es sich um Anti-CSRF Cookies handelt und dass diese durch den als sicher anerkannten Zufallszahlengenerator /dev/urandom generiert werden [77, 78]. Abschließend wurde ein einfaches Python Skript verwendet, welches 100 gültige Sitzungen am Web Server des OpenWrt Routers anmeldet und mittels eines Regulären-Ausdruckes den Wert des Cookies ausließt. Dazu wird das Request Modul von Python verwendet, sowie die POST-Anfrage, welche bereits für das Bruteforce-Skript verwendet wurde. Abschließend wird geprüft, ob die 100 verschiedenen Sitzungen einzigartige Session-IDs und Anti-CSRF Token besitzen.

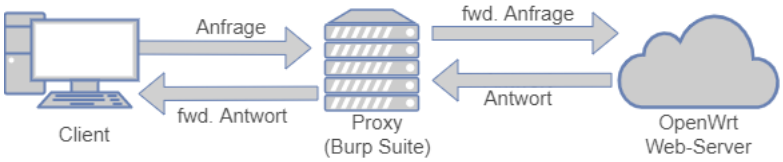


Abbildung 3.6: Vereinfachte Darstellung eines MITM-Proxies wie Burp Suite.

Modul E – Firmware Updates

Modul E der Technischen Richtlinie prüft die Firmware Update Funktion des Geräts. Hier ist vor allem der Mechanismus der Firmware-Validierung von Interesse. Nach Angaben der Entwickler werden einige Firmware Dateien signiert. OpenWrt liefert standardmäßig ein Kommandozeilenprogramm, mit dem Signaturen und Metadaten aus den Firmwareabbildern extrahiert werden können. Der Aufruf

```
$ fwtool -s - <Dateiname.bin>
```

Listing 3.9: Nutzung des in OpenWrt integrierten Programmes „fwtool“ zur Extraktion von Signaturen aus OpenWrt Firmware-Abbildern

zeigt die Signatur an, wenn diese vorhanden ist. Ebenso muss ermessen werden, wie lange der Hersteller benötigt, um Sicherheitslücken zu beheben. Die sogenannten „Git Hashes“, genaue Identifizierungsmerkmale eines git commits, sind hier förderlich, da sie einen genauen Zeitstempel tragen. Des Weiteren ist der entsprechende git commit, welcher eine Sicherheitslücke behebt, in den Sicherheitsnotizen auf der OpenWrt Website spezifiziert, sodass das Erstellen einer Zeitleiste mit Sicherheitsvorfällen und deren Beheben einfach realisierbar ist.

Modul G – Domain Name System (DNS)

Zur weiteren Einschränkung der Angriffsoberfläche wird in Modul G die Implementierung des DNS-Dienstes des DUT geprüft. Ein möglicher Angriff auf DNS-Dienste ist eine sogenannte DNS Rebinding Attacke (vgl. Abschnitt 2.2.3). Die Überprüfung der Anforderung TR.G.2 basiert auf der Untersuchung der verwendeten Methoden zur Mitigation von DNS Rebinding Attacken und einem funktionalen Test dieser Umsetzung. Da OpenWrt DNS-Dienste mittels dnsmasq anbietet, muss geprüft werden, ob die Option „–stop-dns-rebind“ aktiviert ist. Dies ist sowohl über die Kommandozeile als auch über das LuCI Web-Frontend möglich. Ein funktionaler Test dieser Sicherheitsmaßnahme kann mittels des Singularity of Origin Web-Toolkits der NCC Group getestet werden [31]. Als Target Host wird dabei die IP-Adresse des OpenWrt Routers spezifiziert. Des Weiteren wurde das Intervall auf zwei reduziert und die Option „Flood DNS Cache“ aktiviert. Diese Option konnte genutzt

werden, da der Test mit einem Chromium basierten Browser durchgeführt wurde. Das Web-Tool spezifiziert, dass diese Option erfolgreich im Chrome-Browser getestet wurde (vgl. Abbildung 3.7). Es bietet sich ebenfalls an verschiedene „Attack Payloads“ und Strategien zu testen.

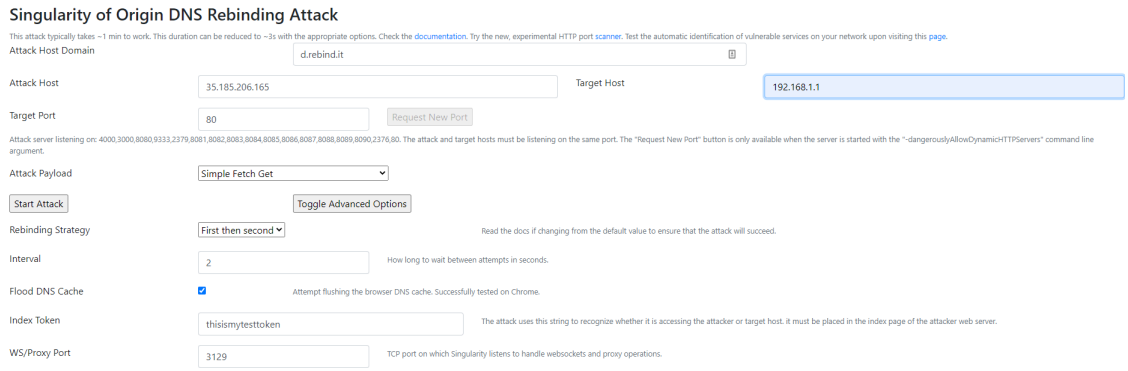


Abbildung 3.7: Das Singularity of Origin Web-Interface. Die Webseite wird von der NCC Group bereitgestellt, um verschiedene Arten von DNS Rebinding Angriffen zu testen. In diesem Kontext wurde es genutzt, um zu prüfen, ob OpenWrt diese Angriffe erfolgreich abwehrt bzw. erkennt. `http://rebind.it:8080/manager.html`

Eine ebenso relevante Sicherheitsfunktion von DNS-Diensten ist die sogenannte „Source Port Randomization“ und „Transaction ID Randomization“, also die zufällige Wahl eines Quell-Ports, sowie einer Transaktions-ID für eine DNS-Anfrage. Diese Werte, welche vom DNS-Client generiert werden, dienen als Synchronisationsmethode zwischen dem DNS-Server und Client. Wenn der Quell-Port und die Transaktionsidentifikationsnummer von einem Angreifer berechnet oder geraten werden können, dann kann ein Angreifer diese nutzen, um dem Opfer manipulierte DNS-Antworten zu senden. Der DNS-Client würde diese aber als korrekt akzeptieren und eine potenziell schädliche Verbindung zu einem dritten Server aufbauen [79]. Für einen funktionalen Test werden zunächst mithilfe des Python Skriptes send_dns_requests.py eine große Anzahl verschiedene DNS-Anfragen generiert. Dazu wird eine Liste mit 1000 häufig besuchten Webseiten genutzt [80]. Dies bietet sich an, da so sichergestellt wird, dass diese Webseiten verfügbar sind und in einer geringen Zeit antworten. Ebenso erfüllt diese Anzahl an Anfragen die minimale Stichprobengröße (n) für $\rho = 0.5$ (Stichprobenfehler $e = 0.03$ / Signifikanzniveau $\alpha = 0.05$) [81, p. 13]. Während die DNS-Anfragen gestellt werden wird ein Mitschnitt aller Netzwerkpakete durch das Programm Wireshark gemacht. Die so erstellte Datei wird in einem weiteren Schritt analysiert. Dazu liest das Python-Skript „analyze_pcap.py“ diese ein und selektiert im ersten Schritt alle DNS-Pakete, welche vom OpenWrt Router gesendet wurden. Daraufhin werden der DNS-Quell-Port sowie die Transaktions-ID aus diesen Paketen ausgelesen. Im letzten Schritt werden die Anzahl der DNS Anfragen, die Anzahl der einzigartigen Ports und

Transaktions-IDs, die jeweiligen minimalen und maximalen Werte, die Standardabweichung und die häufigsten Werte angezeigt. Des Weiteren wird ein Kolmogorow-Smirnow-Test durchgeführt, um zu prüfen, ob die Verteilung der Daten mit einer Gleichverteilung übereinstimmt [82]. Schlussendlich werden noch jeweils zwei Grafiken generiert, welche die Daten in einem Säulendiagramm und einen Streudiagramm darstellen. Auf diese Art kann visuell prüfen, ob Muster in den Darstellungen zu erkennen sind.

```
Test results for DNS port randomization:

  Number of samples: 1086
  Number of unique ports: 1086
  Range: 61 - 65508
  Standard Deviation: 18668.148912615263
  5 most common ports: [(59336, 1), (27475, 1), (14318, 1), (57429, 1), (31375,
      1)]



Test results for transaction ID randomization:

  Number of samples: 1086
  Number of unique ports: 1037
  Range: 45 - 65415
  Standard Deviation: 19128.480563438716
  5 most common ports: [(22681, 2), (16653, 2), (25739, 2), (20337, 2), (57986,
      2)]

KstestResult(statistic=0.03222836095764273, pvalue=0.6257210434465147)
KstestResult(statistic=0.027624309392265192, pvalue=0.8019298430829213)
```

Listing 3.10: Ergebnisse der DNS Port und DNS Transaktions-Identifikationsnummern Analyse. Der Kolmogorow-Smirnow Test zeigt, dass die Daten annähernd gleichverteilt sind.

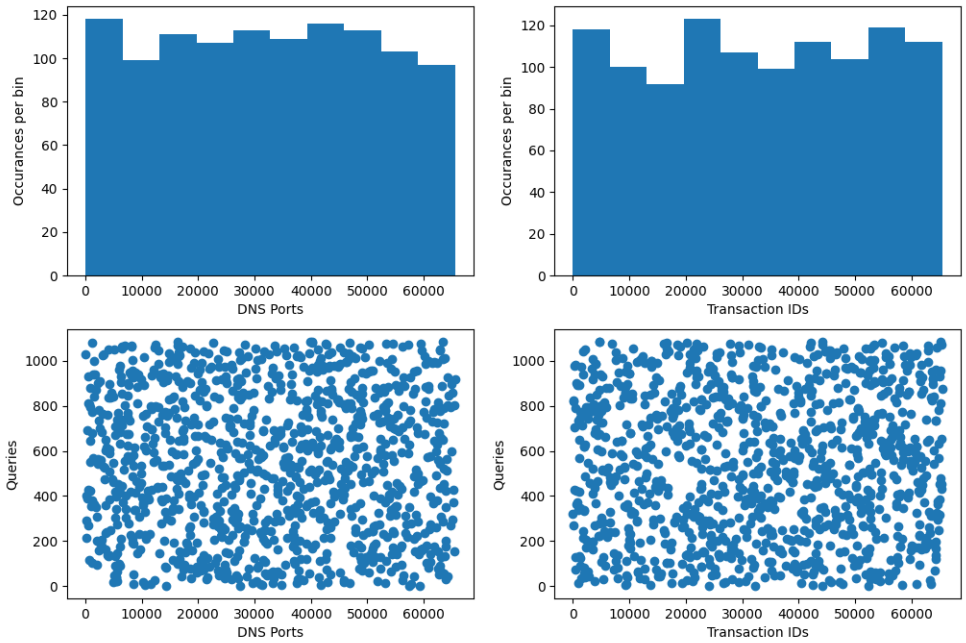


Abbildung 3.8: Darstellung der Ergebnisse als Säulendiagramm und als Streudiagramm. Die X-Achse beschreibt die Source-Ports bzw. die Transaktions-ID. Aus der Y-Achse der Säulendiagramme sind ist die Häufigkeit pro Sammelbehälter dargestellt. Die Y-Achse der Streudiagramme zeigt die Anzahl der Anfragen. Man kann sehen, dass die volle Spannbreite von 0 bis 65535 ausgenutzt wird. Da kein Muster in den Streudiagrammen erkennbar ist und die Säulendiagramme eine Gleichverteilung andeuten, kann angenommen werden, dass zufällige Source-Ports und Transaktions-IDs gewählt wurden.

Modul I – Factory Reset

Das Testen der Zurücksetzfunktion des OpenWrt Routers fällt aufgrund des uneingeschränkten Systemzugriffs einfach. Es können verschiedene Methoden eingesetzt werden. Zunächst sollte eine Leitlinie (Baseline) erstellt werden. Dazu dient ein Konfigurationsbackup, welches direkt nach dem ersten Einschalten des Geräts erstellt wurde. Dieses wird anschließend mittels des Kommandozeilenprogramms „diff“ mit einem Backup verglichen, welches nach der Nutzung des Routers und einem anschließenden Zurücksetzen des Geräts erstellt wurde. Alternativ kann das ebenfalls auf OpenWrt zur Verfügung stehende Kommandozeilenprogramm „md5sum“ verwendet werden, um MD5 Hash-Werte aller lesbarer Dateien auf dem System zu generieren und diese zu exportieren. Diese sollten nach dem Zurücksetzen des Geräts wieder übereinstimmen. Die Erstellung von CRC-Prüfsummen mit dem „cksum“ Befehl kann unter Umständen schneller sein, als MD5 Hash-Werte. Es bietet sich also an diese Prüfsummen auf leistungsschwachen Geräten zu verwenden. Da die MD5 Hash-Werte und

CRC Summen lediglich genutzt werden sollen, um zu prüfen, ob Einstellungen zurückgesetzt wurden, sind an dieser Stelle keine kryptografisch sicheren Hash-Werte wie SHA256 nötig. Die Wahrscheinlichkeit für zufällige Kollisionen bei MD5 ist sehr gering [83]. Darüber hinaus werden diese Prüfsummen bzw. Hash-Werte ausschließlich in einem lokalen System generiert und verwendet.

3.3.3 Nicht anwendbare Test Prozeduren

Ebenso wie die Natur des OpenWrt Projektes ein einfaches Testen vieler „Test Requirements" ermöglicht, so werden einige Aspekte der Firmware anders gehandhabt als bei handelsüblichen Heimroutern. So sucht man vergeblich nach einem initial verfügbaren WLAN-Netz, nachdem der Router gestartet und eingerichtet wurde. Ebenso sind viele Funktionen, die ein Nutzer vielleicht von anderen Geräten gewöhnt ist, nur als zusätzliches Software-Paket verfügbar, oder durch aufwendige Konfiguration. Beispiele sind Wi-Fi Protected Setup, ein Community WLAN, Fernwartung, automatische Firmware-Updates oder Meldungen zu neuen Firmware-Updates, Voice over IP und Virtual Private Network Funktionen.

3.4 Statische Code-Analyse einiger quelloffenen Router Firmware Alternativen mittels FACT

Neben der Methodik der Technischen Richtlinie des BSI gibt es noch viele weitere Arten, um Aspekte einer Software zu evaluieren. Die Sicherheit einer betrachteten Software, in diesem Fall OpenWrt, lässt sich unter anderem durch sogenannte statische Tests abschätzen (siehe Abschnitt 2.5.2). Es wird sich für die Durchführung einer statischen Code-Analyse von Router-Firmware an der Methodik des „Home Router Security Reports 2020“ des Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) orientiert [51]. In dieser Veröffentlichung des FKIE wurden 127 verschiedene, aktuelle Firmware-Abbilder von sieben Herstellern automatisch durch das ebenfalls vom FKIE entwickelte „Firmware Analysis and Comparison Tool“ (vgl. Abschnitt 2.5.2) analysiert und ausgewertet.

3.4.1 Installation und Testumgebung

FACT, welches vom FKIE kostenfrei zur Verfügung gestellt wird, wurde lokal auf einem Desktop Computer installiert. Es handelt sich hierbei um ein System mit 6 physischen und 6 virtuellen Prozessorkernen, welche jeweils auf einer Taktfrequenz von 4.2GHz betrieben

werden, sowie 16GB RAM. Ebenfalls stehen dem System 256GB persistenter Speicher zur Verfügung. Da die Installation auf Ubuntu 16.04, 18.04, 20.04 (stable) empfohlen wird, wurde Ubuntu 20.04 als aktuellster Vertreter des Ubuntu-Betriebssystems ausgewählt [84]. Die zum Zeitpunkt der Arbeit aktuelle Version von FACT, FACT_core v3.1.1, wurde mittels der bereitgestellten Anleitung installiert (siehe 3.11) [47].

```
$ sudo apt update && sudo apt upgrade && sudo apt install git
$ git clone https://github.com/fkie-cad/FACT_core.git ~/FACT_core
$ ~/FACT_core/src/install/pre_install.sh && sudo mkdir /media/data && sudo chown
    -R USER /media/data
$ sudo reboot
$ ~/FACT_core/src/install.py
$ ~/FACT_core/start_all_installed_fact_components
```

Listing 3.11: Installationsschritte für das „Firmware Analysis and Comparison Tool“ des FKIE. Diese Schritte Updaten die installierten Pakete, downloadet das Git Repository und führt alle nötigen Schritte zur Installation aus. Zuletzt wird das Programm gestartet.

Da das System den minimalen Software Anforderungen von FACT entspricht ist die Installation und Nutzung des Programms prinzipiell möglich, jedoch empfiehlt sich ein System mit mehr RAM, da dies die Performanz der Analyse erhöht. Ebenfalls kam es bei dem eingesetzten System vermehrt dazu, dass kein RAM mehr zur Verfügung stand und der Rechner während der Analyse aufgrund der Auslastung nicht anderweitig genutzt werden konnte. Der Einsatz eines separaten Test Computers oder eines Virtuellen Privaten Servers (VPS) ist zu empfehlen.

Minimal	Recommended	Software
4 Cores	16 Cores	git
8GB RAM	64GB RAM	python 3.5 - 3.8
10 GB disk space	10* GB disk space	OS see below

Abbildung 3.9: Minimale und empfohlene Systemvorraumsetzungen für FACT. Die Grafik stellt auch die benötigte Software dar. [51]

3.4.2 Erstellung des Firmware-Corpus

Der zu testende Firmware-Corpus besteht aus sieben verschiedenen, quelloffenen Router-Firmwares. Neben dem für die Technische Richtlinie verwendeten Abbild von OpenWrt Version 19.7.04, wurden noch sechs weitere Alternativen gewählt, von denen fünf spezi-

fisch für das gewählte TP-Link Model Archer C7 v5 kompiliert sind. Zu der betrachteten Firmware gehören DD-WRT, Gargoyle Router Management, Gluon, LibreCMC, Advanced-Tomato, sowie Version 19.7.05 von OpenWrt. Einzig AdvancedTomato bietet keine Version für den getesteten Router an, weshalb auf eine Version für einen NETGEAR WNDR3700v3 Dual-Gigabit-WLAN-Router zurückgegriffen wurde, da dieser Router ebenfalls eine MIPS Architektur nutzt und im Leistungsumfang vergleichbar ist.

Die aufgelistete Firmware wurde gewählt, da sie in Funktion und Umfang OpenWrt ähnlich sind und die Projekte, denen sie entstammt, ebenfalls mehrere Heimrouter mit einer Codebasis unterstützen. Es wurden keine Firmware-Alternativen gewählt, die auf Desktop Computern oder Servern installiert werden, da diese aufgrund der zur Verfügung stehenden Rechenkapazitäten im Leistungsumfang nicht vergleichbar sind. Das analysierte Korpus wurde am 21.12.2020 erstellt. Es wurde für jede analysierte Firmware die aktuellste Version für den TP-Link AC1750-Dualband-Gigabit-WLAN-Router genutzt, mit Ausnahme des Abbildes von OpenWrt Version 19.07.4 und der Tomato Firmware. Version 19.07.4 wurde getestet, da es sich um die mittels der Technischen Richtlinie geprüfte Version handelt.

Projekt	**Geeignetes Produkt**	**Firmware Version**
AdvancedTomato	NETGEAR WNDR3700v3	3.4-138
DD-WRT	TP-Link Archer C7 v5	12-18-2020-r45036
Freifunk Gluon	TP-Link Archer C7 v5	V2-v2020.2.1
Gargoyle Router Management	TP-Link Archer C7 v5	1.12.0 (stable)
LibreCMC	TP-Link Archer C7 v2	v1.5.3:2020-10-02
OpenWrt	TP-Link Archer C7 v5	19.07.4
OpenWrt	TP-Link Archer C7 v5	19.07.5

Tabelle 3.2: Übersicht über die für die Analyse ausgewählte Firmware. Dargestellt ist jeweils der Name des Projektes, das Produkt für das die Firmware geeignet ist und die ausgewählt Version der Firmware (vollständige Tabelle: Anhang 3.2)

3.4.3 Durchgeführte Tests und Metriken

Um einen Vergleich mit den Ergebnissen des „Home Router Security Reports 2020“ des FKIE zu ermöglichen, wurden die gleichen Aspekte auch bei der quelloffenen Firmware analysiert. Es wurden die folgenden sicherheitsrelevanten Aspekte betrachtet:

- Wann wurde das letzte Update für das Gerät veröffentlicht?
- Welches Betriebssystem wird verwendet und wie viele kritische Schwachstellen sind für dieses bekannt?

- Welche vorbeugenden Maßnahmen gegen Exploits werden eingesetzt und wie häufig sind diese aktiviert.
- Ist privates kryptografisches Schlüsselmaterial enthalten?
- Können hartkodierte Login-Daten und bekannte Passwörter in dem Firmware-Abbild gefunden werden?

Die einzelnen Komponenten des „Firmware Analysis and Comparison Tools“ werden mittels des Befehls

```
$ ~/FACT_core/start_all_installed_fact_components
```

Listing 3.12: Befehl zum starten alle Komponenten von FACT

gestartet. Nachdem der lokale Server gestartet ist, werden die Firmware-Abbilder einzeln über die Upload-Funktion hochgeladen. Die folgenden Analyse-Methoden wurden gewählt:

- CPU Architecture
- Crypto Material
- CVE Lookup
- CWE Checker
- Exploit Mitigations
- Known Vulnerabilities
- Software Components
- Source Code Analysis
- Users and Passwords

Die Ergebnisse der automatischen Analyse werden anschließend durch die REST API von FACT ausgelesen und als Grafiken dargestellt, sodass eine direkte Gegenüberstellung der Ergebnisse des FKIE mit den erhobenen Daten möglich ist.

Kapitel 4

Ergebnisse

4.1 Ergebnisse der Technischen Richtlinie

Von 101 „Test Requirements" konnte der TP-Link Router in 69 getestet werden. Bei den 32 nicht getesteten Fällen handelt es sich in den meisten Instanzen um Funktionalität, welche von dem Gerät ohne weitere Software-Pakete nicht unterstützt wird. So wurden die “Module K – Remote Configuration”, “Modul L – Voice over IP” und “Modul M – Virtual Private Network” vollkommen vom Testvorgang ausgeschlossen. Ebenso wurden „Test Requirements" nicht geprüft, welche mit den bereits genannten Modulen Gemeinsamkeiten haben. Darüber hinaus fielen Testfälle bezüglich der standardmäßig gesetzten Passwörter und Login-Daten ebenso weg wie solche, die Community-Funktionen testen. Die 69 getesteten Anforderungen umfassten 109 Test Prozeduren, von denen wiederum 9 als ergebnislos gewertet wurden. Grafik 4.1 zeigt, dass 72% (78 Test Prozeduren) als bestanden gelten, während 22% (24 Test Prozeduren) als durchgefallen gewertet wurden. Nachfolgend werden zunächst die bestandenen Testfälle betrachtet und anschließend Änderungsvorschläge für nicht bestandene Testfälle beschrieben (siehe Unterkapitel 4.2).

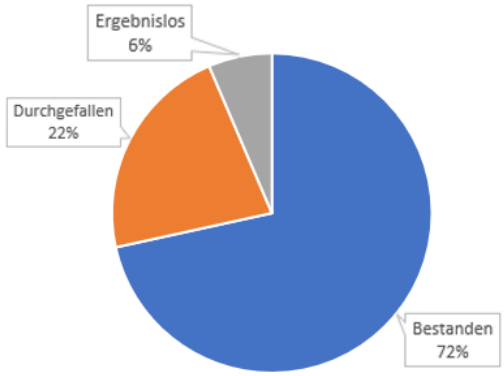


Abbildung 4.1: Darstellung der bestandenen, durchgefallenen und nicht anwendbaren Testfälle der Technischen Richtlinie bei der Untersuchung von OpenWrt. Es wurden insgesamt 69 „Test Procedures“ durchgeführt. Die Testfälle werden in der Grafik ohne Gewichtung dargestellt.

Kondition	Status	Anzahl
MUST - Kriterium	Passed	49
SHOULD - Kriterium	Passed	13
MUST - Kriterium	Failed	12
SHOULD - Kriterium	Failed	8
MUST NOT - Kriterium	Passed	7
MUST - Kriterium	Inc.	4
MUST NOT - Kriterium	Failed	1
MUST NOT - Kriterium	Inc.	1
MAY - Kriterium	Passed	1
MAY - Kriterium	Failed	1
MUST - Kriterium / MAY	Passed	1
MUST - Kriterium / MAY	Inc.	1
RECOMMENDED - Kriterium	Failed	1
SHOULD - Kriterium	Inc.	0
SHOULD NOT - Kriterium	Passed	0
SHOULD NOT - Kriterium	Failed	0
SHOULD NOT - Kriterium	Inc.	0
MAY - Kriterium	Inc.	0
MUST - Kriterium / Should	Passed	0
MUST - Kriterium / Should	Failed	0
MUST - Kriterium / Should	Inc.	0
MUST - Kriterium / MAY	Failed	0
RECOMMENDED - Kriterium	Passed	0

Tabelle 4.1: Darstellung der Anzahl an Testfällen pro Kondition und Status. Die Tabelle wird wie folgt gelesen: 49 Testfälle, welche mit „MUST“ gekennzeichnet sind, wurden bestanden.

Die Durchführung der Technischen Richtlinie an dem mit OpenWrt betriebenen Gerät zeigte, dass OpenWrt die eigenen Ansprüche an Speicherverbrauch und Funktionalität einhalten kann. Das Gerät liefert Kernfunktionen eines Routers und legt dabei besonderes Augenmerk auf die Reduzierung der angebotenen Dienste auf ein Minimum. Die wiederholten Port-Scans mit nmap zeigten, dass lediglich der Webserver, SSH und der DNS/DHCP Dienst über TCP und UDP betrieben werden (siehe Listing 4.1, 4.2)

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times
    will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2020-11-17 11:44 CET as nmap -sSCV
    -T4 -p- -Pn 192.168.1.1
Nmap scan report for OpenWrt.lan (192.168.1.1)
Host is up (0.00038s latency).
Not shown: 65532 closed ports
PORT STATE SERVICE VERSION
22/tcp open ssh Dropbear sshd (protocol 2.0)
53/tcp open domain Cloudflare public DNS
80/tcp open http
MAC Address: B0:95:75:48:F5:EF (Tp-link Technologies)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2773.20 seconds
```

Listing 4.1: Ergebnisse des OpenWrt nmap Scans für alle **TCP**-Ports des **LAN**-Interfaces.

```
# Nmap 7.91 scan initiated Sat Nov 21 15:20:54 2020 as: nmap -n -sUV
    --version-intensity 0 -p- --max-retries 1 -v -oN UDP_SCAN_RESULT.txt
    192.168.1.1
Warning: 192.168.1.1 giving up on port because retransmission cap hit (1).
Nmap scan report for 192.168.1.1
Host is up (0.00047s latency).
Not shown: 65023 open|filtered ports, 511 closed ports
PORT  STATE SERVICE VERSION
53/udp open domain Cloudflare public DNS
MAC Address: B0:95:75:48:F8:02 (Tp-link Technologies)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
# Nmap done at Sat Nov 21 15:33:06 2020 -- 1 IP address (1 host up) scanned in
    732.88 seconds
```

Listing 4.2: Ergebnisse des OpenWrt nmap Scans für alle **UDP**-Ports des **LAN**-Interfaces.

Des Weiteren wurden an keiner Stelle Defizite bezüglich der Testkriterien in der Dokumentation der Software gefunden. Alle in der Technischen Richtlinie geforderten Informationen der Dokumentation konnten ermittelt werden. Neben diesen Ergebnissen sind der vollständig quelloffene Code des Betriebssystems und der vollständige root Zugriff auf das Gerät deutliche Indikatoren dafür, dass dem Nutzer keine Funktionen vorenthalten werden (TR.C.2). Durch die Reduzierung auf die wesentlichen Funktionen eines Routers verringert OpenWrt deutlich die Angriffsoberfläche und spielt somit den Zielen der TR-03148 zu. Die Ergebnisse in „Module B – Private Networks“ unterstützen diese Aussage. Der OpenWrt Router stellt keinen Dienst auf der WAN-Schnittstelle zur Verfügung.

```
# Nmap 7.91 scan initiated Thu Nov 26 18:13:44 2020 as: nmap -sSCV -T4 -Pn -p-
    -oN nmap_wan.txt 192.168.178.115
Nmap scan report for OpenWrt.fritz.box (192.168.178.115)
Host is up (0.012s latency).
All 65535 scanned ports on OpenWrt.fritz.box (192.168.178.115) are closed
    (65494) or filtered (41)
MAC Address: B0:95:75:48:F5:F0 (Tp-link Technologies)
```

```
Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
# Nmap done at Thu Nov 26 19:06:31 2020 -- 1 IP address (1 host up) scanned in
    3167.21 seconds
```

Listing 4.3: Ergebnisse des OpenWrt nmap Scans für alle **TCP**-Ports des **WAN**-Interfaces.

```
# Nmap 7.91 scan initiated Thu Nov 26 19:21:13 2020 as: nmap -sUV
    --version-intensity 0 -p- --max-retries 2 -v -oN nmap_wan_udp.txt
    192.168.178.115
Warning: 192.168.178.115 giving up on port because retransmission cap hit (2).
Increasing send delay for 192.168.178.115 from 0 to 50 due to 11 out of 20
    dropped probes since last increase.
Nmap scan report for OpenWrt.fritz.box (192.168.178.115)
Host is up (0.0027s latency).
All 65535 scanned ports on OpenWrt.fritz.box (192.168.178.115) are open|filtered
    (56258) or closed (9277)
MAC Address: B0:95:75:48:F5:F0 (Tp-link Technologies)

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at
    https://nmap.org/submit/ .
# Nmap done at Thu Nov 26 21:55:05 2020 -- 1 IP address (1 host up) scanned in
    9232.30 seconds
```

Listing 4.4: Ergebnisse des OpenWrt nmap Scans für alle **UDP**-Ports des **WAN**-Interfaces.

So wurde auch das VoIP-Protokoll (vgl. Abschnitt 2.1) nicht in der Standardinstallation mitgeliefert, da dieses für die Funktionalität als Router nicht relevant ist. Ebenfalls konnten die Tests nachweisen, dass OpenWrt international angesehene Standards wie IEEE802.11i erfolgreich inkorporiert.

OpenWrt besteht auch einige weitere Testfälle aufgrund der umfänglichen Informationen und Logs, welche das System für den Nutzer bereitstellt. Das Gerät führt umfassende System- und Kernel-Log Dateien ebenso wie Informationen über verbundene Geräte, aktive und bereitstehende Dienste, Firewall-Funktionen und das System selbst. Die Log-Dateien können über das „Logread“-Programm abgerufen werden, stehen aber nicht als Datei zur Verfügung [85]. Auch werden relevante Informationen wie End-of-Support und Mitteilungen zu Sicherheitslücken klar strukturiert auf der Webseite der Entwickler veröffentlicht. Die Veröffentlichung von Updates, welche Sicherheitslücken beheben, erfolgt dabei stets in wenigen Tagen oder Wochen. Vor allem Module F bis I, welche sich mit Firewall, DNS, DHCP und dem Zurücksetzen des Gerätes beschäftigen, wurden von OpenWrt vollständig bestanden. Dies ist auf die ebenso quelloffenen Komponenten zurückzuführen, welche schon

seit vielen Jahren weiterentwickelt werden und in einigen Bereichen weit verbreitet sind. So nutzt OpenWrt iptables als Firewall und dnsmasq für DNS und DHCP Funktionalität.

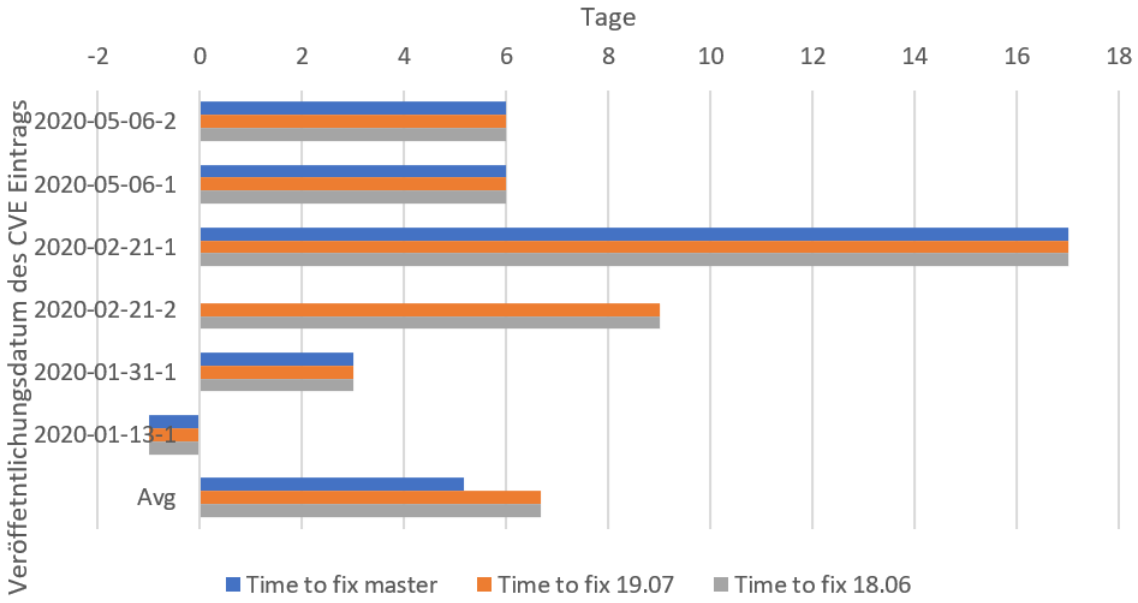


Abbildung 4.2: Benötigte Zeit zur Implementierung und Veröffentlichung von Sicherheitsupdates für OpenWrt im Jahr 2020. Basiert auf dem Veröffentlichungsdatum des CVE-Eintrags und dem Datum des git commits, welcher im Sicherheitshinweis spezifiziert ist.

Einige Defizite bzw. gemischte Ergebnisse liefern die Testfälle des WLAN-Gästenetzes. Da OpenWrt keine klassische Funktionalität liefert, welche automatisch ein WLAN-Netz für Gäste bereitstellt, wurde hier auf die Anleitung in der Dokumentation zurückgegriffen, die ein ähnliches Ergebnis erzielen soll, jedoch dem Nutzer alle Freiheiten lässt, Änderungen zu machen. So ist es kein Garant, dass das Gäste-Netz Nutzer tatsächlich separiert oder, dass ein Nutzer nicht von dort aus auf die Konfiguration des Gerätes zugreifen kann. Die genaue Dokumentation der Ergebnisse kann auch im Ordner „Results“ → TR.X → TP.X.Y abgerufen werden.

4.2 Notwendige Änderungen zum Bestehen der Technischen Richtlinie

Wie bereits im vorherigen Kapitel festgehalten, benötigt OpenWrt nur einige Änderungen, um die Technische Richtlinie 03148 vollumfänglich zu bestehen. Es wird vor allem Wert auf die mit „MUST“ gekennzeichneten Testfälle gelegt. Für Testfälle, die mit „SHOULD“ gekennzeichnet sind wird nachfolgend eine Änderung vorgeschlagen, wenn es sich hierbei um eine simple Anpassung handelt. Darüber hinaus wurde die Funktionalität des Gäste-WLAN

nicht weiter betrachtet, da dieses vom Nutzer vollständig konfiguriert werden muss. OpenWrt bietet keine Möglichkeit ein Gäste-Netzwerk mit einer einzigen Option zu aktivieren. Die vollständige Implementierung einer solchen Funktionalität müsste in Betracht gezogen werden.

Es sind nur einige Änderungen von Nöten, um Modul A vollständig zu bestehen. Der 4. Test des Testfalls TR.A.9 (TP.A.9.4) schlägt fehl, da die Verschlüsselung von WLAN-Netzwerken standardmäßig ausgeschaltet ist. Im initialen Zustand ist die gesamte WLAN-Funktionalität von OpenWrt abgeschaltet. Sie muss zunächst vom Benutzer selbst in den Einstellungen, entweder über das Web-Interface oder SSH, eingeschaltet werden. In der Konfigurationsübersicht des jeweiligen WLAN-Netzes ist das Passwort jedoch erst in einem zweiten Reiter untergebracht. Dort ist standardmäßig „No Encryption (open network)“ angewählt. Diese verzweigte Aufteilung kann dazu führen, dass unerfahrene Nutzer lediglich die ESSID anpassen und daraufhin den Speichern-Button betätigen. Auf diese Weise würde das Netzwerk ohne Passwort initialisiert. Das Verschieben des Passwortfeldes, sowie der Auswahl der Verschlüsselung in den ersten (initialen) Reiter der Übersicht, könnte diesem Problem entgegenwirken. Ebenso könnte die initiale Konfiguration der WLAN-Netzwerkes statt „No Encryption“ stattdessen „WPA2-PSK“ ausgewählt haben. So könnte der Nutzer die Konfiguration nicht speichern ohne ein Passwort einzufüllen. Wenn WPA2 ausgewählt ist, erscheint bei einem unzureichenden Passwort eine Fehlermeldung und die Konfiguration wird nicht gespeichert. Auf diese Weise kann dennoch gezielt ein Netzwerk ohne Passwort erstellt werden, wenn der Nutzer bewusst auf diese Option umgeschaltet hat. Eine noch stärkere Verschlüsselung bietet WPA3. Auf Geräten mit genügend Speicher könnten OpenWrt standardmäßig mit dem zusätzlichen Paket „wpad-openssl“ ausgestattet werden. Auf diese Weise könnte statt WPA3 anstelle von WPA2 eingestellt werden (siehe Abbildung 4.3). Der Nutzer könnte ebenfalls von einem Mechanismus unterstützt werden, welcher die Stärke des WLAN-Passwortes darstellt. Ein ähnlicher Mechanismus wird bereits bei der Prüfung des Geräte-Passwortes eingesetzt und könnte auch im Umfeld des PSK dem Nutzer zusätzliche Hilfestellung bei der Wahl eines Passwortes geben. Dabei sollte der bestehende Mechanismus zur Evaluation des Passwortes allerdings angepasst werden, sodass die Vorgaben der Technischen Richtlinie eingehalten werden.

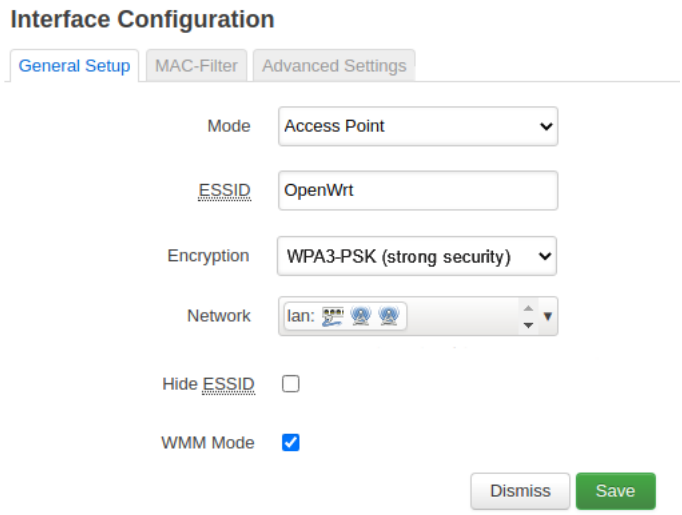


Abbildung 4.3: Mockup der vorgeschlagenen Änderungen des WLAN-Konfigurationsmenüs von OpenWrt.

Ein weiterer Test, welcher während der Durchführung der Technischen Richtlinie scheiterte, ist TR.D.2. Dieser beschreibt, dass der Zugang zur Konfiguration des Gerätes mindestens durch ein Passwort geschützt sein muss, wenn das Gerät sich im initialen oder kundenspezifischen Zustand befindet. Aufgrund der Natur vom OpenWrt als Alternatives Router-Betriebssystem, welches erst nach Erhalt des Gerätes vom Nutzer aufgespielt wird, ist ein Passwort im „factory“-Zustand nicht sinnvoll. Da kein einzigartiges Passwort vergeben werden kann, bevor OpenWrt vom Nutzer eingesetzt wird, würde das Gerät keinen höheren Sicherheitsansprüchen genügen, wenn ein Benutzeraccount mit Passwort voreingestellt wäre. Aufgrund der anhaltenden Nutzung des root Benutzers auf OpenWrt Systemen ist es dem Benutzer allerdings vollkommen freigestellt, diesen Account ohne Passwort zu betreiben. Lediglich ein kleiner Informationstext im Web-Interface erinnert an das Setzen eines Passwortes. Ebenfalls kann über den SSH-Zugang ein bereits gesetztes Passwort gelöscht werden, sodass der Account dann wieder ohne Passwort eingesetzt werden kann. Dies stellt ein hohes Sicherheitsrisiko dar. Jedoch könnte dieses Problem umgangen werden, wenn der Nutzer entweder gezwungen würde, ein Passwort für den root Nutzer zu verwenden, um das Gerät zu initialisieren, oder wenn der Nutzer dazu gezwungen werden würde, einen neuen Nutzeraccount anzulegen und sowohl für den root-Benutzer als auch für den eigenen Nutzeraccount ein Passwort festzulegen. Daraufhin sollte der Nutzer seinen eigenen Account zur Konfiguration des Gerätes nutzen und lediglich auf den root-Benutzer zurückgreifen, wenn höhere Privilegien benötigt werden. Es könnte standardmäßig ein unprivilegierter Nutzeraccount installiert sein und zusätzlich auf ein Programm wie „sudo“ gesetzt werden. Dadurch, dass das „passwd“ Programm durch den root-Nutzer ausgeführt wird, werden alle Überprüfungen des Passwortes übersprungen,

bzw. alle Fehlermeldungen ignoriert. Das „passwd“ Dienstprogramm wird verwendet, um Benutzerpasswörter zu ändern oder zu entfernen. Dieses Vorgehen würde ebenfalls dafür sorgen, dass Kriterien wie TR.D.10 und TR.D.15 kein Problem mehr darstellen. So müsste ein Nutzer zunächst das alte Passwort eingeben, um ein Neues zu wählen. Ebenfalls könnte ein Nutzer gehindert werden, ein schwaches Passwort zu wählen.

Auch wenn es sich dabei nur um ein „SHOULD“-Kriterium handelt, ist HTTPS mit Transport Layer Security eine sicherheitskritische Technologie (TR.D.3) [86]. Ein Entwickler von OpenWrt schlug daher vor eine „technically constrained subordinate Certificate Authority“ (CA) zu etablieren [87]. Diese sollte dann für Subdomänen von „luci.openwrt.org“ Zertifikate ausstellen, welche die Geräte verwenden können (vgl. Abbildung 4.4). Für diesen Ansatz müsste jedoch eine sog. „Root Certificate Authority“ bereit sein, diese „OpenWrt CA“ anzuerkennen. Neben dieser aufwendigen Umsetzung besteht die Möglichkeit selbst-signierte Zertifikate zu verwenden, auch wenn ein Nutzer dann in den meisten Fällen eine Sicherheitswarnung des Browsers akzeptieren muss. Ebenfalls besteht die Möglichkeit den gesamten Verkehr mit SSH zu verschlüsseln. Der Einsatz von HTTPS ist außerdem zu empfehlen, da z.B. der Firefox Browser mit dem „https-only-mode“ den Einsatz von HTTPS erzwingen kann, sodass HTTP-Webseiten nicht mehr aufgerufen werden können [88].

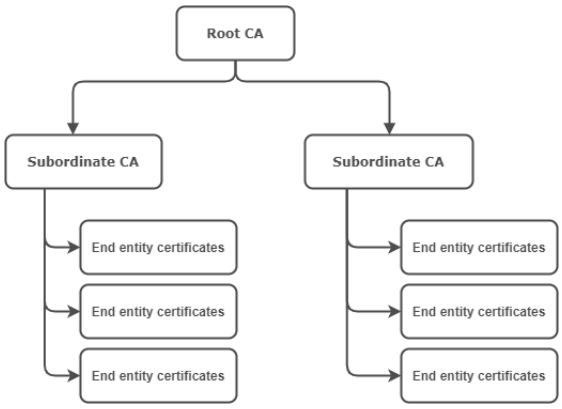
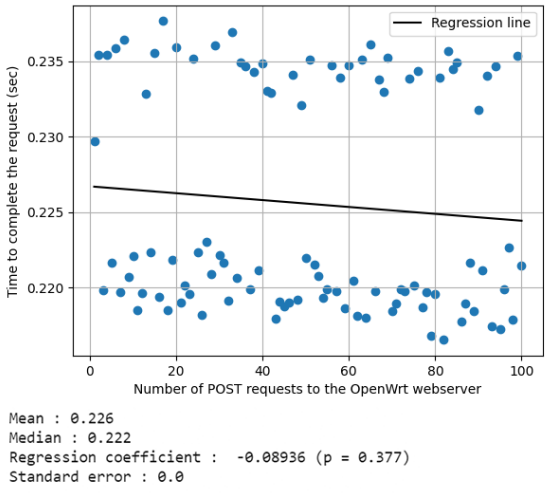


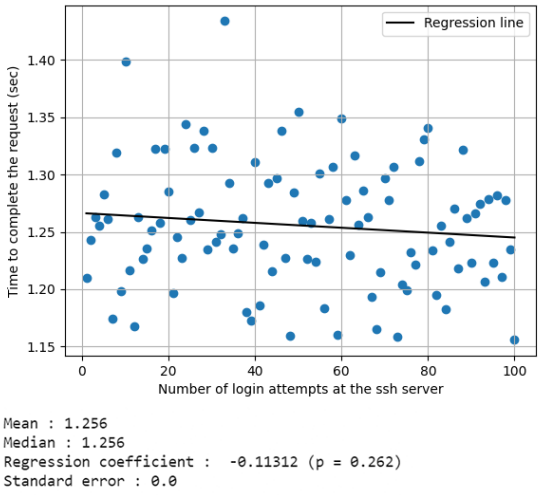
Abbildung 4.4: Vereinfachte Darstellung des Certificate Authority Aufbaus.

OpenWrt zeigt zusätzlich einige Schwächen bei der Implementierung von Sicherheitsmaßnahmen gegen Bruteforce Angriffe (vgl. Abschnitt 2.2.1) auf den Login-Bereich (vgl. Abbildung 4.5) sowie gegen Session-Hijacking Attacken. Da OpenWrt durchaus die fehlgeschlagenen Login-Versuche registriert, wäre ein Zähler die einfachste Option Bruteforce Angriffe auf die Login-Bereiche zu verhindern. Es könnten z.B. eine begrenzte Anzahl an Versuchen zur Verfügung stehen. Nachdem diese abgelaufen sind, muss eine gewisse Zeit gewartet werden, bis ein neuer Versuch unternommen werden kann. Eben-

so könnte ein Zeitlimit zwischen jedem Login-Versuch implementiert werden, sodass ein Angriff verlangsamt wird. Wenn das Passwort ausreichend komplex gewählt ist, so würde dies die Geschwindigkeit und Attraktivität von Bruteforce Angriffen deutlich mindern. Session-Hijacking Angriffe könnten verhindert werden, wenn zusätzlich zu den „anti-cross-site-forgery-request“ (anti-CSFR)–Token (vgl. Abschnitt 2.2.2) der „Session-Timer“ verringert würde. Das kontinuierliche, automatische Updaten der auf der Seite dargestellten Informationen setzt diesen Timer jedoch alle fünf Sekunden zurück. Dieses Verhalten muss unterbunden werden. 300 Sekunden (5 Minuten) für eine Sitzung wären ein geeigneteres Intervall anstelle von den derzeit eingesetzt 3600 Sekunden (60 Minuten).



(a) Teilbild 1: Antwortzeiten des Webservers



(b) Teilbild 2: Antwortzeiten des SSH-Servers

Abbildung 4.5: Antwortzeiten des Web-Servers und des SSH-Servers bei wiederholten Login-Versuchen. Die Regressionslinie zeigt, dass die Antwortzeiten konstant bleiben bzw. sogar tendenziell geringer werden. Ebenso sind der Durchschnitt, der Median, der Regressionskoeffizient und der Standardfehler dargestellt.

Abschließend deckte die Durchführung der Technischen Richtlinie noch einen weiteren Schwachpunkt des OpenWrt Betriebssystems auf. Die Testfälle TR.E.5 bis TR.E.8 wurden alle nicht bestanden, da es keinen automatischen Authentifizierungsmechanismus gibt, welcher Firmware-Updates prüft. Dem Nutzer werden lediglich signierte SHA256 Hash-Werte des Firmware-Updates zur Verfügung gestellt, sodass die Authentizität und Integrität der Datei vom Nutzer geprüft werden muss.

> „ [...] while release image files are usually signed by one or more developers with detached GPG signatures to allow users to verify the integrity of installation files. [...] Note that not every file is signed individually but that we’re signing the sha256sums or - for repositories - the Packages files to establish a chain of trust: The SHA256 checksum will verify the integrity of the actual file while the signature will verify the integrity of the file containing the checksums. [70]“

Dieser Ansatz bietet natürlich nur die geforderten Schutzziele, wenn ein Nutzer tatsächlich die Authentizität und Integrität der sha256sums Datei prüft und anschließend den darin enthalten Hash-Wert mit dem der heruntergeladenen Datei vergleicht. Ebenso wie der OPKG Paket Manager könnte auch der Firmware-Update-Mechanismus auf die usign Ed22519 Signaturen zurückgreifen oder eine GPG-Signatur der Entwickler tragen. Eine automatische Verifizierung der Signatur über das Internet, mit entsprechenden Sicherheitsmaßnahmen, wäre dann möglich. In den Fällen, in denen das Gerät keine Internetverbindung aufweist, könnte dann auf die SHA256 Hash-Werte zurückgefallen werden. Durch das beschriebene Vorgehen könnte das Gerät TR.E.5 bis TR.E.8 bestehen sowie den Nutzern mehr Sicherheit und Nutzerfreundlichkeit bieten.

In einigen Fällen lässt sich keine sinnvolle Lösung finden, die für ein Projekt wie OpenWrt geeignet ist. So auch bei TR.D.24, welches fordert, dass dem Nutzer eine Nachricht auf dem Gerät angezeigt wird, wenn eine neue Firmware verfügbar ist. Für diese Anforderung müsste das Gerät mit dem Internet verbunden sein und zudem müssten von Seiten der OpenWrt Entwickler ein Update-Server zur Verfügung gestellt werden. Dies würde Kosten auf Seiten der freiwilligen Entwickler sowie eine größere Angriffsoberfläche auf Seiten der Nutzer verursachen. Eine Anmeldung beim E-Mail Newsletter der Entwickler wäre die simpelste Möglichkeit um über neue Versionen sowie Sicherheitslücken informiert zu bleiben.

4.3 Ergebnisse der statischen Code-Analyse sowie Gegenüberstellung mit ausgewählten Ergebnissen des Home Router Security Reports 2020

Im Rahmen dieser statischen Code-Analyse durch das „Firmware Analysis and Comparison Tool “ des FKIE wurden sieben verschiedene quelloffene Router-Firmware Alternativen analysiert. Dabei waren fünf Fragen von besonderem Interesse.

- Wann wurde das letzte Update für das Gerät veröffentlicht?
- Welches Betriebssystem wird verwendet und wie viele kritische Schwachstellen sind für dieses bekannt?
- Welche vorbeugenden Maßnahmen gegen Exploits werden eingesetzt und wie häufig sind diese aktiviert.
- Ist privates kryptografisches Schlüsselmaterial enthalten?
- Können hartkodierte Login-Daten und bekannte Passwörter in dem Firmware-Abbild gefunden werden?

FACT konnte während der Analyse erfolgreich 92,73% der Daten aus den Firmware-Abbildern extrahieren. Bei der gesamten betrachteten Firmware wurde durch Analyse von Metadaten eine MIPS 32-Bit Architektur mit „big-endian“ Byte-Reihenfolge festgestellt. Dies hat zwar keinen direkten Einfluss auf die Sicherheit eines Gerätes, jedoch ist diese Architektur nicht quelloffen und die Entwicklung ist in den letzten Jahren ins Stocken geraten [89]. Für die Analyse der „Critial Vulnerabilities and Exposures“ (CVE) (vgl. Abschnitt 2.5.2) wurde aufgrund einiger Fehler in FACT nicht das Ergebnis der automatischen Analyse gewählt. Stattdessen wurden die Ergebnisse durch die Webseite www.cvedetails.com, welche wiederum auf die Daten der „National Vulnerability Database“ der US-Regierung, zugreift, bereitgestellt. Da cvedetail.com ausschließlich CVSS v2 Bewertungen (siehe Abschnitt 2.5.2) bereitstellt, wurden einzig diese für die Analyse verwendet. Um Vergleichbarkeit mit den Ergebnissen des FKIE zu gewährleisten wurden lediglich CVE-Einträge mit einem Schweregrad von „Hoch“ (vgl. Tabelle 2.3) gezählt.

4.3.1 Vergangene Tage seit der letzten Veröffentlichung eines Firmware-Updates

In diesem Abschnitt soll evaluiert werden, wann für die betrachteten Firmware-Abbilder das letzte Mal eine neue Version seit dem 24.12.2020 veröffentlicht wurde. Alle Abbilder des Firmware-Corpus spezifizierten das Veröffentlichungsdatum im Dateinamen selbst oder auf der jeweiligen Webseite. Dieses Kriterium wurde untersucht, da es die Bereitschaft der Entwickler andeutet, ihr Projekt regelmäßig mit Funktions- und Sicherheitsupdates zu unterstützen. Eine neuere Version bedeutet also zumeist, dass weniger sicherheitsrelevante Lücken bekannt sind und das System sicherer ist. Da die Unterstützer der quelloffenen Projekte in vielen Instanzen auf weitere Software zurückgreifen und auch diese Updates erfährt, ist es wahrscheinlich, dass Firmware bekannte Lücken hat, wenn diese längere Zeit nicht erneuert wurde.

Grafik 4.6 zeigt, dass für fünf von sieben untersuchten Firmware-Abbildern in den letzten 365 Tagen eine neue Version veröffentlicht wurde. Aufgrund des Ausreißers in den erhobenen Daten wird im Folgenden der Median statt des Mittelwertes betrachtet. Es ergibt sich, dass die Router-Betriebssysteme nach Median-Berechnung alle 83 Tage und im Schnitt alle 309 Tage eine neue Version erhalten. Ebenfalls muss erwähnt werden, dass bei der Veröffentlichung einer neuen Version meist alle von dem jeweiligen Projekt unterstützen Geräte diese neue Version zur Verfügung gestellt bekommen. So werden bei einer neuen Version von OpenWrt alle ca. 1700 Geräte von diesem neuen Update unterstützt und erfahren somit alle Sicherheitsupdates, die bereitgestellt werden. Dies steht im Gegensatz zu etablierten Herstellern von Routern, welche oft pro Gerät eine eigene Version entwickeln. Gargoyle Router Management wurden nicht in den letzten 365 Tagen erneuert und das Tomato Be-

triebssystem hat in den letzten 1480 Tagen kein Update erfahren. Der Zyklus von 83 Tagen ist höher als der Update-Zyklus von Desktop- oder Server-Betriebssystemen, jedoch noch im Rahmen der 90 Tage, welche normalerweise das Zeitfenster darstellen, in dem Entwickler Zeit haben auf Sicherheitslücken und Probleme zu reagieren („responsible disclosure“) [90]. Darüber hinaus muss besonders darauf hingewiesen werden, dass in manchen Fällen ein Paketmanager (vgl. Abschnitt 2.3) zur Verfügung steht, über welchen Updates für Pakete während der Laufzeit installiert werden können. Somit sind Updates der Firmware nur notwendig, um Kernfunktionalität zu erweitern oder Fehler in dieser zu beheben, sowie um den Kernel zu aktualisieren. Nur eine von acht bisher veröffentlichten Sicherheitslücken im Jahr 2020 konnte ausschließlich durch ein Update auf eine neuere Version von OpenWrt behoben werden, wobei alle weiteren durch ein einfaches Update des betroffenen Paketes nachgebessert werden konnten [91]. In proprietärer Firmware ist ein Paketmanager für die Installation von zusätzlicher Software und für das Herunterladen von Updates in den meisten Fällen nicht vorhanden. Verglichen mit den Ergebnissen des „Home Router Security Reports 2020“ zeigt sich, dass für die quelloffenen Betriebssysteme häufiger neue Versionen veröffentlicht werden. Wenn man die analysierten Abbilder als Gruppe betrachtet, dann schneidet diese vergleichsweise gut ab. Einzig Tomato fällt als Ausreißer heraus. Lediglich ASUS, AVM und Netgear, als Hersteller von handelsüblichen Routern, können mithalten.

Ebenso wie im „Home Router Security Report 2020“ festgestellt, muss zusätzlich beachtet werden, dass alle betrachteten Produkte kleinere Updates auch über die Geräte selbst zu Verfügung stellen könnten, sodass die aktuellste Version nicht im Internet veröffentlicht wird. Darüber hinaus handelt es sich bei den hier festgestellten Daten ausschließlich um eine Momentaufnahme, die keine Aussagekraft darüber hat, ob regelmäßig Updates bereitgestellt werden, oder ob diese Sicherheitslücken überhaupt adressieren [51].

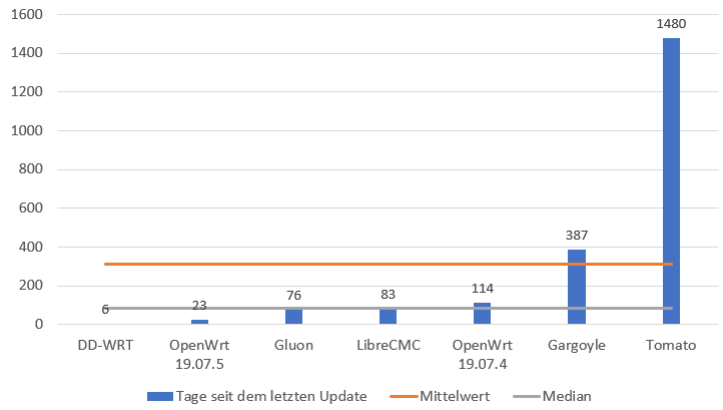


Abbildung 4.6: Vergangene Tage seit der letzten Aktualisierung der betrachteten Firmware. Seit dem letzten Update von DD-WRT ist am geringsten Zeit vergangen. Für Tomato ist seit 1480 Tagen keine neue Version erschienen. (Stand: 30.12.2020)

4.3.2 Betriebssysteme

Da es sich bei allen analysierten Firmware-Abbildern um quelloffene Projekte handelt, ist es nicht verwunderlich, dass der Linux-Kernel dominant vertreten ist. Der Linux-Kernel, welcher 1991 von Linus Tovalds entwickelt wurde und seither stetig weiterentwickelt wird stellt einen der am häufigsten genutzten Betriebssysteme für IoT Geräte dar [92]. Die geringe Größe des Kernels, der große Funktionsumfang und die umfangreiche Dokumentation und Verbreitung sind für eine community-getriebene Entwicklung auf speicher- und rechenleistungslimitierten Geräten wie z. B. Heim-Routern gut geeignet. Grafik 4.7 zeigt, dass alle untersuchten Projekte einen Linux Kernel verwenden. Dieser Trend deckt sich ebenfalls mit den Ergebnissen des „Home Router Security Reports“ des FKIE. In den untersuchten Produkten des Verbrauchermarktes wurde Linux in 91% der Fälle verwendet [51, p. 2].

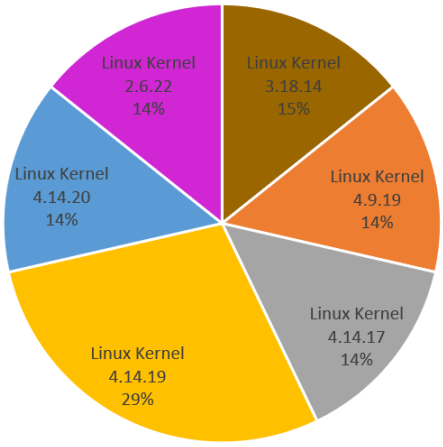


Abbildung 4.7: Verwendete Linux Kernel der betrachteten Firmware.

Aufgrund der unzureichenden Ergebnisse der FACT-Analyse bezüglich der vorhandenen CVE-Einträge für die verwendeten Linux-Kernel wurden die Ergebnisse in diesem Fall direkt über „www.cvedetails.com“ abgerufen. FACT erstellt zunächst eine „Common Platform Enumeration“ (CPE) der Software Version und stellt mit dieser CPE eine Anfrage an die „National Vulnerability Database“. Da die zurückgegebenen Ergebnisse allerdings auch Schwachstellen beinhalten, welche nur für bestimme Geräte mit der jeweiligen Linux-Kernel Version gelten, wurden die jeweiligen Schwachstellen des Kernels über die Website „cvedetail.com“ abgefragt. Bei einer Stichprobe der von FACT gelieferten CVE-Einträge sind verschiedene Einträge aufgefallen, welche z.B. nur für bestimmte IoT-Geräte wie Smartwatches eingetragen sind. Cvedetail nutzt ebenfalls die „National Vulnerability Database“, stellt jedoch noch zusätzliche Informationen und Statistiken bereit. Auf diese Art wurde

sichergestellt, dass die betrachteten Schwachstellen spezifisch für den Kernel sind und nicht für ein bestimmtes Gerät, welches diesen Kernel nutzt. Da nicht alle eingetragenen CVEs eine direkte Bedrohung darstellen, wurden die Ergebnisse weiter eingeschränkt. So wurden lediglich solche CVEs betrachtet, welche mit einen CVSS2 Wert von sieben oder höher eingestuft wurden. Wie Grafik 4.9 zeigt, stehen für alle betrachteten Geräte einige CVE Einträge des Linux Kernels zur Verfügung. Ebenfalls kann man sehen, dass der in DD-WRT verwendete Kernel mehr CVE-Einträge hat als der von Gargoyle Router Management, obwohl bei DD-WRT die geringste Zeit seitdem letzten Firmware Update vergangen ist. Tomato schneidet erneut am schlechtesten ab. Grafik 4.8 zeigt zusätzlich, dass für zwei der sechs verschiedenen Linux Kernel schon seit einigen Jahren keine Sicherheitsupdates entwickelt werden. Sowohl der von Tomato verwendete Kernel, 2.6.22, als auch Linux Kernel 3.8.14, welcher von DD-WRT verwendet wird, werden nicht mehr mit Updates unterstützt. Dies spiegelt sich auch in der hohen Anzahl CVE-Einträge wider (siehe Abbildung 4.9).

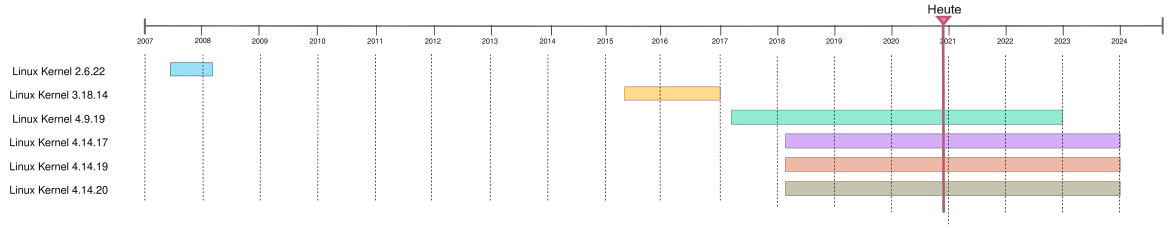


Abbildung 4.8: Stellt jeweils den Zeitraum von Veröffentlichung bis zum Ende der Entwicklerunterstützung für alle gefundenen Linux Kernel dar. Der Kernel 4.14.19 wurde in zwei Firmware-Abbildern genutzt.

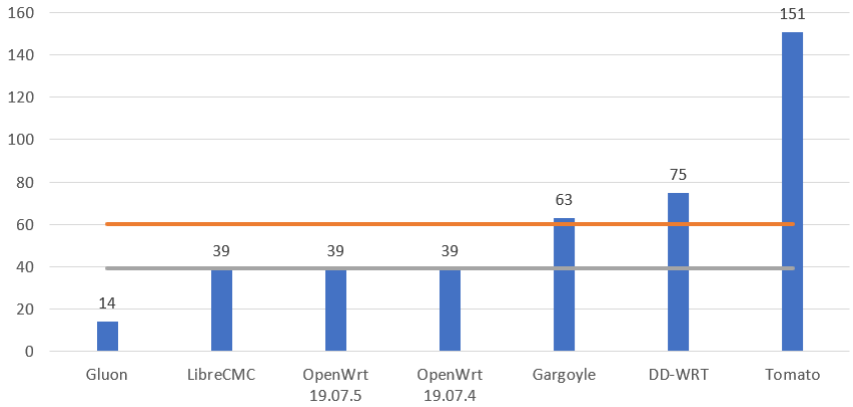


Abbildung 4.9: Anzahl der gefundenen CVE-Einträge pro Firmware mit einer CVSS-Einschätzung von sieben oder höher.

Die Ergebnisse sind aufgrund der unterschiedlichen Beschaffung sowie der fehlenden CVSS3 Werte nicht wirklich mit denen des „Home Router Security Reports 2020“ vergleichbar. Jedoch kann man sagen, dass die quelloffenen Router-Betriebssysteme mehrheit-

lich modernere Linux-Kernel Versionen nutzen. Lediglich zwei der betrachteten Firmware-Abbilder nutzen einen Kernel, der nicht mehr unterstützt wird. Der „Security Report“ gibt an, dass ein Drittel der betrachteten Geräte einen Kernel vor Version 3 nutzen und lediglich ca. 22% einen aktuellen Kernel der 4. Version [51, p. 8]. Im Gegensatz dazu nutzen ca. 70% der betrachteten quelloffenen Software-Projekte einen Linux-Kernel der Version 4.9.19 oder höher (siehe Abbildung 4.8).

Im Gegensatz zu den Ergebnissen des „Security Reports“ können falsch positive Ergebnisse bei der Erkennung der Kernel Version beinahe ausgeschlossen werden, da diese ebenfalls von den Entwicklern auf der Webseite oder in den Veröffentlichungsdokumenten der jeweiligen Version veröffentlicht wird. Jedoch besteht die Möglichkeit, dass die Entwickler eigene Korrekturen für Sicherheitslücken des Kernels entwickeln und veröffentlichen. Dies ist bei dieser Art community-getriebener Entwicklung nicht unwahrscheinlich, da hier keine Entwickler bezahlt werden müssen, welche zusätzlich zu ihren anderen Aufgaben für das Beheben von Sicherheitslücken im Kernel eingesetzt werden. Ebenfalls ist es möglich, dass aufgrund der uneindeutigen CPE-Spezifikation einige CVE-Einträge nicht von „cvedetails.com“ gelistet werden [51, p. 7].

4.3.3 Härtungsmaßnahmen

FACT ist in der Lage die folgenden Exploit Mitigationsmaßnahmen (siehe Abschnitt 2.5.2) zu identifizieren:

- Stack Canary
- FORTIFY_SOURCE
- NX
- PIE
- RELRO

Sowohl RELRO als auch das NX-Bit werden vermehrt bei den quelloffenen Router-Betriebssystemen eingesetzt (siehe Abbildung 4.10). Außer Tomato nutzen alle der betrachteten Firmwares zu beinahe 100% das NX-Bit. Mit Ausnahme von Tomato und DD-WRT nutzen im Schnitt ca. 50% aller ausführbarer Dateien der Firmware-Abbilder RELRO. Tomato und DD-WRT setzen hingegen kaum auf RELRO. PIE wird andererseits im Schnitt zu ca. 40% genutzt. Tomato scheint bevorzugt auf PIE zu setzen (siehe Abbildung 4.11). Die Nutzung von Stack Canaries und FORTIFY_SOURCE verhält sich pro Firmware nahezu identisch. Gargoyle Router Management, LibreCMC und OpenWrt nutzen es bei ca. 19% aller Dateien, Gluon bei ca. 8%, während DD-WRT und Tomato beinahe vollständig auf diese Techniken verzichten. Die Verbreitung von PIE ist vergleichbar mit

den Ergebnissen der FKIE Veröffentlichung (siehe Abbildung 4.10) [51, p. 15]. Ebenso wie im „Security Report“ berichtet, nutzen auch die quelloffenen Betriebssysteme annähernd alle vollumfänglich NX-Bits. Dies lässt sich leicht durch den vergleichsweise guten Schutz bei infinitesimalen Geschwindigkeitseinbußen erklären. Die Daten des FKIE zeigten, dass RELRO nur selten von allen Herstellern eingesetzt wird mit Ausnahme von AVM. Dem steht eine Nutzung von ca. 50% bei den freien Firmware-Produkten gegenüber. Ebenso wie die betrachtete Firmware der Markthersteller, wird nur selten auf Stack Canaries und FORTIFY_SOURCE gesetzt. Obwohl Stack Canaries keinen merkbaren Einfluss auf die Geschwindigkeit eines Systems hat, scheint diese Technik nur bei wenigen Dateien angewendet worden zu sein. Es könnte sich hierbei um systemkritische Dateien handeln. Dies gilt ebenso für die FORTIFY_SOURCE Option (siehe Abbildung 4.11).

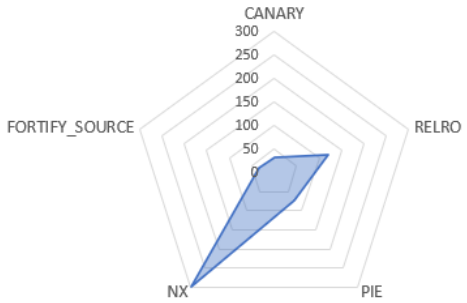


Abbildung 4.10: Netzdiagramm (Kiviat-Diagramm, Radardiagramm) der verwendeten Härtungsmaßnahmen. Es werden alle Firmware-Abbilder gemeinsam dargestellt. NX, RELRO und PIE werden am häufigsten genutzt. Stack Canaries und FORTIFY_SOURCE wird kaum eingesetzt.

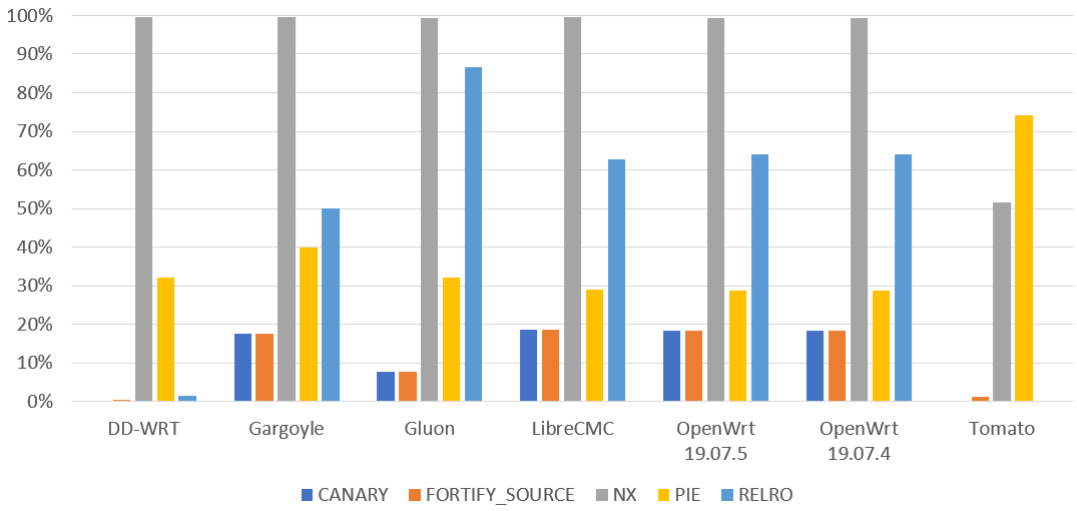


Abbildung 4.11: Säulendiagramm der verwendeten Härtungsmaßnahmen nach Analyse der FACT Daten. Pro Firmware sind Stack Canaries, FORTIFY_SOURCE, NX, PIE und RELRO dargestellt.

Zusammenfassend kann man sagen, dass vor allem auf NX und RELRO für den Großteil der Dateien gesetzt wird. PIE, Stack Canaries und FORTIFY_SOURCE wird nur bei wenigen ausführbaren Dateien genutzt.

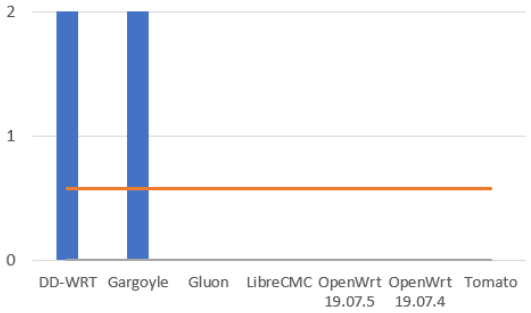
4.3.4 Privates Schlüsselmaterial

Wenn private kryptographische Schlüssel in den Firmware-Abbildern enthalten sind, so haben diese keine Sicherheitsfunktion mehr. Um die korrekte Funktionalität zu gewährleisten, in dem Fall, dass private Schlüssel enthalten sein müssen, so sollten die Vorgaben der OWASP eingehalten werden:

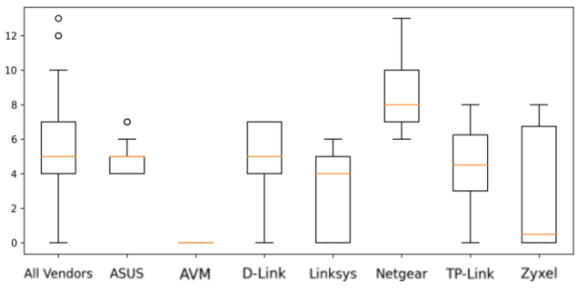
> "Do not hardcode secrets such as passwords, usernames, tokens, private keys or similar variants into firmware release images. This also includes the storage of sensitive data that is written to disk. If hardware security element (SE) or Trusted Execution Environment (TEE) is available, it is recommended to utilize such features for storing sensitive data. Otherwise, use of strong cryptography should be evaluated to protect the data. If possible, all sensitive data in clear-text should be ephemeral by nature and reside in a volatile memory only [93]."

Die Einhaltung dieser Vorgaben ist jedoch deutlich erschwert, wenn die Firmware nicht spezifisch für ein Gerät geschrieben ist. Ebenso stehen den Entwicklern der quelloffenen Firmware nicht alle Entwicklerwerkzeuge der Hersteller zur Verfügung um z.B. auf ein „Hardware Security Element" zuzugreifen. Zugleich wird für den Zugriff in einigen Fällen ein physischer Zugang zu dem Gerät benötigt.

Trotz dieser Probleme konnte FACT nur aus DD-WRT und Gargoyle Router Management private Schlüssel extrahieren. Bei beiden Betriebssystemen wurden jeweils ein Pkcs8PrivateKey sowie ein SSLPrivateKey gefunden. Da PKCS#8 ein Container-Format für private kryptographische Schlüssel ist, kann man ohne weitere Nachforschung nicht bestimmen, welchen Nutzen diese Schlüssel für die Systeme haben. Die gefundenen SSL-Schlüssel dienen vermutlich dazu den vom Webbrowser an den Webserver gesendeten Session-Key zu entschlüsseln [94]. Es lässt sich also vermuten, dass DD-WRT und Gargoyle Transport Layer Security verwenden, jedoch kann ein Man-in-the-Middle Angriff einfach durchgeführt werden, wenn der private SSL Schlüssel bekannt ist [95]. Die genauen Details der Implementierung und Nutzung der gefundenen Schlüssel ist jedoch vollkommen unbekannt. Es könnte sich ebenso um ungenutztes oder veraltetes Material handeln. Darüber hinaus könnte der SSL Schlüssel auch nur für die initiale Konfiguration des Gerätes genutzt werden, um danach durch einen neuen ersetzt zu werden.



(a) Teilbild 1: Quelloffene Betriebssysteme



(b) Teilbild 2: Ergebnisse der FKIE Untersuchung

Abbildung 4.12:
Teilbild 1: Anzahl der privaten Schlüssel in den untersuchten quelloffenen Betriebssystemen. Lediglich in DD-WRT und Gargoyle wurden private Schlüssel gefunden.
Teilbild 2: Anzahl der privaten Schlüssel in der vom FKIE untersuchten Firmware. Außer bei AVM wurden bei allen Hersteller private Schlüssel gefunden [51, p. 17].

4.3.5 Angelegte Benutzeraccounts

Diese Analyse dient dazu hartkodierte Accountinformationen in der untersuchten Firmware zu finden. FACT extrahiert dazu die Daten aus der „/etc/shadow“ und „/etc/passwd“ Datei. Diesen Dateien speichern Informationen zu allen Nutzeraccounts, welche auf dem System angelegt sind. Dazu gehören unter anderem der Nutzername, das Passwort, die Nutzerrechte und weitere Informationen der Nutzer. Das Passwort, welches in der „/etc/shadow“ Datei gespeichert wird, liegt in Hash-Form vor. FACT nutzt eine Passwortliste mit häufig genutzten Passwörtern und das Programm „john“, um das Passwort im Klartext darzustellen. Problematisch sind bereits angelegte Nutzeraccounts vor allem, wenn diese nicht geändert oder abgeschaltet werden können. Ebenso bergen sie das Risiko, dass ein unerfahrener Nutzer diesen Account benutzt, ohne ein neues Password für den Account festzulegen. Auf diese Art kann ein Angreifer sehr einfach auf die Konfiguration des Gerätes zugreifen.

Die Analyse der quelloffenen Firmware zeigt, dass lediglich Gargoyle Router Management einen bereits angelegten Nutzeraccount mit schwachem Passwort ausweist. Im Test des FKIE wurden auf 50 Geräten (40%) vom Hersteller angelegte Accounts gefunden [51, p. 19]. Da es sich bei dem Befund des Gargoyle Betriebssystems allerdings um den root Account handelt, ist es nicht unwahrscheinlich, dass der Nutzer nach einmaliger Eingabe des Passwortes „password“ ein neues Passwort wählen muss. In diesem Falle bietet Gargoyle Router Management nicht mehr Sicherheit als OpenWrt, bei welchem der root Account ohne Passwort initialisiert ist. In dieser Instanz ist es umso wichtiger, dass der Nutzer auf das Risiko ausreichend hingewiesen wird, bzw. aufgefordert wird, dass Passwort zu ändern.

Kapitel 5

Diskussion

5.1 Limitationen

Eine mögliche Limitation bei der Durchführung der Technischen Richtlinie ist die Testumgebung. Besonders die double NAT Konfiguration (vgl. Abschnitt 3.2) ist nicht optimal zur Durchführung der Technischen Richtlinie. Der beschriebene Aufbau kann dazu führen, dass einige Ergebnisse nicht zuverlässig angegeben werden können, vor allem wenn der Zugriff auf die Konfiguration des ersten Routers oder des Modems nicht gegeben ist. So könnten einige Pakete nicht zum eigentlichen OpenWrt Router zugstellt werden, wenn diese bereits von der vorgelagerten Firewall abgefangen wurden. Ebenfalls hätte ein zusätzlicher Testrechner und ggf. weitere Router den Testvorgang weiter beschleunigt, indem nmap-Scans über Nacht oder parallel ausgeführt hätten werden können. Ebenso hätte dies die Durchführung einiger zusätzlicher Tests erlaubt, welche nun als „inconclusive“ markiert wurden, da nicht genug Systeme zur Verfügung standen, um die vorgegebene Testprozedur durchzuführen. Des Weiteren musste in diesem Falle das „Conformance Statement“ der Technischen Richtlinie vom Tester selbst ausgefüllt werden, statt vom Hersteller oder Entwickler. Dies stellt eine sehr einseitige Betrachtung des Gerätes durch den Tester dar. Auch könnte hier eine gewisse Voreingenommenheit unterstellt werden, da der Tester ggf. gewisse Ergebnisse bereits erwartet. Anschließend muss an dieser Stelle ebenso betrachtet werden, dass die Möglichkeit besteht, bereits bei der Anfertigung des „Conformance Statements“ etwas zu übersehen, wodurch Ergebnisse der TR verfälscht werden können.

Eine weitere Limitation zeigt sich im Zusammenspiel von OpenWrt und der Technischen Richtlinie selbst. OpenWrt ist zwar durchaus für Heim-Router und Router aus dem SOHO-Bereich gedacht, jedoch müssen die Nutzer schon für die Installation einige technische Grundkenntnisse vorweisen, sowie überhaupt von der Möglichkeit wissen. So wird OpenWrt durch die TR an einigen Stellen für die Umsetzung von Funktionen bestraft, welche für den durchschnittlichen Nutzer von OpenWrt vielleicht geeignet sind. Darüber hinaus darf die TR nur als ein Mittel von vielen gesehen werden, um die Sicherheit solcher komplexen Systeme zu untersuchen. Es ist vielmehr das Ziel der Technischen Richtlinie ein

Grundmaß an Sicherheit auf Heim-Routern zu schaffen, statt in jeder Hinsicht sichere Router. Aus diesem Grunde geht die Richtlinie zu Teilen tiefer in Details hinein als anderswo, wo die Existenz einer Funktion wichtiger ist als die perfekte Implementierung. Auch wirkt die Technische Richtlinie nicht direkt automatisierten Angriffen wie Heartbleed, Sambacry oder BCMUPnP entgegen [96, 96, 97]. Die TR sorgt allerdings für eine verringerte Angriffsoberfläche und viele Maßnahmen, die den Nutzer dabei unterstützen sollen, sein Gerät sicherer zu betreiben. Schon sicherere Login- und WLAN-Passwörter können einige Angriffe verlangsamen und uninteressant machen. Die Technische Richtlinie sollte also lediglich als Teil des Weges zu sichereren Geräten verstanden werden. Weitere Techniken zum Testen von Software sollten dennoch weiter eingesetzt werden, um einen weiteren Blick auf die IT-Sicherheitslage zu bekommen.

Zu den genannten Limitationen kommt zusätzlich eine zeitliche Komponente. Die Durchführung anhand von OpenWrt war im gesetzten zeitlichen Rahmen machbar, jedoch wäre es dennoch interessant gewesen, eine möglichst vollständige Durchführung der TR anzustreben. OpenWrt hätten durch den Paket-Manager sämtliche zusätzlichen Komponenten geboten, um jedes Modul der TR vollständig zu testen. Dies hätte als konzeptioneller Beweis weitere Einblicke in die Möglichkeiten und Limitationen der Technischen Richtlinie und auch OpenWrt gegeben. Ebenso interessant wie die Ergebnisse von OpenWrt bei der TR wäre ein Vergleich mit dem Resultat von anderen handelsüblichen Routern. Der Zertifizierungsprozess hat jedoch erst vor kurzem begonnen und die Daten der bisher durchgeführten Testdurchläufe stehen nicht für die Öffentlichkeit zur Verfügung. So wird es noch eine Weile dauern, bis Vergleichswerte verfügbar sind.

Neben den Limitationen bezüglich der Technischen Richtlinie, müssen auch einige Einschränkungen bei der Durchführung der statischen Code-Analyse aufgezeigt werden. Die betrachteten Firmware Abbilder hätten schneller und ausführlicher analysiert werden können, wenn mehr Zeit und mehr Rechenkapazitäten zur Verfügung gestanden hätten. Neben den gewählten Metriken liefert FACT noch weitere interessante Plug-ins. Ebenso kann nur eine eingeschränkte Vergleichbarkeit mit den Ergebnissen des „Home Router Security Reports 2020“ dargestellt werden. Dies liegt unter Anderem an der geringen Anzahl an untersuchter Firmware. Im Gegensatz zu den Herstellern, welche im FKIE Report betrachtet wurden, wird bei der quelloffenen Firmware in den meisten Fällen eine Codebasis für alle unterstützen Geräte kompiliert, sodass es die Ergebnisse nicht beeinflusst hätte, wenn Firmware für verschiedene Prozessorinstruktionssätze vertreten gewesen wäre. Ebenfalls wurden in dieser Analyse bereits die bekanntesten quelloffenen Alternativen betrachtet, welche gefunden werden konnten. Ein weiterer Punkt, welcher die Vergleichbarkeit mit dem „Home Router Security Report 2020“ betrifft, war die Analyse der veröffentlichten CVE-Einträge pro verwendetem Linux-Kernel. So lassen sich diese Werte zwar nicht direkt vergleichen,

jedoch geben die Angaben des FKIE Reports und der in dieser Arbeit aufgeführten Analyse einen Einblick in die Lage der IT-Sicherheit der betrachteten Geräte.

5.2 Implikationen und zukünftige Forschung

Die Ergebnisse zeigen, dass die Technischen Richtlinie durchaus auch für quelloffenen Router-Betriebssysteme geeignet ist. Nur aufgrund der relativ guten Ergebnisse von OpenWrt kann man jedoch nicht sagen, dass es sich hier von einem IT-Sicherheitsstandpunkt aus um ein sicheres System handelt. Lediglich ein Mindestmaß an Sicherheit kann festgestellt werden und für das vollständige Bestehen der TR sind noch einige Änderungen notwendig. Ebenso wurden nur einige Tests mit FACT durchgeführt, sodass auch in dieser Hinsicht nicht von einem vollständig nachgewiesen sicheren System gesprochen werden darf. Es handelt sich hier nur um Indikatoren und Momentaufnahmen. FACT selbst erweist sich jedoch als geeignetes Programm, um mit wenig Aufwand und geringen technischen Fähigkeiten eine statische Code-Analyse an Firmware durchzuführen.

Zukünftig wäre ein Vergleich verschiedener Geräte anhand der Technischen Richtlinie von Interesse. Ebenso wäre die Durchführung an anderen quelloffenen Router-Betriebssystemen sowie eine Gegenüberstellung interessant. Wie bereits erwähnt wäre es zusätzlich eine Möglichkeit die TR vollständig anhand von OpenWrt durchzuführen und darüber hinaus mithilfe des „Software Developer Kits“ (SDK) der OpenWrt-Entwickler eine Version bereitzustellen, welche alle Anforderungen der TR erfüllt. Weiterhin kann eine sinnvolle Erweiterung der Technischen Richtlinie um mehr Testfälle in Betracht gezogen werden. Auf diese Weise könnte mehr Funktionalität geprüft werden oder bereits geprüfte Funktionen eingehender getestet werden. Wenn die Verbreitung der TR fortgeschritten ist und mehrere Geräte eine Zertifizierung erhalten haben, so wäre eine Marktanalyse interessant. So könnte die Auswirkung der TR auf die Hersteller und auf die Wahrnehmung der Kunden betrachtet werden.

Literaturverzeichnis

[1] Bundesamt für Sicherheit in der Informationstechnik, "Die Lage der IT-Sicherheit in Deutschland 2020." https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2, 2020. [Abgerufen am: 02.11.2020].

[2] Statistisches Bundesamt, "Ausstattung privater Haushalte mit Internetzugang und Breitbandanschluss im Zeitvergleich." https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/Ausstattung-Gebrauchsgueter/Tabellen/zeitvergleich-ausstattung-ikt.html, 2020. [Abgerufen am: 30.10.2020].

[3] S. Triantopoulou, D. Papanikas, and P. Kotzanikolaou, "An Experimental Analysis of Current DDoS attacks Based on a Provider Edge Router Honeynet," in *2019 10th International Conference on Information, Intelligence, Systems and Applications (IISA)*, pp. 1–5, IEEE, 15.07.2019 - 17.07.2019. [Abgerufen am: 20.01.2021].

[4] OpenWrt Webseite. https://openwrt.org. [Abgerufen am: 28.10.2020].

[5] DD-WRT Webseite. https://dd-wrt.com. [Abgerufen am: 29.10.2020].

[6] AdvancedTomato Webseite. https://advancedtomato.com. [Abgerufen am: 29.10.2020].

[7] libreCMC Webseite. https://librecmc.org. [Abgerufen am: 29.10.2020].

[8] Bundesamt für Sicherheit in der Informationstechnik, "BSI TR-03148:Secure Broadband Router: Requirements for secure Broadband Routers." https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03148/TR03148.pdf?__blob=publicationFile&v=3, 2020. [Abgerufen am: 26.10.2020].

[9] A. P. Ortega, X. E. Marcos, L. D. Chiang, and C. L. Abad, "Preventing ARP cache poisoning attacks: A proof of concept using OpenWrt," in *2009 Latin American Network Operations and Management Symposium*, pp. 1–9, IEEE, 19.10.2009 - 21.10.2009. [Abgerufen am: 08.11.2020].

[10] C. E. Palazzi, M. Brunati, and M. Roccetti, "An OpenWRT solution for future wireless homes," in *2010 IEEE International Conference on Multimedia and Expo*, pp. 1701–1706, IEEE, 19.07.2010 - 23.07.2010. [Abgerufen am: 08.11.2020].

[11] Andrew McDonnell, "Evaluating the security of OpenWRT." https://blog.oldcomputerjunk.net/2014/evaluating-the-security-of-openwrt-part-1/, 2014. [Abgerufen am: 08.11.2020].

[12] OpenWrt Webseite, "OpenWrt Version History." https://openwrt.org/about/history, 13.12.2020. [Abgerufen am: 28.10.2020].

[13] Linus Torvalds, "Linux—a free unix-386 kernel." https://tech-insider.org/linux/research/acrobat/911010.pdf, 1991. [Abgerufen am: 08.11.2020].

[14] G. K.-H. Jonathan Corbet, "Linux Kernel Development: How Fast It is Going, Who is Doing It, What They Are Doing and Who is Sponsoring the Work." https://www.linuxfoundation.org/wp-content/uploads/linux-kernel-report-2016.pdf, 2016. [Abgerufen am: 11.11.2020].

[15] H. Chen, Z. Zhang, S. Moon, and Y. Zhou, eds., *Proceedings of the Second Asia-Pacific Workshop on Systems - APSys '11*, (New York, New York, USA), ACM Press, 2011.

[16] M. Jimenez, M. Papadakis, and Y. Le Traon, "An Empirical Analysis of Vulnerabilities in OpenSSL and the Linux Kernel," in *2016 23rd Asia-Pacific Software Engineering Conference (APSEC)*, pp. 105–112, IEEE, 06.12.2016 - 09.12.2016. [Abgerufen am: 08.11.2020].

[17] Lennart Beringer, Adam Petche, Katherine Q. Ye, Andrew W. Appel, "Verified Correctness and Security of OpenSSL HMAC," in *24th USENIX Security Symposium*. [Abgerufen am: 05.11.2020].

[18] J. Viega, M. Messier, and P. Chandra, *Network Security with OpenSSL: Cryptography for Secure Communications*. Sebastopol: O'Reilly Media Inc, 2009.

[19] V. J. D. Barayuga and W. E. S. Yu, "Packet Level TCP Performance of NAT44, NAT64 and IPv6 Using Iperf in the Context of IPv6 Migration," in *2015 5th International Conference on IT Convergence and Security (ICITCS)*, pp. 1–3, IEEE, 24.08.2015 - 27.08.2015. [Abgerufen am: 12.11.2020].

[20] D. Lowe, *Networking all-in-one for dummies*. Learning made easy, Hoboken, New Jersey: John Wiley & Sons Inc, 7th edition ed., 2018.

[21] R. Perlman, *Interconnections: Bridges, routers, switches and internetworking protocols*. Addison-Wesley professional computing series, Reading, Mass.: Addison-Wesley, 2. ed., 1. print ed., 1999.

[22] P. Fischer and P. Hofer, *Lexikon der Informatik*. Berlin: Springer, 15., überarb. aufl. ed., 2011.

[23] A. Schemberg, M. Linten, and K. Surendorf, *PC-Netzwerke: Das umfassende Handbuch*. Rheinwerk Computing, Bonn: Rheinwerk, 7., aktualisierte und erweiterte auflage ed., 2016.

[24] Ubuntu-Forum Wiki Autoren, "OSI-Referenzmodell." http://wiki.ubuntu-forum.de/index.php?title=Baustelle:OSI-Referenzmodell, 2011. [Abgerufen am: 19.01.2021].

[25] Stephen Hilt, Fernando Mercês, Mayra Rosario, and David Sancho, "Worm War: The Botnet Battle for IoT Territory." https://documents.trendmicro.com/assets/white_papers/wp-worm-war-the-botnet-battle-for-iot-territory.pdf, 2020. [Abgerufen am: 19.01.2021].

[26] OWASP Foundation, "Brute Force Attack." https://owasp.org/www-community/attacks/Brute_force_attack, 2020. [Abgerufen am: 19.01.2021].

[27] D. Stuttard and M. Pinto, *The web application hacker's handbook: Finding and exploiting security flaws*. Indianapolis, Ind.: Wiley, 2nd. ed. ed., 2011.

[28] P. Kim, *The hacker playbook 2: Practical guide to penetration testing*. Leipzig: CreateSpace by Amazon Distribution GmbH, 2015.

[29] P. Yaworski, *Real-world bug hunting: A field guide to web hacking*. 2019.

[30] Martin Müller, "SAMESITE COOKIES - STRICT, ODER SOLL ES DOCH LIEBER LAX SEIN?." https://blog.viadee.de/samesite-cookies-strict-oder-lax, 2019. [Abgerufen am: 05.12.2020].

[31] R. M. Gérald Doussot, "State of DNS Rebinding: Attack & Prevention Techniques and the Singularity of Origin." https://docs.google.com/presentation/d/1O7MxvbIfRcPSlbyZbFxD-fAR34XlquQSlRAHPb2kR4E/edit#slide=id.p, 2019. [Abgerufen am: 02.12.2020].

[32] radware, "DDoS Survival Handbook." https://www.radware.com/getattachment/Security/Research/702/Radware_DDoS_Handbook_2015.pdf.aspx?lang=en-US, 2015. [Abgerufen am: 19.01.2021].

[33] Stefano Albrecht, "Denial of Service." http://www.highgames.com/?set=hardwareview&view=8, 2005. [Abgerufen am: 19.01.2021].

[34] Bundesamt für Sicherheit in der Informationstechnik, "Der Bot im Babyfon." https://www.bsi-fuer-buerger.de/BSIFB/DE/Service/Aktuell/Informationen/Artikel/Botnetz_iot_24102016.html, 2016. [Abgerufen am: 18.01.2021].

[35] OpenWrt Webseite, "About the OpenWrt/LEDE project." https://openwrt.org/about, 16.10.2020. [Abgerufen am: 28.10.2020].

[36] OpenWrt Webseite, "Package table." https://openwrt.org/_media/packages_dump_tab_separated.zip, 03.01.2021. [Abgerufen am: 04.01.2021].

[37] OpenWrt Webseite, "Table of Hardware." https://openwrt.org/toh/start, 18.01.2020. [Abgerufen am: 28.10.2020].

[38] OpenWrt Webseite, "OpenWrt Download Statistik November 2020," 29.11.2020. [Abgerufen am: 30.11.2020].

[39] Bundesamt für Sicherheit in der Informationstechnik, "BSI TR-03148 Sichere Breitband Router." https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03148/tr03148_node.html. [Abgerufen am: 26.10.2020].

[40] Ulrich Hottelet, "BSI will Router mit neuer Technischen Richtlinie sicherer machen." https://www.heise.de/security/meldung/BSI-will-Router-mit-neuer-Technischen-Richtlinie-sicherer-machen-4222689.html, 16.11.2018. [Abgerufen am: 04.01.2021].

[41] Friedhelm Greis, "CCC und OpenWRT kritisieren Router-TR als Farce." https://www.golem.de/news/bsi-richtlinie-ccc-und-openwrt-kritisieren-router-tr-als-farce-1811-137796.html, 19.11.2018. [Abgerufen am: 04.01.2021].

[42] A. Spillner and T. Linz, *Basiswissen Softwaretest: Aus- und Weiterbildung zum Certified Tester : Foundation Level nach ISTQB-Standard*. 6., überarbeitete und aktualisierte auflage ed., 2019.

[43] G. J. Myers, T. Badgett, and C. Sandler, *The art of software testing: Now covers testing for usability, smartphone apps, and agile development environments*. Hoboken, NJ: Wiley, 3. ed. ed., 2012.

[44] A. Mili and F. Tchier, *Software testing: Concepts and operations*. Quantitative software engineering series, Hoboken, NJ: Wiley, 2015.

[45] S. C. Johnson and M. Hill, "Lint, a c program checker." https://wolfram.schneider.org/bsd/7thEdManVol2/lint/lint.pdf, 1978. [Abgerufen am: 20.01.2021].

[46] Secure Software, Inc., "RATS - Rough Auditing Tool for Security." https://github.com/andrew-d/rough-auditing-tool-for-security, 2013.

[47] Fraunhofer FKIE, "FACT Core." https://github.com/fkie-cad/FACT_core, 2020. [Abgerufen am: 26.10.2020].

[48] K. W. Ruben Gonzalez, "Hackerpraktikum WS-18: Folien zur Vorlesung," 29.04.2019.

[49] xorl, "Linux GLibC Stack Canary Values." https://xorl.wordpress.com/2010/10/14/linux-glibc-stack-canary-values/, 2010. [Abgerufen am: 24.12.2020].

[50] Siddharth Sharma, "Enhance application security with FORTIFY_SOURCE." https://access.redhat.com/blogs/766093/posts/1976213, 2014. [Abgerufen am: 24.12.2020].

[51] Peter Weidenbach, Johannes vom Dorp, "Home Router Security Report 2020." https://www.fkie.fraunhofer.de/content/dam/fkie/de/documents/HomeRouter/HomeRouterSecurity_2020_Bericht.pdf, 2020. [Abgerufen am: 27.10.2020].

[52] M. Payer, "Too much PIE is bad for performance." https://doi.org/10.3929/ethz-a-007316742. [Abgerufen am: 24.12.2020].

[53] The MITRE Corporation, "About CVE." https://cve.mitre.org/about/, 2020. [Abgerufen am: 20.01.2021].

[54] Prof. Dr.-Ing. Luigi Lo Iacono, "Management der IT-Sicherheit: Folien zur Vorlesung," 2020.

[55] Peter Mell, Karen Scarfone , Sasha Romanosky, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0." https://www.first.org/cvss/v2/cvss-v2-guide.pdf, 2007. [Abgerufen am: 20.01.2021].

[56] FIRST, "Common Vulnerability Scoring System v3.0: Specification Document." https://www.first.org/cvss/v3.0/cvss-v30-specification_v1.9.pdf, 2015. [Abgerufen am: 20.01.2021].

[57] G. Lyon, *nmap network scanning*. Sunnyvale, CA: Insecure.Com LLC, 2008.

[58] Gordon Fyodor Lyon, "Nmap 7.90 Released! First release since August 2019.." https://seclists.org/nmap-announce/2020/1, 2020. [Abgerufen am: 17.11.2020].

[59] A. Acosta-López, E. Y. Melo-Monroy, and P. A. Linares-Murcia, "Evaluation of the WPA2-PSK wireless network security protocol using the Linset and Aircrack-ng tools," *Revista Facultad de Ingeniería*, vol. 27, no. 47, 2018. [Abgerufen am: 18.11.2020].

[60] M. Waliullah, A. B. M. Moniruzzaman, and M. S. Rahman, "An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network," *International Journal of Future Generation Communication and Networking*, vol. 8, no. 1, pp. 9–18, 2015. [Abgerufen am: 19.11.2020].

[61] P. Goyal and A. Goyal, "Comparative study of two most popular packet sniffing tools-Tcpdump and Wireshark," in *2017 9th International Conference on Computational Intelligence and Communication Networks (CICN)*, pp. 77–81, IEEE, 16.09.2017 - 17.09.2017. [Abgerufen am: 19.11.2020].

[62] C. Sanders, *Practical packet analysis: Using Wireshark to solve real-world network problems*. San Francisco: No Starch Press, 3rd edition ed., 2017.

[63] Robert David Graham, "Masscan: Mass ip port scanner," 2021.

[64] Anton Keks, "Angry IP Scanner: Fast and friendly network scanner." https://angryip.org, 2020.

[65] netsniff-ng, "netsniff-ng toolkit." http://netsniff-ng.org, 2021.

[66] M. V. Alberto Ornaghi, "About the Ettercap Projekt." https://www.ettercap-project.org/about.html, 2021.

[67] OpenWrt Webseite, "Factory install: First-time installation on a device." https://openwrt.org/docs/guide-quick-start/factory_installation, 2019. [Abgerufen am: 02.11.2020].

[68] OpenWrt Webseite, "Router vs switch vs gateway and NAT." https://openwrt.org/docs/guide-user/network/switch_router_gateway_and_nat, 2020. [Abgerufen am: 02.11.2020].

[69] Stefan Viehböck, "Brute forcing Wi-Fi Protected Setup." https://sviehb.files.wordpress.com/2011/12/viehboeck_wps.pdf, 2011. [Abgerufen am: 24.11.2020].

[70] OpenWrt Webseite, "Release Signing." https://openwrt.org/docs/guide-user/security/release_signatures, 2019. [Abgerufen am: ß5.01.2021].

[71] Paul Russell, "Netfilter - Project history." https://www.netfilter.org/about.html#history. [Abgerufen am: 25.11.2020].

[72] Simon Kelley, "dnsmasq Archiv." http://www.thekelleys.org.uk/dnsmasq/archive/?C=M;O=A, 2001. [Abgerufen am: 25.11.2020].

[73] Daniel Stenberg, "curl.1 the man page." https://curl.se/docs/manpage.html, 2020. [Abgerufen am: 20.01.2021].

[74] Thomas d'Otreppe de Bouvette. https://github.com/aircrack-ng/aircrack-ng, 25.01.2020. [Abgerufen am: 25.11.2020].

[75] D. Wetter, "testssl.sh." https://testssl.sh, 2020. [Abgerufen am: 26.11.2020].

[76] The OWASP® Foundation, "Owasp® zed attack proxy (zap)," 2020.

[77] OpenWrt Team, "Luci dispatcher.lua." https://github.com/openwrt/luci/blob/master/modules/luci-base/luasrc/dispatcher.lua, 2020. [Abgerufen am: 28.11.2020].

[78] Patrick Lacharme, Andrea Röck, Vincent Strubel, Marion Videau, "The Linux Pseudo-random Number Generator Revisited." https://eprint.iacr.org/2012/251.pdf, 2012. [Abgerufen am: 27.11.2020].

[79] Microsoft, "MS08-020 : How predictable is the DNS transaction ID?." https://msrc-blog.microsoft.com/2008/04/09/ms08-020-how-predictable-is-the-dns-transaction-id/, 2008. [Abgerufen am: 27.11.2020].

[80] Ben Sooter, "URLchecker - Top 1000 Websites." https://github.com/bensooter/URLchecker/blob/master/top-1000-websites.txt, 15.03.2016. [Abgerufen am: 19.11.2020].

[81] Siegfried Gabler, Sabine Häder, "Sampling in Theory." https://www.gesis.org/fileadmin/upload/SDMwiki/GablerH%C3%A4der_Sampling_in_Theory.pdf, 2016. [Abgerufen am: 14.01.2021].

[82] F. J. M. Jr., "The kolmogorov-smirnov test for goodness of fit," *Journal of the American Statistical Association*, vol. 46, no. 253, pp. 68–78, 1951. [Abgerufen am: 15.01.2021].

[83] Ronald L. Rivest, "The MD5 Message-Digest Algorithm." https://dl.acm.org/doi/pdf/10.17487/RFC1321?casa_token=BY42P3KQ8XcAAAAA:GtB7dinUB7LEy1HwulUgrB-C3DLqqho6WWUqn1ztqADIa7B28k1ruRNDmHp4Tush1yvf7PR_-NQ, 1992. [Abgerufen am: 11.01.2021].

[84] Fraunhofer FKIE, "FACT Core." https://github.com/fkie-cad/FACT_core/blob/master/README.md, 2020. [Abgerufen am: 26.10.2020].

[85] OpenWrt Website, "Runtime Logging in OpenWrt." https://openwrt.org/docs/guide-user/base-system/log.essentials. [Abgerufen am: 16.01.2021].

[86] The Internet Society, "HTTP Over TLS." https://tools.ietf.org/html/rfc2818, 2000. [Abgerufen am: 20.01.2021].

[87] Jake Edge, "OpenWrt and self-signed certificates." https://lwn.net/Articles/837491/, 2020. [Abgerufen am: 18.11.2020].

[88] Mozilla Foundation, "HTTPS-Only Mode in Firefox." https://support.mozilla.org/en-US/kb/https-only-prefs, 2020. [Abgerufen am: 20.01.2021].

[89] G. Halfacree, "Wave Computing Closes Its MIPS Open Initiative with Immediate Effect, Zero Warning." https://www.hackster.io/news/wave-computing-closes-its-mips-open-initiative-with-immediate-effect-zero-warning-e88b0df9acd0, 2020. [Abgerufen am: 14.01.2021].

[90] A. Lazarov, B. Shishkov, D. Mitrakos, and M. Janssen, eds., *Proceedings of the Eighth International Conference on Telecommunications and Remote Sensing - ICTRS '19*, (New York, New York, USA), ACM Press, 2019.

[91] OpenWrt Website, "Security." https://openwrt.org/docs/guide-developer/security. [Abgerufen am: 20.01.2021].

[92] P. Gaur and M. P. Tahiliani, "Operating Systems for IoT Devices: A Critical Survey," in *2015 IEEE Region 10 Symposium*, pp. 33–36, IEEE, 13.05.2015 - 15.05.2015. [Abgerufen am: 24.12.2020].

[93] OWASP Embedded Application Security Project, "Securing Sensitive Information." https://scriptingxss.gitbook.io/embedded-appsec-best-practices/4_securing_sensitive_information, 2019. [Abgerufen am: 24.12.2020].

[94] "SSL Private-Key." https://ssl.de/ssl-glossar/private-key.html. [Abgerufen am: 25.12.2020].

[95] J. Du, X. Li, and H. Huang, "A Study of Man-in-the-Middle Attack Based on SSL Certificate Interaction," in *2011 First International Conference on Instrumentation, Measurement, Computer, Communication and Control*, pp. 445–448, IEEE, 21.10.2011 - 23.10.2011. [Abgerufen am: 12.12.2020].

[96] M. Carvalho, J. DeMott, R. Ford, and D. A. Wheeler, "Heartbleed 101," *IEEE Security & Privacy*, vol. 12, no. 4, pp. 63–67, 2014. [Abgerufen am: 16.01.2021].

[97] R. K. Konoth, R. van Wegberg, V. Moonsamy, and H. Bos, "Malicious cryptocurrency miners: Status and Outlook." http://arxiv.org/pdf/1901.10794v1. [Abgerufen am: 16.01.2021].

Anhang A

Verwendete Firmware für FACT Analyse

PROJEKT	ROUTER	VERSION	VERÖFFENTLICHUNGS-DATUM	LINK
OPENWRT	ARCHER C7 v5	19.07.4	09.2020	https://downloads.openwrt.org/releases/19.07.4/targets/ath79/generic/openwrt-19.07.4-ath79-generic-tplink_archer-a7-v5-squashfs-factory.bin
OPENWRT	ARCHER C7 v5	19.07.5	12.2020	https://downloads.openwrt.org/releases/19.07.5/targets/ath79/generic/openwrt-19.07.5-ath79-generic-tplink_archer-c7-v5-squashfs-factory.bin
LIBRECMC	ARCHER C7 v2	v1.5.3:2020-10-02	02.10.2020	https://librecmc.org/librecmc/downloads/snapshots/v1.5.3/targets/ath79/generic/librecmc-ath79-generic-tplink_archer-c7-v2-squashfs-factory.bin
GLUON	ARCHER C7 v5	V2-v2020.2.1	09.10.2020	https://images.ffkbu.de/BonnV2/stable/Wireguard/factory/gluon-ffkbu-V2-v2020.2.1-Wireguard-tp-link-archer-c7-v5.bin
GARGOYLE	ARCHER C7 v5	1.12.0 (stable)	03.12.2019	https://www.gargoyle-router.com/downloads/images/ar71xx/gargoyle_1.12.0-ar71xx-generic-archer-c7-v5-squashfs-factory.bin
TOMATO	NETGEAR WNDR3700v3	3.4-138	05.12.2016	https://advancedtomato.com/downloads/router/wndr3700v3
DDWRT	ARCHER C7 v5	12-18-2020-r45036	18.12.2020	ftp://ftp.dd-wrt.com/betas/2020/12-18-2020-r45036/tplink_archer-c7-v5/

Anhang B

OpenWrt Veröffentlichungshistorie

Version (Code Name)	Veröffentlichungsdatum	Linux Kernel	libc
White Russian 0.9	2007 January	2.4.30	uClibc
Kamikaze 7.06	2007 June	2.6.19	
Kamikaze 7.07	2007 July	2.6.21	
Kamikaze 7.09	2007 September		
Kamikaze 8.09	2008 September	2.6.26	
Kamikaze 8.09.1	2009 June	2.6.26.8	
Kamikaze 8.09.2	2010 January		
Backfire 10.03	2010 April	2.6.32	
Backfire 10.03.1	2011 December		
Attitude Adjustment 12.09	2013 April	3.3	
Barrier Breaker 14.07	2014 October	3.10.49	
Chaos Calmer 15.05	2015 September	3.18.20	
Chaos Calmer 15.05.1	2016 March	3.18.23	
LEDE 17.01.0	2017 February	4.4.50	musl
LEDE 17.01.1	2017 April	4.4.61	
LEDE 17.01.2	2017 June	4.4.71	
LEDE 17.01.3	2017 August	4.4.89	
LEDE 17.01.4	2017 October	4.4.92	
LEDE 17.01.5	2018 July	4.4.140	
LEDE 17.01.6	2018 September	4.4.153	
OpenWrt 18.06.0	2018 July	4.9.111, 4.14.52	
OpenWrt 18.06.1	2018 August	4.9.120, 4.14.63	
OpenWrt 18.06.2	2019 February	4.9.152, 4.14.95	
OpenWrt 18.06.3	skipped	skipped	
OpenWrt 18.06.4	2019 July	4.9.184, 4.14.131	
OpenWrt 18.06.5	2019 November	4.9.198, 4.14.151	
OpenWrt 18.06.6	2020 January	4.9.208, 4.14.162	
OpenWrt 18.06.7	2020 January	4.9.211, 4.14.167	
OpenWrt 18.06.8	2020 March	4.9.214, 4.14.171	
OpenWrt 19.07.0	2020 January	4.14.162	
OpenWrt 19.07.1	2020 January	4.14.167	
OpenWrt 19.07.2	2020 March	4.14.171	
OpenWrt 19.07.3	2020 May	4.14.180	
OpenWrt 19.07.4	2020 September	4.14.195	
OpenWrt 19.07.5	2020 December	4.14.209	

Tabelle B.1: Veröffentlichungshistorie von OpenWrt, sowie genutzer Linux Kernel und libc Version