Fachhochschule
Münster University of
Applied Sciences

Fachhochschule Münster

Fachbereich Elektrotechnik und Informatik

Kompromittierung von Multifunktionsdruckern

Eine Sicherheitsanalyse am Beispiel des Epson WF-2540

Bachelorarbeit

im Studiengang Informatik

Abgabedatum:	17. September 2015
Autor:	Yves-Noel Weweler ‹y.weweler@gmail.com›
Matrikelnummer	733687
Unternehmen	OpenSource Security Ralf Spenneberg
Betreuer:	Prof. Dr. Sebastian Schinzel
Zweitprüfer:	M.Sc. Hendrik Schwartke

Eidesstattliche Erklärung

Ich versichere, dass ich diese schriftliche Arbeit selbständig angefertigt, alle Hilfen und Hilfsmittel angegeben und alle wörtlich oder im Sinne von Veröffentlichungen oder anderen Quellen, insbesondere dem Internet entnommenen Inhalte, kenntlich gemacht habe.

_____

Abstract

Seit vielen Jahren sind Unzulänglichkeiten bei der informationstechnischen Sicherheit eingebetteter System bekannt. Geräte, die direkt an das Internet angeschlossen sind, stehen meist unter strenger Beobachtung. Eingebetteten Systemen wird dabei oft keine Beachtung geschenkt, da die technischen Fähigkeiten der Geräte unterschätzt werden, oder die Geräte vermeintlich keine Verbindung zur Außenwelt besitzen, die als Bedrohung erkannt wird. Eine Analyse dieser Systeme ist oft herstellerspezifisch und erfordert eine nähere Betrachtung der Hardware. In dieser Arbeit wurden Multifunktionsdrucker des Herstellers Epson untersucht, für die es zum Verfassungszeitpunkt der Arbeit keine öffentlichen Untersuchungen gab. Dabei wurden speziell mangelnde Sicherheitsvorkehrungen bei Firmware sowie Firmware-Updates gezeigt und demonstriert wie Angreifer die identifizierten Schwachstellen nutzen können um die Geräte zu übernehmen. Die gefundenen Schwachstellen stellen eine hohe Bedrohung dar und erreichen einen CVSS-Wert von 10.0. Nach der Übernahme eines Gerätes wird demonstriert, wie das eingebaute Modem zu Infiltration und Exfiltration von sensiblen Daten über das Telefonnetz ausgenutzt werden kann. So können Angreifer in Netze, die über keine IP-Konnektivität zum Internet oder der Außenwelt verfügen, eindringen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Akronyme

APT Advanced Persistent Threat

CIA Central Intelligence Agency

CPHA Clock Phase

CPOL Clock Polarity

CS Chip Select

CSRF Cross-Site Request Forgery

CVE Common Vulnerabilities and Exposures

CVSS Common Vulnerability Scoring System

DI Data In

DO Data Out

DPU Digital Processing Unit

EJL Epson Job Language

IC Integrated Circuit

ISR Interrupt Service Routine

IVT Interrupt Vector Table

MFP Multifunction Printer

MISO Master In Slave Out

MMU Memory Management Unit

MOSI Master Out Slave In

MSB Most Signifikant Bit

MuFuG Multifunktionsgerät

PCL Printer Control Language

PJL Printer Job Language

QPI Quad Peripheral Interface

RFC Request For Comments

SCK Serial Clock

SNMP Simple Network Management Protocol

SOC System-on-a-Chip

SOP Same-Origin-Policy

SPI Serial Peripheral Interface

SS Slave Select

URI Uniform Resource Identifier

XSS Cross-Site Scripting

1 Einleitung

Multifunktionsgeräte sind Geräte, die mehrere Funktionen wie beispielsweise Drucken, Scannen und FAX-Funktionalität in einem einzelnen Gerät vereinen. Diese Geräte sind schon lange selbstverständlich und man findet sie heutzutage in jedem Bereich des alltäglichen Lebens. In Anbetracht der starken Verbreitung dieser Systeme und der Tatsache das ihnen große Mengen sensibler Dokumente anvertraut werden, muss die Frage nach deren Sicherheit gestellt werden. In der Vergangenheit wurden immer wieder Gefahren und mögliche Angriffe auf Drucker gefunden (Kapitel 1.2). Trotz der gezeigten Verwundbarkeit und offensichtlichen Attraktivität für Angreifer, sind dennoch bis heute keinerlei Berichte von großangelegten Angriffen, Würmern oder Trojanern für diese Systeme in freier Wildbahn bekannt. Die Komplexität der Geräte ist in den letzten Jahren so stark gestiegen, dass man sie mittlerweile mit "normalen" Computern vergleichen kann, die nur für spezielle Aufgaben angepasst wurden. Dennoch sind die Software und Inhalte dieser Geräte für Untersuchungen weitaus weniger zugänglich, als es bei den üblichen Desktop-Computern der Fall ist. Diese Systeme und die darauf laufende Software sind nicht selten durch historisch gewachsene herstellerspezifische Lösungen geprägt. Daher sind Erkenntnisse überwiegend auf einen Hersteller beschränkt und Untersuchungen müssen für jeden gesondert durchgeführt werden.

1.1 Motivation

Drucker und Multifunktionsgeräte sind stark verbreitet. Man findet diese Geräte in vielen Büros oder Haushalten und auch in Umgebungen, die vom öffentlichen Netz getrennt sind, um gesondert geschützt zu werden. Die Anwender vertrauen den Geräten große Mengen hochsensibler Daten an, machen sich aber nur wenig Gedanken um die Sicherheit dieser Systeme. Und das, obwohl es bereits in der Vergangenheit Betrachtungen von Multifunktionsgeräten und Druckerlösungen mehrerer Hersteller hinsichtlich ihrer Angreifbarkeit gab (siehe 1.2 Verwandte Arbeiten). All diese Untersuchungen zeigten starke Defizite bei der Sicherheit der Geräte. Multifunction Printer (MFP) sind heute, wie viele eingebettete Systeme, deutlich komplexer als noch vor wenigen Jahren. Diese Systeme unterscheiden sich mittlerweile im Kern meist nur noch gering von anderen Systemen wie Desktop-Computern, sind aber immer noch stark herstellerspezifisch geprägt. Sie sind schon lange netzwerkfähig und stellen eine Vielzahl von Diensten für andere Netzwerkteilnehmer zur Verfügung. Trotzdem fehlen den Geräten nach wie vor zentrale Fähigkeiten, um sich selbst vor Angriffen zu schützen. Schutzmaßnahmen wie interne Firewalls oder Maßnahmen zur Erkennung von Schadsoftware sind schlicht nicht vorhanden. Updates der Systeme erfolgen gar nicht, sehr unregelmäßig oder nur wenn es eigentlich schon zu spät ist. Wird ein Gerät kompromittiert, kann dies nur schwer festgestellt werden. Unter Umständen muss das Gerät hierzu zerlegt werden. Eine lückenlose Bereinigung nach einer Infizierung wäre aufgrund des fehlenden Wissens über das System und dessen Unzugänglichkeit somit kaum zu erreichen.

Trotz all dieser Erkenntnisse und der Veröffentlichungen der letzten Jahre sind die Anwender dieser Geräte und auch das IT-Sicherheitspersonal nur wenig für diese Probleme

sensibilisiert. So empfiehlt beispielsweise der BSI-Grundschutzkatalog für Drucker den Einsatz von Paketfiltern und den Schutz der Administrativen-Geräteschnittstellen, damit diese nicht für alle Netzwerkteilnehmer ansprechbar sind ([1]). Es wird bei Multifunktionsgeräten sogar zur besonderen Vorsicht mit z.B. der FAX-Funktionalität geraten ([2]). Solche Empfehlungen werden aber selten eingehalten und wie die demonstrierten Schwachstellen der letzten Jahre zeigen, reichen diese Vorkehrungen zum Schutz der Systeme auch oft nicht aus. Drucker sind trotz dieser Empfehlungen viel zu selten Bestandteil von Sicherheitsbetrachtungen. Ungeachtet der technischen Ausstattung dieser Geräte und den bekannten Gefahren erwartet kaum jemand einen infizierten Drucker im Netzwerk oder wäre in der Lage ein kompromittiertes Gerät zu erkennen.

Es wird daher in dieser Arbeit untersucht, welche Gefahren von einem Drucker und insbesondere einem Multifunktionsgerät ausgehen und geklärt, ob und wie sich ein solches Geräte angreifen lässt, mit welchem Aufwand Angriffe verbunden sind und wer dazu in der Lage ist. Durch die Hardwarenähe und die große Menge an herstellerspezifischen Lösungen werden die Betrachtungen auf Geräte eines Herstellers beschränkt. Es wird mit Hilfe eines Testsystems versucht, Schwachstellen zu finden und untersucht wie ein Angreifer möglichst unbemerkt mit dem System kommunizieren kann. Diese Erkenntnisse sind für die Absicherung der Geräte und aller mit ihrem Betrieb involvierten Komponenten und Personen unerlässlich und tragen zur Sensibilisierung aller Beteiligten bei.

1.2 Verwandte Arbeiten

Die ersten bekannten Angriffe auf MFP's gehen bis in die 1960er Jahre zurück. Damals versuchte die Central Intelligence Agency (CIA) mit Hilfe der ersten vollautomatischen Fotokopierer/Drucker an geheime Dokumente der Sowjetunion zu gelangen. Zu diesem Zwecke wurden Mikrofilmkameras entwickelt, die in die, damals noch recht großen, Maschinen eingesetzt wurden und Fotos von allen kopierten Dokumenten machten (siehe [3, S.68.ff]).

Die ersten Betrachtungen an moderneren Geräten von HP werden 2002 neben Untersuchungen anderer eingebetteter Systeme durch FX/KIM0 auf der Blackhat präsentiert ([4]). Schon damals wurden neben Angriffen über die Printer Job Language (PJL), mit der Druckeinstellungen verändert werden konnten, auch Angriffe über das Simple Network Management Protocol (SNMP) demonstriert. Damit konnten beispielsweise die Passwörter der Systeme ausgelesen werden. Die wichtigste damals gefundene Schwachstelle erlaubte jedoch das Ausführen von eigenem Java Code auf einer ganzen Reihe von HP Druckern. Danach wird der Themenbereich um 2006 herum insbesondere von Adrian Crenshaw (irongeek) auf der notacon wieder aufgegriffen. Crenshaw beschrieb damals systematisch eine ganze Reihe von Angriffsmöglichkeiten mit ausführlichen Anleitungen. Neben Erklärungen und Demonstrationen von Angriffen über SNMP und PJL für Display Hacks, beschrieb er auch Probleme mit Sniffing/Replay Attacken und Dateiuploads über schlecht gesicherte Webinterfaces für HP JetDirect Drucker (siehe [5], [6])

Insbesondere die Printer Display Hacks, haben in der Vergangenheit Bekanntheit erlangt. Dabei wird mittels PJL ein Text auf dem Display eines Druckers angezeigt. PJL wurde konzipiert um Druckern eine Steuerung und Unterteilung in Druckaufträge hinzuzufügen. Dabei wird ausgenutzt, dass diese Erweiterung auch die Möglichkeit hinzugefügt hat, Statusnachrichten anzuzeigen. PJL und auch die Printer Control Language (PCL) sowie ihre meist herstellerspezifischen Erweiterungen erlauben aber noch diverse weitere Konfigurationen und somit Angriffe auf Drucker, sofern die Geräte die Funktionalitäten voll implementiert haben. Insbesondere die Display Hacks haben aber in den letzten Jahren immer weiter an Bedeutung verloren, da diese Funktionen von den Druckern scheinbar nicht mehr vollständig implementiert werden.

Seit 2010 gab es zahlreiche weitere Betrachtungen von Geräten diverser Hersteller, die schon bekannte Angriffe verfeinerten oder an neuen Produkten demonstrierten. Besonders relevante Neuerungen waren aber ausnutzbare Schwachstellen in den Postscript Interpretern auf den Geräten. Postscript ist eine Beschreibungssprache für Seiteninhalte und wird üblicherweise als Vektorgrafikformat eingesetzt. Postscript ist nebenbei aber auch eine interpretierte Turing-vollständige, stackorientierte Programmiersprache, die sogar Dateisystemzugriffe erlaubt ([7]). Die große Komplexität eines solchen Formates wurde in Verbindung mit der hardwarenahen Implementierung zum Ziel von Angriffen mit denen Endlosschleifen, Abstürze und sogar selbstmodifizierender Code erzeugt werden konnte. Damit erlaubten es alleine die Möglichkeiten von Postscript, dass sich Dokumente auf einem Drucker im Moment des Druckens selbst modifizieren ([8]). Gefundene Fehler und Abstürze der Interpreter konnten dabei ausgenutzt und als Angriffe in speziell präparierten Dokumenten eingebettet werden. Da es in den Anfangszeiten der Drucker üblich gewesen ist, Software-Updates mittels Druckfunktion zu installieren, kommt erschwerend hinzu, dass dies historisch bedingt bei einigen Herstellern auch heute noch möglich ist. Das führte dazu, dass es möglich wurde ganze Firmware-Updates in druckbaren Dokumenten einzubetten und darauf zu warten, das ein Opfer diese druckt ([9]). Untersuchungen zu Firmware-Update-Prozessen sind nur wenig vorhanden. Vermutlich nicht zuletzt durch die Tatsache, dass die große Fülle an nutzbaren Schwachstellen oft dazu führte, dass eine Betrachtung dieser Prozesse gar nicht erst erfolgte (siehe [9], [10], [11]).

Sucht man auf den offiziellen Common Vulnerabilities and Exposures (CVE)-Listen nach dem Stichwort "Printer" so findet man für den Zeitraum 2009 bis 2015 26 CVE Einträge, die konkrete Druckermodelle verschiedener Hersteller betreffen ([12]). Schaut man sich die gelisteten Einträge genauer an, fällt auf, dass mit 12 Einträgen knapp die Hälfte auf Schwachstellen und Fehlkonfigurationen der Webserver und Weboberflächen zurückzuführen sind. Dabei handelt es sich in 8 Fällen um Probleme mit XSS. Mit XSS kann ein Angreifer Schadcode in Form von z.B. Javascript im Browser eines Opfers ausführen. Aufgrund der großen Funktionalität der Multifunktionsdrucker ergeben sich viele weitere Möglichkeiten für Angriffe. So können beispielsweise, wie von Adi Shamir 2014 auf der Blackhat Europe beschrieben, mit dem Licht eines Scanners Daten über Infrarot ausgeleitet werden ([13]).

1.3 Beitrag der Arbeit

Mit dieser Arbeit soll die Frage nach der Sicherheit heutiger Drucker und Multifunktionsgeräte näher betrachtet werden. Dazu wird anhand eines Beispiels geklärt, ob sich ein solches Gerät angreifen und übernehmen lässt. Es wird ermittelt wie aufwändig Angriffe auf ein solches System sind, welche Angreifer dazu die technischen Fähigkeiten besitzen und wie relevant Angriffe in der Praxis sind. Die technische Umsetzbarkeit einer Kompromittierung wird dazu am Beispiel durch eigene Angriffe untersucht. Dabei wird erstmalig eine öffentliche Untersuchung des Epson Multifunktionsdrucker Ökosystems vorgenommen und die Geräte auf Sicherheitsrisiken überprüft. Die Erkenntnisse werden zukünftig die Basis für weitere Untersuchungen dieser Geräte bilden und sollen zu mehr Untersuchungen bei dieser Klasse von Geräten im Allgemeinen beitragen. Damit wird zur Identifizierung, Behebung und dem Schutz vor Bedrohungen für diese Geräte und deren Anwendern beigetragen und eine Sensibilisierung der Nutzer und der verantwortlichen Hersteller erreicht.

1.4 Aufbau der Arbeit

Diese Arbeit ist unterteilt in sieben Abschnitte

1. Im ersten Teil der Arbeit wird die Herangehensweise der Untersuchung erläutert, ein Testgerät ausgewählt und es werden Vorbereitungen für die Analyse getroffen. (Kapitel 2)

2. Im zweiten Teil der Arbeit wird das ausgewählte System auf Bedrohungen analysiert, die als Ansatzpunkt für folgende Untersuchungen verwendet werden. (Kapitel 3)

3. Der dritte Teil dieser Bachelorarbeit beschreibt den Analyseprozess des ausgewählten Multifunktionsgerätes. Dabei werden insbesondere das Firmware-Dateiformat und die Update-Prozesse untersucht.
   Dieser Teil entspricht dem gesamten Kapitel 4.

4. In Kapitel 5 wird der Aufbau einer Umgebung zum Erstellen eigener Firmware beschrieben. Dabei wird unter anderem eine Toolchain erstellt, die es ermöglicht, eigene Programme und Kernel-Komponenten für das Gerät zu erzeugen.

5. In Kapitel 6 werden mögliche Angreifer betrachtet und in einer Testumgebung durchgeführte Angriffe beschrieben.

6. Die Ergebnisse dieser Arbeit werden in Kapitel 7 präsentiert.

7. Zum Schluss der Arbeit werden die wichtigsten Punkte der Arbeit noch einmal in einem Fazit zusammengefasst und ein Ausblick auf mögliche zukünftige Untersuchungen gegeben. (Kapitel 8 und 9)

2 Vorbereitung

2.1 Herangehensweise

Um Bedrohungen und mögliche Angriffe auf Multifunktionsgeräte untersuchen zu können, muss ein grundlegendes Verständnis der beteiligten Hardware und Software-Komponenten in einem solchen System gegeben sein. Daher wird ein repräsentatives Testgerät angeschafft, an dem Untersuchungen durchgeführt und gebildete Hypothesen verifiziert werden können. An diesem Gerät kann direkt in ablaufende Prozesse eingegriffen werden, um diese zu beobachten und zu verstehen. Bevor Test und Veränderungen am Gerät vorgenommen werden, wird der Ausgangszustand festgehalten. So kann insbesondere bei späteren Modifikationen auf einen Referenzzustand zurückgegriffen werden. Danach werden Schwachstellen identifiziert, mittels derer in das System eingedrungen werden kann. Anschließend wird die Anwendbarkeit der gewonnen Erkenntnisse auf Baureihen und ganze Produktfamilien überprüft.

2.2 Geräteauswahl

Für die Untersuchungen, wurde ein Geräte aus der Klasse der Multifunktionsgeräte ausgewählt und hinsichtlich der Fragestellungen untersucht. Wir haben uns dabei für einen Epson WF-2540 MFP entschieden. Epson gehört weltweit zu den drei größten Herstellern von Druckerlösungen ([14]). Epson ist scheinbar der einzige der drei Hersteller, zu dessen Produkten zum Verfassungszeitpunkt dieser Arbeit weder öffentliche Untersuchungen zur Sicherheit der Geräte, noch gemeldete CVE-Schwachstellen existieren, die deren Sicherheit betreffen. Für Geräte dieses Herstellers wird oft mit einem sogenannten Recovery-Mode geworben, der es erlauben soll Geräte wiederherzustellen und defekte Updates und Firmware zu reparieren. Die Möglichkeit defekte Geräte und Software zurückzusetzen und so Problemen mit der Zerstörung des Gerätes durch Tests ohne größeren Aufwand auszuweichen, ist besonders nützlich.

Betrachtet man beispielsweise die Marktanteile von Tintenstrahldruckern in Deutschland (28%) und Multifunktionsdruckern (26.73%) so wird klar, dass sich als repräsentatives Gerät ein Tintenstrahl-/ Multifunktionsdrucker empfiehlt ([15]). Daher fiel die Wahl auf den WF-2540, der von Epson für Kleinraumbüros geführt wird, aber denoch ein extrem günstiges Mittelklasse-Gerät ist, welches eine große Zahl an Funktionalitäten in sich vereint. Gleichzeitig ist es mit der Zugehörigkeit zur Workforce-Serie Teil einer der größten Produktlinien in diesem Segment. Ein solches Gerät ist in Abbildung 1 dargestellt.

Epson hat neben Geräten dieser Serie aber noch eine enorme Anzahl weiterer Multifunktionsdrucker im Handel. Von Interesse ist hier, ob sich hinter der großen Produktvielfalt eine weitestgehend einheitliche Software-Landschaft verbirgt, so dass die Erkenntnisse auf andere Geräte der Workforce-Serie übertragbar sind und möglicherweise auch auf andere Produktlinien angewendet werden können.

2.3 Epson WF-2540

Als Arbeitsgrundlage, werden im folgenden Informationen über Hardware und Software des WF-2540 gesammelt.

Abbildung 1: Epson WF-2540 Testgerät

2.3.1 Hardware

Um die Analysen zu unterstützen, wurde der MFP geöffnet und eine Übersicht über die relevanten Hardware-Komponenten erstellt (siehe Abbildung 2). Das System verfügt über 12 MB persistenten Speicher in Form von zwei Flash-Speicherbausteinen, mit 8 MB und 4 MB Kapazität. Die Speicherbausteine enthalten die für den Betrieb des Gerätes benötigte Software. Der größere der zwei Bausteine wird dabei zum Booten des Systems genutzt. Als Hauptspeicher befinden sich im Gerät 64 MB DDR2 SDRAM. Gesteuert wird das Gerät durch einen von Epson selbst produzierten Prozessor. Dieser Prozessor wurde von Epson in Kooperation mit Tensila speziell für den Einsatz in den eigenen Druckern entwickelt. Der REALOID Printer ist ein System-on-a-Chip (SOC) der eine Vielzahl von Xtensa Prozessoren zusammen mit einem ARM9 Prozessor auf einem Chip vereint. Der ARM Prozessor fungiert dabei als eigentlicher Hauptprozessor mit Memory Management Unit (MMU) und steuert die anderen Kerne an. Die Xtensa Prozessoren sind vergleichbar mit vordefinierten Digital Processing Unit (DPU)s, die über ein Bussystem mit einem Steuerprozessor zusammengeschlossen werden können. Einzelne DPUs sind dabei auf besondere Aufgaben spezialisiert, wie z.B. das Dekodieren von JPEG-Grafiken oder die Beschleunigung spezieller Operationen zur Bildaufbereitung.

Das Multifunktionsgerät (MuFuG) stellt zusätzlich eine 100Mbit Ethernet, eine WiFi-Schnittstelle, ein Modem und zwei USB-Anschlüsse bereit.

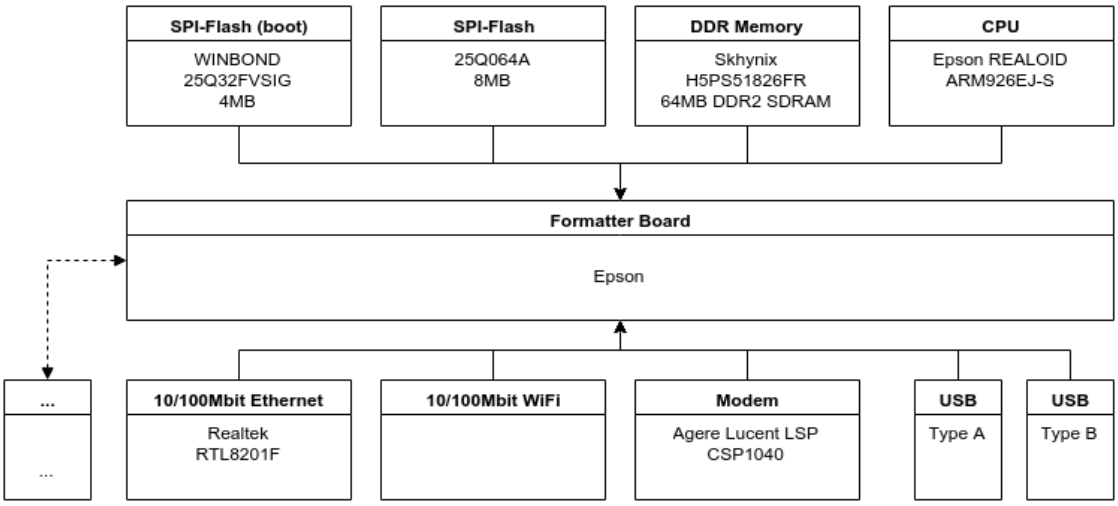

Abbildung 2: Logisches Blockschaltbild der relevanten Hardwarekomponenten

Der WF-2540 enthält 12 MB Flash-Speicher und wird durch einen von Epson speziell für Drucker entwickelten Prozessor mit integriertem ARM-Kern gesteuert. Das System verfügt dabei über 64 MB Hauptspeicher. Diese Abbildung zeigt schematisch den Aufbau des Gerätes. Das Mainboard auf dem die Komponenten verbaut sind, ist in Abbildung 3 dargestellt.

2.3.2 Software

Da zu diesem Zeitpunkt unklar ist, welche Software genau auf dem Gerät läuft, müssen zunächst von außen Informationen darüber zusammengetragen werden. Als Grundlage, wurde versucht an Informationen über das Betriebssystem des Gerätes und die nach außen bereitgestellten Dienste zu gelangen. Die hier aufgelisteten Ergebnisse sind dabei mit der LJ05DC Firmware des WF-2540 und nmap entstanden.

```
MAC Address: B0:E8:92:59:A9:59 (Seiko Epson)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
```

Listing 1: Betriebssystem-Erkennung

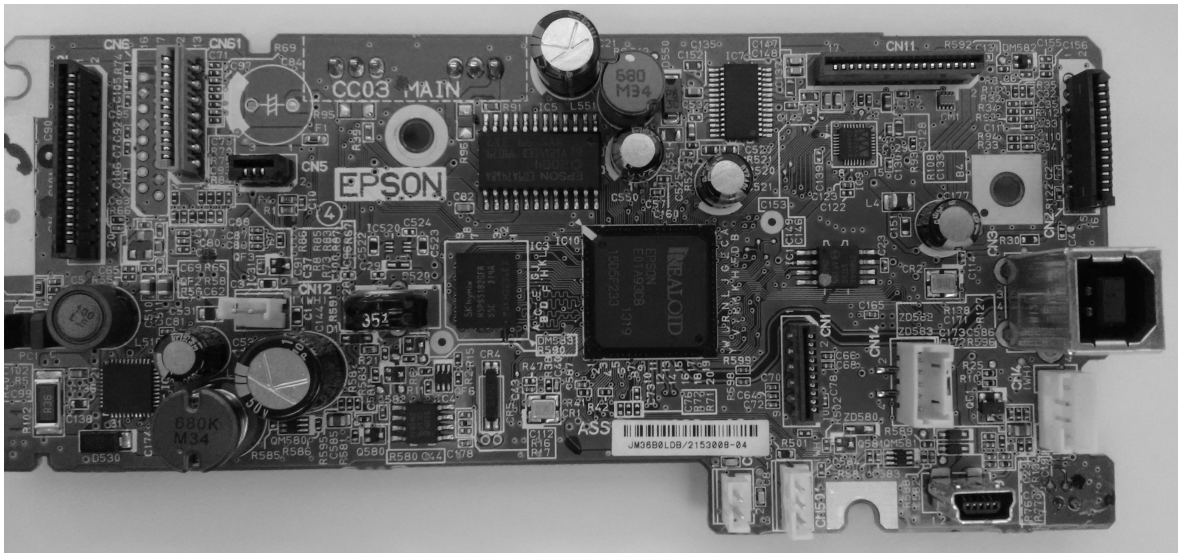

Abbildung 3: Ausgebautes Mainboard des WF-2540

```
Not shown: 65528 closed ports
PORT     STATE SERVICE
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
515/tcp  open  printer
631/tcp  open  ipp
1865/tcp open  unknown
9100/tcp open  jetdirect
```

Listing 2: TCP-Portscan

```
PORT     STATE         SERVICE
137/udp  open          netbios-ns
138/udp  open|filtered netbios-dgm
161/udp  open|filtered snmp
427/udp  open|filtered svrloc
1022/udp open|filtered exp2
1023/udp open|filtered unknown
3072/udp open|filtered unknown
3073/udp open|filtered unknown
3075/udp open|filtered orbix-locator
3078/udp open|filtered unknown
3289/udp open|filtered enpc
3702/udp open|filtered ws-discovery
5353/udp open          zeroconf
5355/udp open|filtered llmnr
```

Listing 3: UDP-Portscan

2.4 Speicherabzüge

Um den Ausgangszustand des Systems festzuhalten und das Gerät auch nach missglückten Veränderungen wiederherstellen zu können, müssen Kopien der verbauten Speicherbausteine angefertigt und geschrieben werden können. Die Flash-Speicher können dazu über verschiedene Wege angesprochen werden. Zum einen über das Serial Peripheral Interface (SPI) und über die Erweiterung Quad Peripheral Interface (QPI). QPI ist eine Erweiterung von SPI zur höheren Datenübertragung. SPI ist einfach umzusetzen, daher bieten selbst kleine Einplatinenrechner wie das Raspberry PI über ihre GPIO-Schnittstelle Möglichkeiten, über SPI zu kommunizieren. Als Alternative kann man einen SPI-Programmierer nutzen, der das Auslesen und Beschreiben von Speicherbausteinen erlaubt. Die ersten Versuche, den Speicher auszulesen, wurden mit einem Raspberry PI durchgeführt. Danach wurde aus Komfortgründen jedoch auf einen SPI-Programmierer zurückgegriffen.

2.4.1 Kurzeinführung in SPI

Das Serial Peripheral Interface (SPI) genannt ist ein Bus-System, das die serielle Kommunikation zwischen digitalen elektrischen Komponenten standardisiert. SPI wurde nicht formal definiert, was über die Jahre zu einer großen Vielfalt an Optionen führte. Mit SPI können Integrated Circuit (IC) in einer Master-Slave Architektur vernetzt werden und so Vollduplex kommunizieren ([16]).

Dabei besteht der Bus aus folgenden Leitungen:

- Master Out Slave In (MOSI) oft auch Data Out (DO)
- Master In Slave Out (MISO) oft auch Data In (DI)
- Serial Clock (SCK)
- Slave Select (SS) oft auch Chip Select (CS)

SPI erlaubt theoretisch beliebig viele Slaves in einer Schaltung, wobei es für jeden Slave eine zusätzliche SS Leitung vom Master gibt. Es existiert dabei immer nur genau ein Master der einen Slave oder eine Gruppe von Slaves durch das Ziehen der SS Leitungen von HIGH auf LOW auswählt. Der schematische Aufbau einer SPI-Schaltung wird in Abbildung 4 dargestellt.

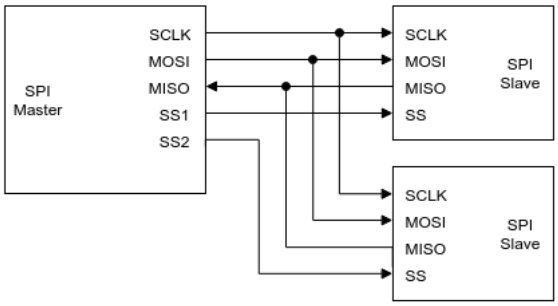

Abbildung 4: SPI Master-Slave Schaltung als Sternarchitektur

SPI erlaubt es eine beliebige Anzahl von Slaves an das Bussystem anzubinden. Einzelne Slaves werden dabei über die SS Leitung vom Master ausgewählt und Daten über die MISO und MOSI Leitungen passend zum Taktsignal ausgetauscht. (In Anlehnung an [17])

Zu beachten ist, dass die Kommunikation in vier verschiedenen Modi erfolgen kann. Diese werden über die Parameter Clock Polarity (CPOL) und Clock Phase (CPHA) der einzelnen Bausteine ausgewählt und legen fest, ab welcher Taktflanke ein Slave Daten vom Master liest oder schreibt. So kann z.B. erreicht werden, dass, wenn ein Slave über das Setzen der SS Leitung ausgewählt wird, Daten direkt (CPHA = 0) oder bei der ersten Taktflanke (CPHA = 1) an MISO angelegt werden. Diese Betriebsmodi können für jeden Baustein unterschiedlich sein. Viele Bausteine unterstützen jedoch eine Teilmenge dieser Modi, so dass nur auf eine einheitliche Konfiguration geachtet werden muss ([16]).

Mode	CPOL	CPHA
0	0	0
1	0	1
2	1	0
3	1	1

Tabelle 1: SPI Operations Modi

Bausteine können Daten über SPI in vier verschiedenen Modi austauschen. Diese Modi werden durch die Einstellung CPOL und CPHA an jedem Bauteil ausgewählt und legen fest wie und wann in Relation zum Taktsignal Daten an die MISO und MOSI Leitungen gelegt werden. ([18])

Datenübertragungen werden in SPI durch einen Instruktionscode eingeleitet. Diese Instruktionscodes sind nicht verbindlich festgehalten und können sich zwischen einzelnen Herstellern und Bausteinen unterscheiden. Allerdings haben sich für viele Bausteine einheitliche Opcodes herausgebildet, sodass generische Treiber in Teilen möglich wurden. Ein Instruktionscode hat dabei in der Regel eine Länge von einem Byte. Abhängig vom Instruktionscode folgen daraufhin Daten, wie z.B. Speicheradressen oder Nutzdaten. Dabei setzen Bausteine meist voraus, dass die übertragenen Daten ein Vielfaches von 8-Bit sind.

2.4.2 Speicherbausteine auslesen

Da durch Tests am System jederzeit systemrelevante Software zerstört werden kann und das Gerät unbrauchbar wird, wird eine Kopie des persistenten Speichers benötigt. Damit können ungewollte Veränderungen an Daten im System erkannt und das Gerät wiederhergestellt werden. Die erstellten Kopien des Speichers können außerdem für die spätere Analyse des Systems hilfreich sein. Um die Inhalte der im WF-2540 verbauten Speicherbausteine auslesen zu können, muss man als Master die entsprechenden Instruktionen an die Speicherbausteine übermitteln. Für den Speicher des WF-2540, listet das Datenblatt 45 unterstützte SPI Instruktionen. Von diesen 45 Instruktionen werden für das Lesen und Schreiben aber nur wenige benötigt. (siehe Appendix A.1)

Die Speicherbausteine können in den SPI Modi 0 und 3 betrieben werden und befinden sich standardmäßig im Modus 0 (siehe 2.4.1 Kurzeinführung in SPI). Instruktionen beginnen immer mit einer fallenden SS/CS Flanke und werden mit einer steigenden SS/CS Flanke wieder beendet. Daten werden dabei immer mit der steigenden Taktflanke verarbeitet und beginnen mit dem Most Signifikant Bit (MSB). Bei Datenübertragungen muss immer ein Vielfaches von 8 Bit übertragen werden, sonst wird die Instruktion ignoriert. Um den Speicherbaustein ansprechen zu können, muss laut Datenblatt CS beim Einschalten VCC folgen. Für diesen Zweck werden Pull-Up Widerstände in die Schaltung eingesetzt. Es sollte dabei beachtet werden, dass sich die Speicherbausteine alle SPI Leiterbahnen bis auf die CS Leitung teilen (siehe Abbildung 5).

Zum Auslesen der Bausteine wird die Read Data (03h) Instruktion genutzt (siehe Tabelle 2). Diese erlaubt das sequentielle Lesen von einem oder mehreren Bytes aus dem Speicher (siehe Abbildung 6). So kann man wie folgt den gesamten Speicherbaustein mit nur einer Instruktion auszulesen.

Data Input Output	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6
Clock Number	(0 - 7)	(8 - 15)	(16 - 23)	(24 - 31)	(32 - 39)	(40 - 47)
Read Data	03h	A23-A16	A15-A8	A7-A0	(D7-D0)	

Tabelle 2: Flash-Baustein Read Instruktion Aufbau

Die Read Data Instruktion der Bausteine erlaubt es, eine beliebige Anzahl von Bytes zu lesen. Der Read-Befehl setzt sich dabei aus dem Instruktionscode (03h) gefolgt von einer 24-Bit Speicheradresse zusammen, von der aus gelesen werden soll. (siehe Appendix A.1)

Die vom Master durchzuführenden Schritte sehen dabei wie folgt aus:

1. Master beginnt Instruktion: SS (HIGH -> LOW)
2. Master sendet Read Data Instruktionscode (03h -> MOSI)
3. Master sendet 24 Bit Adresse (Adresse -> MOSI)
4. Master gibt Clock Signal

5. Master liest Bit seriell von MISO
6. Master wiederholt 4 und 5
7. Master beendet Instruktion: SS (LOW -> HIGH)

Nachdem 8-Bits gelesen wurden, wird die Adresse vom Bauteil passend zum Takt inkrementieren. Dadurch können sequentiell beliebig viele Bytes gelesen werden (siehe Abbildung 6).

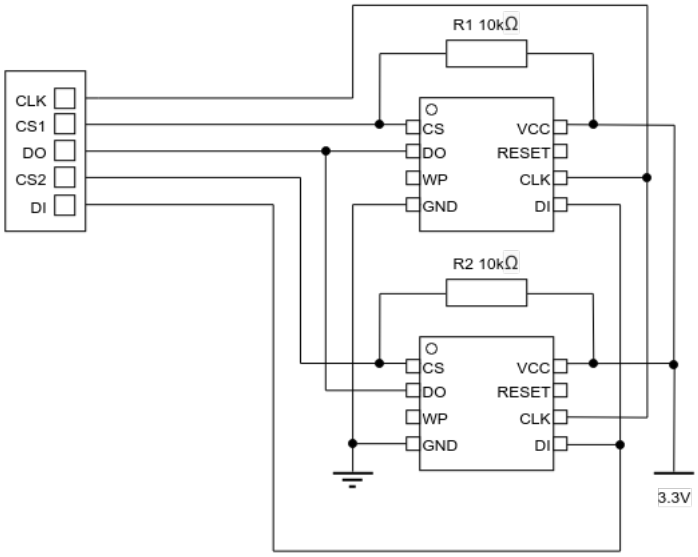

Abbildung 5: Schaltplan SPI Flash

Um die Speicherbausteine des WF-2540 mittels SPI ansprechen zu können, müssen die entsprechenden Leitungen von einem Master ansteuerbar sein. Da beide Bausteine sich bis auf die CS Leitung alle anderen SPI Leitungen teilen, verringert sich der Verkabelungsaufwand erheblich.

Data Input Output	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6
Clock Number	(0 - 7)	(8 - 15)	(16 - 23)	(24 - 31)	(32 - 39)	(40 - 47)
Write Enable	06h					
Chip Erase	C7h/60h					
Page Program	02h	A23-A16	A15-A8	A7-A0	D7-D0	D7-D0

Tabelle 3: Flash-Baustein Instruktionen für Schreibvorgänge

Aufbau der Write Enable, Chip Erase und Page Program Anweisungen (siehe A.1)

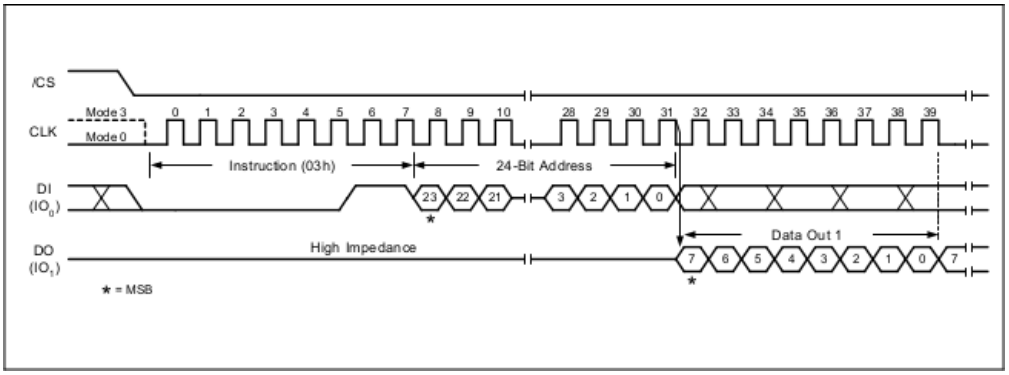

Abbildung 6: Flash-Baustein Read Instruktion Taktung

Die Read Instruktion (03h) bekommt als Parameter lediglich eine 24-Bit Adresse. So kann eine beliebige Anzahl von Bytes bitweise durch das Senden von Taktsignalen ausgelesen werden. (siehe Appendix A.1)

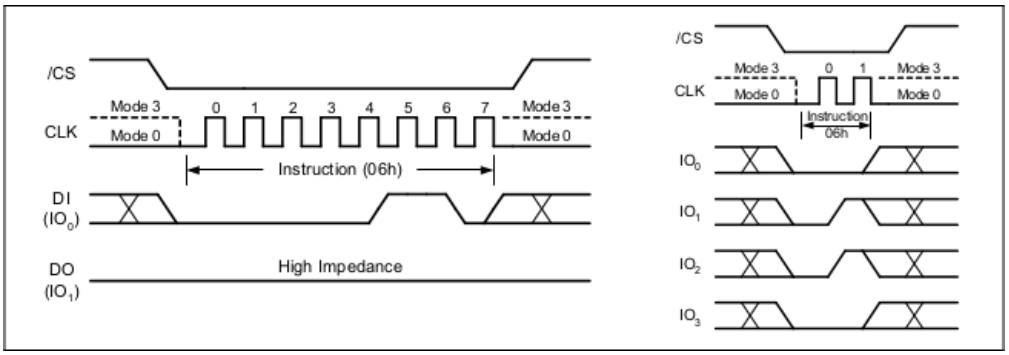

Abbildung 7: Flash-Baustein Write Enable Instruktion Taktung

Die Write Enable Funktion besteht nur aus dem 8-Bit Instruktionscode und versetzt den Speicherbaustein in einen beschreibbaren Zustand. (siehe Appendix A.1)

2.4.3 Speicherbausteine beschreiben

Wenn man das Gerät in den Ausgangszustand bringen möchte, muss man in der Lage sein, vorher angefertigte Kopien des Speichers wieder zurück in die Flash-Bausteine zu schreiben. Bei den Bausteinen handelt es sich um NOR-Speicher, daher sind Schreibzugriffe etwas umständlicher als die reinen Lesezugriffe. Bedingt durch die NOR-Technik können einzelne Bits im Speicherbaustein nur vom Zustand 1 in den Zustand 0 übergehen. Der umgekehrte Weg von 0 auf 1 ist nur durch eine Löschoperation möglich. Das bedeutet wenn man den Baustein neu beschreiben will, dass dieser erst durch eine Löschoperation in einen Zustand gebracht werden muss, in dem er nur 1'en enthält. Erst danach können neue Daten geschrieben werden. Üblicherweise würde man einzelne 256 Byte Blöcke löschen und wiederbeschreiben. Da aber der gesamte Speicher beschrieben werden soll, wird der ganze Baustein durch ein Write Enable (Abbildung 7) gefolgt von einer Chip Erase Instruktion

(Abbildung 8) gelöscht. Daten können dann nach einem erneuten Write Enable durch die Page Program Instruktion (siehe Tabelle 3) in 256 Byte Blöcken geschrieben werden (siehe Abbildung 9).

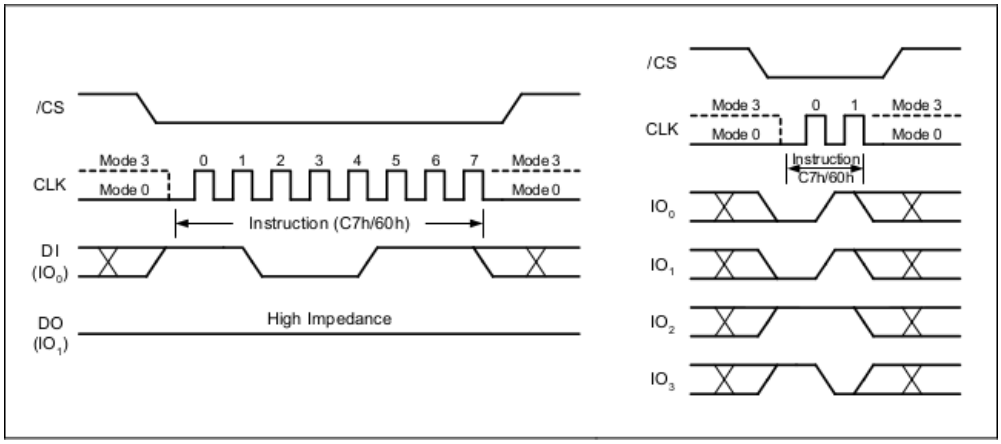

Abbildung 8: Flash-Baustein Chip Erase Instruktion Taktung

Die Chip Erase Funktion besteht nur aus dem 8-Bit Instruktionscode und löscht den gesamten Inhalt eines Speicherbausteins. (siehe Appendix A.1)

Die einzelnen Schritte zum Beschreiben der Bausteine sehen wie folgt aus. Beginn und Ende einer Instruktion wurden dabei nicht explizit aufgeführt.

1. Master sendet Write Enable Intruktion (06h -> MOSI)
2. Master sendet Chip Erase Instruktion (C7h/60h -> MOSI)
3. Master sendet Write Enable Instruktion (06h -> MOSI)
4. Master sendet Program Data Instruktion (02h -> MOSI)
5. Master sendet 24 Bit Adresse (Adresse -> MOSI)
6. Master schreibt Bit seriell auf MOSI
7. Master gibt Clock Signal
8. Master wiederholt 6 und 7

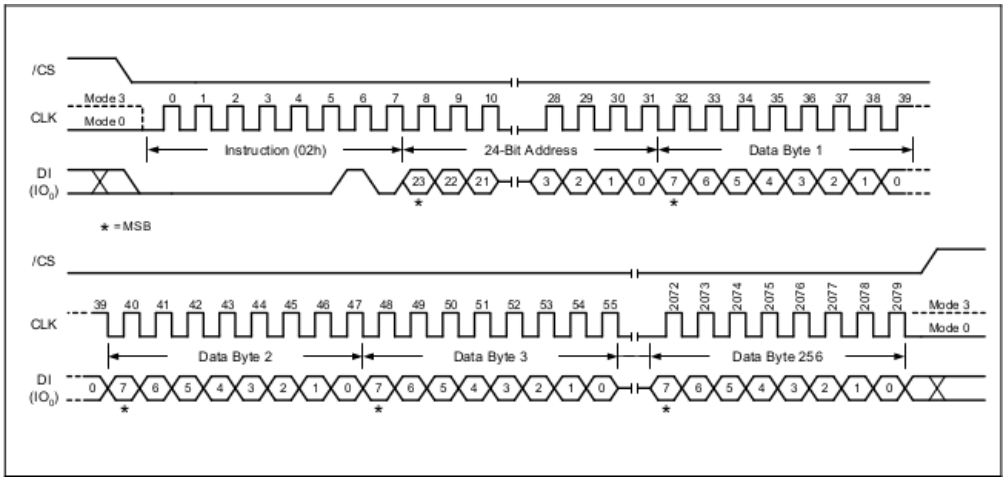

Abbildung 9: Flash-Baustein Page Program Instruktion Taktung

Die Write Funktion bekommt als Parameter eine 24-Bit Adresse, an die Daten geschrieben werden sollen. Auf die Adresse können dann bis zu 256 Bytes zu schreibende Daten folgen. (siehe Appendix A.1)

3 Bedrohungsmodell

Im Folgenden wird der WF-2540 auf Sicherheitsrisiken untersucht, um potentielle Sicherheitslücken zu identifizieren und Bedrohungen einzugrenzen. Es wird untersucht welche Wege einem Angreifer zur Verfügung stehen, um in das System einzudringen, damit der vielversprechendste Angriffsvektor später zielgerichtet analysiert werden kann. Damit soll geklärt werden, ob ein solches System übernommen werden kann und wie hoch der damit verbundene Aufwand für einen Angreifer ist. Ziel ist es Dritten, Entscheidungen über Vorkehrungen und Gegenmaßnahmen zum Schutz der Systeme zu erleichtern. Die hier gewonnenen Erkenntnisse über Angriffspunkte und Schnittstellen unterstützen die späteren Analysen und die geplante Penetration des Systems.

Im ersten Schritt wird zunächst die Architektur genauer betrachtet, um das System und dessen Aktionen besser verstehen zu können. So kann ein Überblick über die Akteure gewonnen werden die mit dem System interagieren und bestimmt werden, welche Berechtigungen sie haben sollten. Mit Hilfe der Informationen aus der Vorbereitung 2.3, können dann die Schnittstellen des Gerätes näher untersucht werden. Im zweiten Schritt wird untersucht, welche Zugriffe möglich sind, wie genau im einzelnen zugegriffen werden kann und welche Akteure dazu die Berechtigungen haben. Darüber wird dann ein Ansatzpunkt für weitere Untersuchungen bestimmt.

3.1 Architekturübersicht

Zunächst wird das System von einem stark abstrahierten Standpunkt aus betrachtet. Diese abstrakte Architekturübersicht wird dann an den relevanten Stellen weiter verfeinert. Das hilft dabei die involvierten Komponenten und Benutzer besser herauszustellen (siehe Abbildung 10).

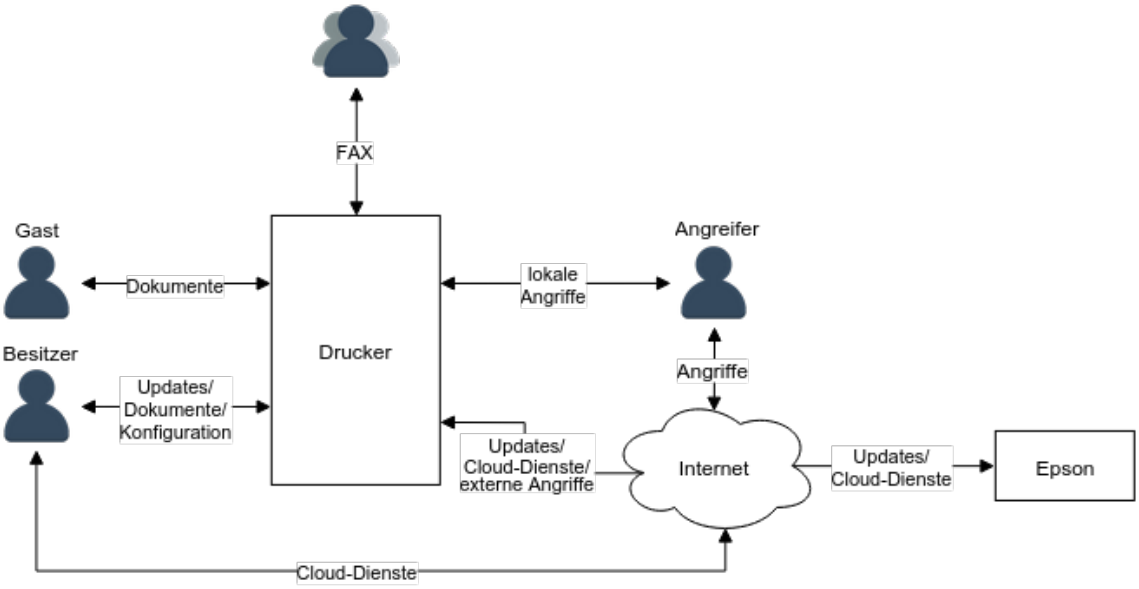

Abbildung 10: Einfache Architekturübersicht des Druckersystems

Abstrakte Übersicht des Multifunktionsgerätes und der mit ihm interagierenden Komponenten und Akteure. Es gibt Nutzer die Zugriff auf das Gerät haben und dessen Funktionen nutzen. Das Gerät kann dabei von außen über FAX und Epsons Cloud-Dienste erreicht werden.

Durch gezielte Beobachtungen des Systems im Betrieb, werden die Verbindungen der Akteure mit dem System konkretisiert. Durch die Beobachtungen der von außen erreichbaren Systemdienste, werden Erkenntnisse über deren internes Zusammenspiel im Gerät möglich (siehe Abbildung 11).

3.2 Akteure

Für die einzelnen Akteure, die mit dem Drucker kommunizieren, muss festgehalten werden, welche Rechte ihnen im System einzuräumen sind. Dazu werden anhand der zuvor erstellten Architekturübersicht die grundlegenden Akteure im Modell identifiziert. Für diese wird dann unabhängig von ihren tatsächlichen Rechten im System festgelegt, was ihnen erlaubt und was untersagt sein sollte. Diese Rechte können später mit den tatsächlichen Rechten verglichen werden.

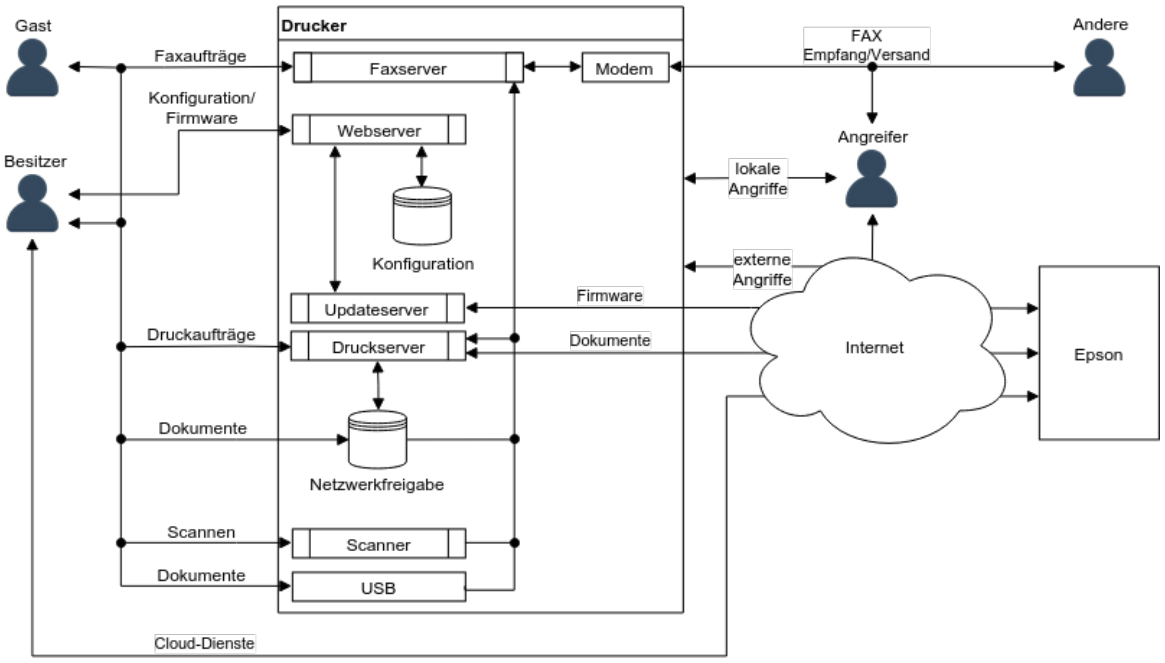

Abbildung 11: Erweiterte Architekturübersicht des Druckersystems

Durch Beobachtung des Systems im Betrieb konnten die Verbindungen der Akteure mit dem Multifunktionsgerät konkretisiert werden. Dabei wurden auch die Beziehungen der beobachteten geräteinternen Komponenten festgehalten.

1. Besitzer
   Der Besitzer darf nahezu die volle Kontrolle über das Gerät haben. Er darf alle vom Gerät angebotenen Dienste nutzen und die Einstellungen des Gerätes einsehen und verändern. Er darf Firmware-Updates auf seinem Gerät durchführen. Die Nutzung der Cloud-Funktionen von Epson erlauben ihm die Verwendung des Gerätes auch ohne physikalischen Zugang.

2. Gast
   Ein Gast befindet sich im gleichen Netzwerk wie das Gerät und verfügt wie der Besitzer über physikalischen Zugang zum Drucker. Er darf als Gast die Grundfunktionalitäten des Gerätes wie Drucken, Scannen, FAX, etc. nutzen. Es sollte ihm jedoch nicht möglich sein, Einstellungen einzusehen oder zu verändern. Die Nutzung des Druckers über die Cloud-Dienste und Firmware-Updates sollten ihm ebenfalls nicht möglich sein.

3. Angreifer
   Der Angreifer hat in unseren Betrachtungen wie schon in der Architekturübersicht erkennbar nicht nur Zugriff auf das Gerät über das Netzwerk, sondern könnte möglicherweise auch physikalischen Zugriff haben. Der Angreifer kann, da er nicht als

solcher erkennbar ist, grundsätzlich nicht vom Gast-Benutzer unterschieden werden. Daher hat er die gleichen Rechte zur Interaktion mit dem System wie der Gast.

4. Hersteller
   Dem Hersteller des Systems, in diesem Fall Epson, werden durch die Nutzung von diversen Cloud-Diensten, erweiterte Interaktionen mit dem System erlaubt. So kann der Hersteller mittels des Cloud-Druck Dienstes für den Kunden Druckaufträge und FAX Funktionalität von außerhalb ansprechen. Im Zuge automatischer Updates ist es dem Hersteller sogar erlaubt, für den Kunden automatisiert Firmware-Updates durchführen. Der Hersteller sollte der einzige sein, der Firmware für Geräte austellen darf.

3.3 Identifizierung

Um zu erfahren wie das System angegriffen werden kann, werden dessen Schnittstellen näher betrachtet. Indem analysiert wird, was über welche Zugangspunkte zum System für wen erreichbar ist, wird eine Übersicht über die potentiellen Ansatzpunkte für Angriffe gewonnen. Diese Zugriffspunkte können hinsichtlich erkennbarer Sicherheitsprobleme in Verbindung mit den erlaubten Zugriffen durch die Akteure genutzt werden um Risiken und Bedrohungen zu identifizieren und einzugrenzen. Dabei werden die Schnittstellen mit dem höchsten Risiko für die Sicherheit des Systems festgehalten (siehe Tabelle 4). Damit soll geklärt werden, welche Akteure mehr Rechte haben, als sie sollten und welche Probleme sich für einzelne Schnittstellen schon auf den ersten Blick ergeben. Zur Übersicht, werden alle Schnittstellen des Systems vollständig im Appendix aufgeführt (siehe A.7).

Als problematisch erweisen sich ungenügend geschützte Schnittstellen, die es erlauben sensible Einstellungen des Systems auszulesen oder zu verändern. Das beinhaltet auch die Vorrichtungen zur Installation von Firmware auf dem Gerät. Bei physikalischem Zugriff auf das Gerät, wird der USB-Typ A Anschluss des Gerätes zum Risiko. Über diesen Anschluss können Systemeinstellungen verändert und Firmware installiert werden. Dabei erfolgt durch das Gerät keine Authentifizierung die eine Autorisierung administrativer Nutzer erlauben würde. Als ähnlich Risikobehaftet, erweist sich das nicht öffentliche ENPC Protokoll. Über ENPC können Informationen über die Konfiguration des Gerätes von jedem Netzwerkteilnehmer unverschlüsselt abgefragt werden. Damit ein Gerät auch ohne direkten physikalischen Zugang gewartet und konfiguriert werden kann, unterstützt das Gerät SNMP. SNMP erlaubt es einem administrativen Nutzer eine passwortbasierte Authentifizierung gegenüber dem System durchzuführen. Die Kommunikation erfolgt aber unverschlüsselt, weshalb das Passwort jederzeit im Klartext übertragen wird. Bruteforce Angriffe auf das Passwort werden nicht erkannt und eingedämmt.

Insbesondere die über Port 80 bereitgestellten Dienste des Gerätes erwiesen sich jedoch als Risikoreich. Über diesen Port werden durch einen selbst entwickelten HTTP Server, sowohl Konfigurationen über ein Webinterface, Konfigurationen durch einen SOAP/XML Service und Firmware-Updates durchgeführt. Die gesamte Kommunikation über diesen Port er-

folgt unverschlüsselt und unterstützt auch keine Authentifizierung die eine Autorisierung administrativer Aufgaben nur für den Besitzer erlaubt.

Zugang	Beschreibung	soll Zugriffe	mögliche Zugriffe	Anmerkungen
TCP / 80	Startseite des Webinterface	Alle	Alle	-
	Konfigurationsseite für Epson Connect-Services	Besitzer	Alle	keine Verschlüsselung, keine Authentifizierung
	Konfigurationsseite für Google Cloud Print-Services			
	Konfigurationsseite für DNS und Proxy			
	Firmware-Update Seite, (Automatisches Firmware-Updates von Epson Servern)			
	Konfigurationsseite für AirPrint			
	Seite für Geräte Informationsübersicht			
	Firmware-Updates durch Update-Tools			
	SOAP/XML Service für Konfiguration durch externe Tools			
UDP / 161	Simple Network Management Protocol	Besitzer	Alle	keine Verschlüsselung
UDP / 3289	(ENPC) proprietäres Binärprotokoll von Epson um Geräteinformationen abzufragen und zu verändern.	Besitzer	Alle	keine Verschlüsselung, keine Authentifizierung
USB Typ A	Systemeinstellungen verändern	Besitzer	Besitzer, Gast, Angreifer	keine Authentifizierung
	Firmware-Updates durch Update-Tools	Besitzer	Besitzer, Gast, Angreifer	keine Authentifizierung

Tabelle 4: Risikobetrachtung der gefährlichsten Systemschnittstellen

Für die Schnittstellen die das höchste Risiko für das System darstellen, werden den erlaubten die tatsächlichen Zugriffsrechte durch Akteure gegenübergestellt. Zusätzlich werden erkannte Sicherheitsprobleme für die Schnittstellen festgehalten.

3.4 Bewertung

Um eine möglichst umfassende Kontrolle über das System zu erlangen, muss der Angriffsvektor mit der höchsten konkreten Gefahr für das System ausgewählt und analysiert werden. Anhand der durchgeführten Identifizierung zeigt sich, dass ein Schutz des Systems vor Angriffen faktisch nicht gegeben ist. Für die Übernahme eines Gerätes hilfreich, erweist sich jedoch insbesondere der Firmware-Update Mechanismus, der von allen Akteuren im System genutzt werden kann. Gelingt es einem Angreifer die Firmware gezielt zu modifizieren, kann er darüber im schlimmsten Fall, volle Kontrolle über Hardware und Software erlangen. Ein solcher Angriffsvektor würde insbesondere, wenn er aus der Ferne ausnutzbar ist, mit dem höchstmöglichen CVSS3-Basiswert von 10 eingestuft werden.

Deshalb wird im Folgenden der Update Mechanismus und die Firmware analysiert und so geklärt ob es einem Angreifer realistisch gelingen kann, diese zu modifizieren um damit die Kontrolle über ein Gerät zu erlangen.

4 Firmware Analyse

Für die Analyse werden die vom Hersteller bereitgestellten Firmware-Updates und die erstellten Kopien der Speicherbausteine im WF-2540 genutzt. Mit diesen Daten werden die Zusammensetzung, Inhalte und Funktionsweise der Firmware und damit aller Software-Komponenten ermittelt. Die Verbindung aus Firmware, Speicherabzügen und Testsystem ermöglicht dann, den Prozess des Aufspielens der Firmware zu verstehen. Die so am Testsystem erarbeiteten Erkenntnisse lassen sich möglicherweise auf ganze Baureihen oder sogar Produktfamilien anwenden.

4.1 Update Mechanismus

Es existieren mehrere Wege Firmware-Updates auf dem Gerät zu installieren. Der Mechanismus ist auf das Austauschen zusammenhängender Speicherbereiche und einzelner Speicherbausteine ausgelegt. Soll daher ein einzelnes Program ausgetauscht werden, muss eines der Dateisysteme oder sogar das Gesamtsystem neu auf die Flash-Bausteine gespielt werden. Eine Überprüfung der Firmware-Version wird dabei nicht vom Gerät, sondern von den Update-Tools durchgeführt. Daher kann dieselbe Firmware ohne weiteres erneut aufgespielt oder in der Version heruntergestuft werden.

Epson sieht neben den automatischen Updates von ihren Servern vor, dass die Endbenutzer über USB oder die Netzwerkschnittstellen Geräte aktualisieren dürfen. Zu diesem Zweck werden Anwendungen zur Verfügung gestellt, mit denen die Updates durchgeführt werden können. Updates sind dabei wahlweise über die USB-Typ-B Schnittelle an der Rückseite des Gerätes oder über LAN und WLAN möglich. Zusätzlich bieten die Geräte einen Recovery Mode, der es erlaubt, ohne lauffähiges Betriebssysytem beispielsweise nach einem missglückten Update, das Gerät mit lauffähiger Firmware wiederherzustellen (siehe 4.1.1).

4.1.1 Recovery Mode

Der Recovery Mode ist ein spezieller Betriebsmodus des Druckers und wird durch das Drücken der Tastenkombination

```
STOP/RESET + LEFT + COPY + POWER
```

im ausgeschalteten Zustand des Systems aufgerufen. Dieser Modus lässt sich zwischen Bootcode und Betriebssystem einordnen und erlaubt das Einspielen von Firmware-Updates über USB, ohne dass ein bootbares Linux vorhanden sein muss (siehe 4.1.2). Dieser Modus ist von Epson nur zum Wiederherstellen defekter Geräte zum Beispiel nach missglückten Updates vorgesehen. Möchte man den Update-Prozess näher verstehen, so ist dieser Modus außerordentlich hilfreich, da er beim Durchführen der Updates Informationen über den aktuellen Status des Updates-Prozesses angezeigt. Nach erfolgreichem Abschluss eines Updates werden sogar Prüfsummen für die verbauten Speicherbausteine angezeigt (Abbildung 12).

```
EPSON PRINTER ROM
Program Update Mode
Finished!
Checksum  806A
Rom Ver.  48.48.LJ05DC
Checksum2 2369
Rom Ver2. LJ05DC
```

Abbildung 12: Recovery Mode Prüfsummen

Nach erfolgreichem Abschluss eines Firmware-Updates werden im Recovery-Mode Informationen über die neue Firmware und die Prüfsummen der Flash-Speicherbausteine angezeigt.

Befindet man sich bereits im Recovery Modus, kann durch Drücken der

```
DOWN
```

Taste für 2 Sekunden ein weiteres Untermenü aufrufen, welches es erlaubt eine einzelne Prüfsumme über alle Flash-Bausteine im Gerät zu berechnen. Die angezeigten Statusinformationen ermöglichen es, die einzelnen Schritte des Updateprozesses näher festzuhalten (Abbildung 13).

Das Gerät liest und prüft der Reihe nach zwei mit IPL bezeichnete Dateien. Da dem Drucker nur die rohe Firmwaredatei als einzelne Datei gesendet wird, werden diese scheinbar durch den Update-Prozess aus der Firmware extrahiert. Tests zeigen, dass, wenn man die Firmare modifiziert und keine Prüfsummen anpasst, dass die IPL Überprüfungen fehlschlagen und das Update mit einer “FILE NOT FOUND”-Meldung abbricht. Nach der Überprüfung der zwei IPL-Dateien, werden diese scheinbar mit dem ersten und zweiten Speicherbausteinen verglichen. Erst danach werden die Speicherbausteine gelöscht und neu beschrieben. Vermutlich geschieht dies, da die Speicherbausteine nur begrenzt wiederbeschrieben werden können. Daher wird vorher geprüft, ob der Inhalt überhaupt ersetzt werden muss. Nachdem die Speicherbausteine beschrieben sind, wird der geschriebene Inhalt nocheinmal auf Korrektheit überprüft. Da nach diesem Schritt sofort die Prüfsummen auf dem Display angezeigt werden, müssen diese im Verifizierungs-Schritt berechnet werden (siehe Abbildung 13).

4.1.2 USB

Software-Updates über die USB Schnittstelle können an dem Gerät nur über den Typ-B Anschluss an der Rückseite erfolgen. Der Typ-A Anschluss an der Vorderseite kann ausschließlich für Mass-Storage Devices verwendet werden und ist scheinbar für das Linux-System nicht sichtbar. Vermutlich existiert daher eine Ansteuerung mit einer eigenen USB-Implementierung von Epson. Updates über USB stehen im Gegensatz zu Updates über die Netzwerkschnitstelle sowohl mit lauffähigem Betriebssystem als auch im Recovery Mode zur Verfügung.

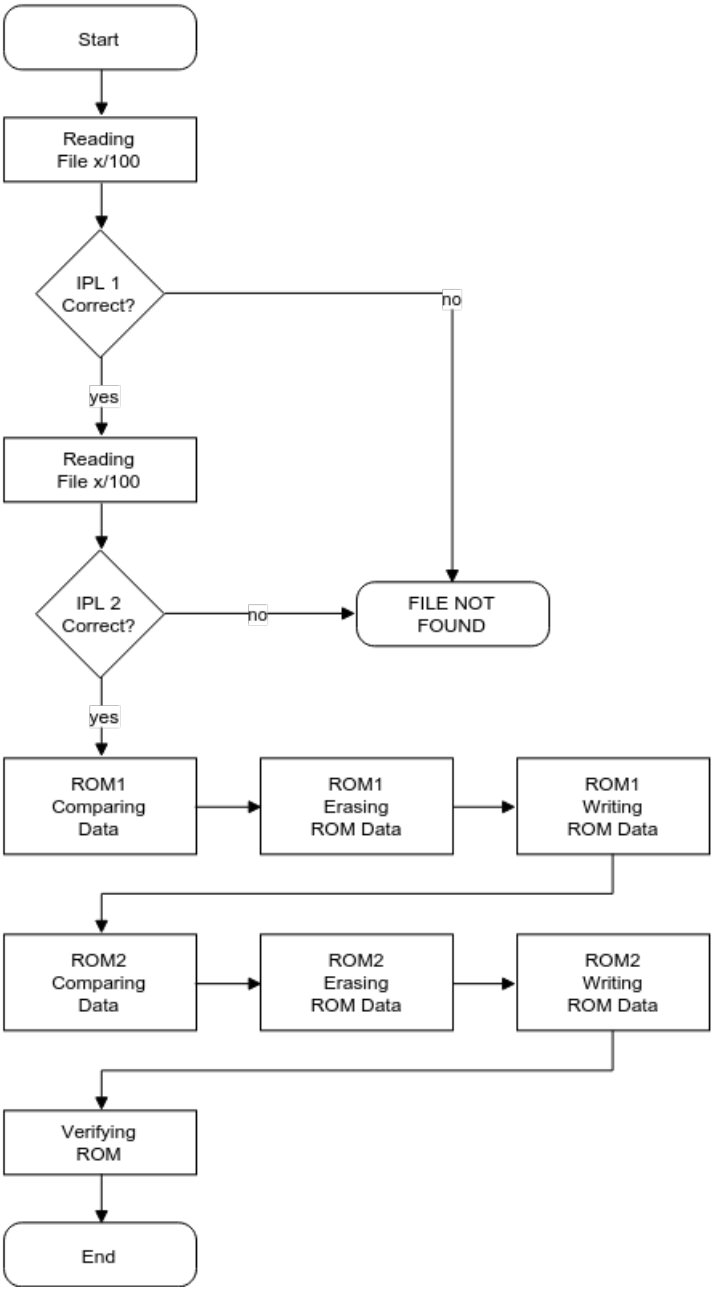

Abbildung 13: Recovery-Mode Firmware-Update Verlauf

Während Firmware-Updates werden im Recovery-Mode Statusmeldungen angezeigt. Diese Statusmeldungen erlauben es, einen groben Überblick über den Update-Prozess zu gewinnen und geben Aufschluss über die Art und Weise wie die Firmware verarbeitet wird und wie viele Prüfsummen möglicherweise eingesetzt werden.

Soll ein Update über USB erfolgen, wird der Drucker zunächst auf das Firmware-Update vorbereitet. Dies geschieht in dem die Anwendung von der das Update ausgeht und der Drucker eine Art Handshake starten. Daraufhin kann die Update-Software scheinbar die gewünschte Aktion mitteilen und der Drucker antwortet mit zwei weiteren unbekannten Datenpaketen (siehe Abbildung 14).

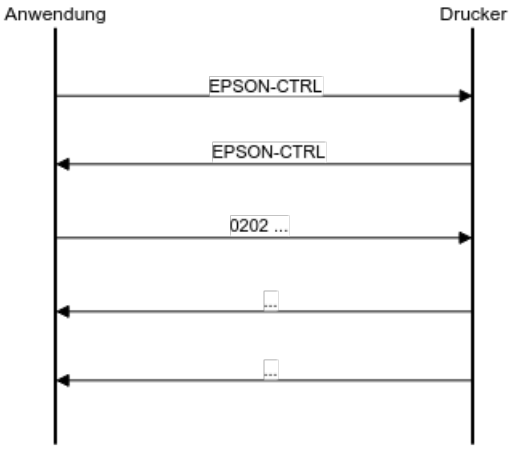

Abbildung 14: Vorbereiten des Firmware-Updates über USB

Beim Durchführen eines Updates über USB, wird dem Drucker zunächst mitgeteilt, dass ein Firmware-Update durchgeführt werden soll. Die Kommunikation mit dem Gerät erfolgt scheinbar über ein proprietäres Binärprotokoll.

Nachdem der Drucker auf das Update vorbereitet wurde, kann mit dem eigentlichen Firmware-Update begonnen werden (siehe Abbildung 15). Dazu wird der Drucker durch einen EPSON-CTRL Handshake auf die Datenübertragung vorbereitet. Sobald das Gerät dann mit fl:01:OK signalisiert, dass es zum Empfang der Firmware bereit ist, kann die Datenübertragung beginnen. Die Datenübertragung wird durch EPSON-DATA Nachrichten eingeleitet auf die dann die Firmwaredatei in 32kByte Blöcken folgt. Sind alle Daten übertragen quittiert der Drucker den Erhalt all dieser Blöcke durch fl:03:OK und beginnt eigenständig mit dem Einspielen des Updates. Die Firmware-Update Tools von EPSON fragen nach der Übertragung der Firmware, durch das Senden von Epson Job Language (EJL)-Kommandos scheinbar permanent nach dem Fortschritt. EJL ist eine von Epson entwickelte nicht öffentliche Erweiterung von PJL. Eine weitergehende Analyse des Aktualisierungsvorgangs mittels USB wurde nicht durchgeführt.

4.1.3 Netzwerk

Updates über das Netzwerk sind über LAN oder WLAN möglich und basieren auf einfachen HTTP Nachrichten (siehe Abbildung 16). Zur Übertragung der Firmware werden POST Nachrichten genutzt (siehe [19]). Da die Updates über Port 80 durchgeführt werden und dieser grundsätzlich Verbindungen von IPADDR_ANY zulässt, kann ein Firmware-Update von außen durch jeden eingeleitet werden. Genau wie bei Updates über die USB

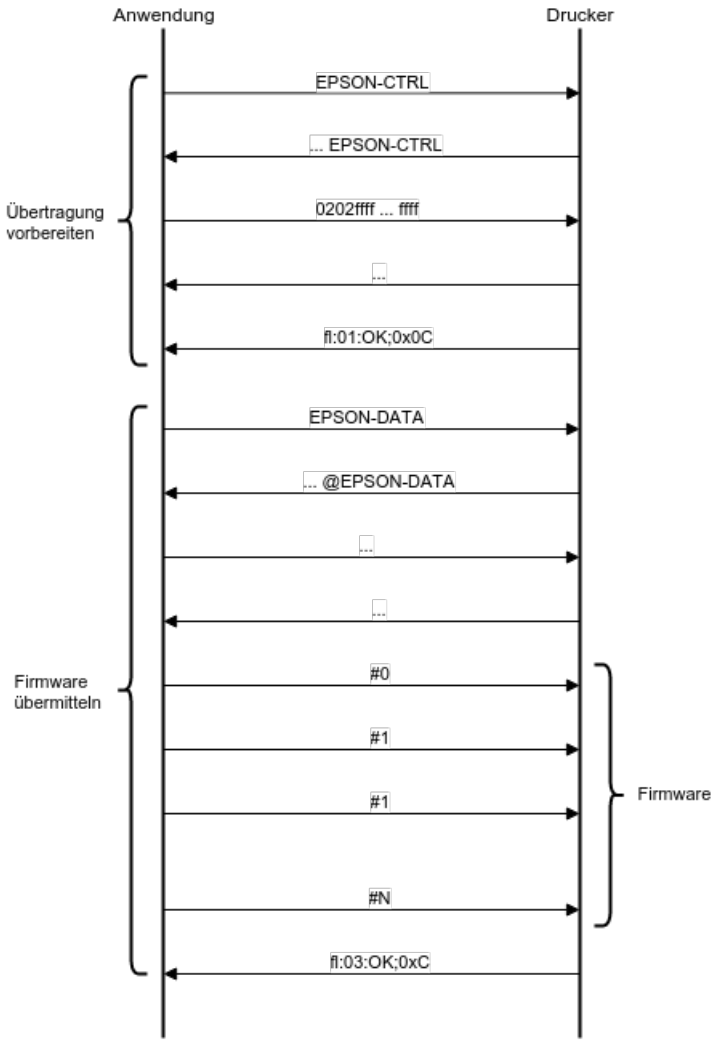

Abbildung 15: Dateiübertragung bei Firmware-Updates über USB

Die Übertragung der Firmware über USB wird durch einen EPSON-CTRL Handshake vorbereitet. Die eigentliche Dateiübertragung wird danach durch EPSON-DATA Nachrichten begonnen und übermittelt die Firmware in 32kB Blöcken. Sowohl die Vorbereitung der Dateiübertragung als auch die Dateiübertragung selbst werden vom Gerät quittiert.

Schnittstelle wird der Drucker auch hier zuerst durch eine einfache HTTP-GET Anfrage auf das Firmware-Update vorbereitet. Nach der Bestätigung durch den Drucker kann die Dateiübertragung beginnen. Ist die Firmware vollständig übertragen quittiert der Drucker den Erhalt mit 204 No Content, da die übertragende Datei nicht durch einen Uniform Resource Identifier (URI) von außen erreicht werden kann (siehe 9.5 POST, [20]). Das Gerät beginnt auch hier automatisch mit dem Einspielen des Updates, nachdem die Übertragung abgeschlossen wurde. Die form-data-Boundary die von Epson genutzt wurde, enhält gegen Ende die Jahreszahl 1999 (siehe Listing 4). Daher vermuten wir, dass der Update-Mechanismus passend zum HTTP/1.1 Request For Comments (RFC) der ebenfalls von 1999 stammt, entstanden ist.

```
POST /DOWN/FIRMWAREUPDATE/ROM1 HTTP/1.1\r\n
Accept: */*\r\n
Content-Type: multipart/form-data; boundary=--------------------------
    EPSONOP2HANAOKAGROUP1999\r\n
Content-Length: 11616476\r\n
Connection: Keep-Alive\r\n
\r\n
--------------------------EPSONOP2HANAOKAGROUP1999\r\n
Content-Disposition: form-data; name="fname"; filename="/DUMMY.DAT"\r\n
Content-Type: application/octet-stream\r\n
\r\n
...
\r\n
--------------------------EPSONOP2HANAOKAGROUP1999--\r\n
```

Listing 4: HTTP-POST Firmware-Upload

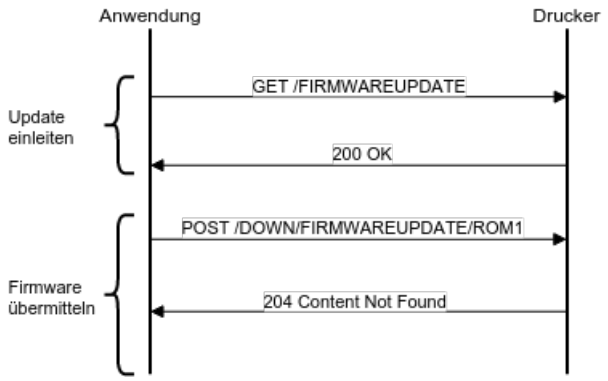

Abbildung 16: Durchführung eines Firmware-Updates über das Netzwerk

Firmware-Updates über die Netzwerkschnittstellen werden mittels HTTP durchgeführt. Das Gerät wird zunächst mit einer GET Anfrage auf das Firmware-Update vorbereitet. Anschließend wird die Firmware durch eine POST Anfrage an den Drucker übertragen. Nach Erhalt der Firmware, beginnt das Gerät selbstständig mit dem Update.

4.2 Tools

Da keine Informationen über die Struktur der Firmware vorliegen und nicht bekannt ist, ob die Firmware gepackt oder sogar verschlüsselt ist, wird zunächst eine automatisierte Analyse durchgeführt. So kann der manuelle Analyseaufwand in Anbetracht von Komplexität und Dateigröße möglichst gering gehalten werden. Ein paar der genutzten Werkzeuge werden im folgenden kurz vorgestellt.

4.2.1 Binwalk

Binwalk ist ein Werkzeug, dass für die Analyse von Firmware entwickelt wurde. Binwalk sucht, ähnlich wie ein File-Carver, nach einfachen Mustern in der Firmware, um diese zu extrahieren. Der Funktionsumfang ist dabei jedoch nicht nur auf einfaches Filecarving beschränkt. Das Tool ist in der Lage, komprimierte Daten sowie bekannte und weitverbreitete Datenmuster wie Lookuptables wichtiger Algorithmen zu erkennen. Es bietet die Möglichkeit nach bekannten Opcode-Mustern zu suchen und unterstützt eine Entropie-Analyse von Dateien.

4.2.2 Firmware Mod Kit

Das Firmware Mod Kit ist eine primär für Linux-basierte Router entwickelte Ansammlung von Programmen und Shell-Skripten, die das Entpacken und Packen einer Vielzahl von bekannten Datei und Firmware-Formaten erlauben. Das Firmware Mod Kit setzt dabei auch auf Programme wie Binwalk, um seine Aufgabe zu erledigen (siehe 4.2.1 Binwalk). Obwohl es eigentlich für Router entwickelt wurde, ist es in der Lage, auch andere Linux-basierte Firmware für beliebige Geräte zu verarbeiten, sofern diese sich aus den unterstützten Datei-Formaten zusammensetzt.

4.3 Firmware Dateiformat

Die Firmware wird von Epson scheinbar ausschließlich in Form von selbstentpackenden Installern für Microsoft Windows Betriebssysteme bereitgestellt. Dabei wird von Epson für jede Firmware-Version ein separater Installer ausgeliefert, der die eigentliche Firmware enthält. Durch manuelles dekomprimieren, können alle im Installer enthaltenen Dateien extrahieren. Jeder Installer enthält die Firmware in ebenfalls wieder ZIP-komprimierter Form als Datei mit der Dateiendung ".efu". Durch erneute Dekompression dieser Datei erhält man die rohe Firmware mit der Dateiendung ".rcx" für das jeweilige Gerät.

4.3.1 Struktur

Die ".rcx" Firmware-Datei ist zu Beginn mit einem Klartext-Header versehen, der dem Firmware-Update Tool von Epson Informationen über den Inhalt der Datei liefert (siehe Listing 5). Der Header erinnert dabei vom Aufbau stark an INI-Konfigurationsdateien. Das Update-Tool selbst ist scheinbar nicht in der Lage die eigentliche Firmware-Datei auszuwerten, um so z.B. auf die Firmware-Version zu schließen und greift daher auf den

Header zurück. Der Header wurde bei den mitgeschnittenen Firmware-Updates niemals mit übertragen (siehe Appendix A.2).

```
RCX
SEIKO EPSON EpsonNet Form
[A]
1="2"
2="11"
13="3"
16="*.LJ*.FY12"
[B]
1="TRUE"
2="TRUE"
3="10"
4="400"
5="FALSE"
6="FALSE"
[D]
1="Firmware"
3="48.48.LJ05DC.FY12"
4="$(0,12)"
5="TRUE"
7="$(0,5),$(10,1)+$(11,1)+$(8,2)"
[Z_1]
5="7413760"
[Z_2]
5="4202496"
```

Listing 5: Klartext-Header der LJ05DC Firmware

Da der Klartext-Header für den eigentlichen Update Prozess irrelevant ist, wird er von der weiteren Analyse ausgeklammert und alle folgenden Analysen werden auf Firmware durchgeführt, bei der, der Header entfernt wurde. Zunächst muss eine strukturelle Übersicht über die Datei gewonnen werden, damit relevante Regionen identifiziert und analysiert werden können. Dazu wird ein Entropie Graph der Firmware-Datei mit Binwalk erzeugt. Die Entropie beschreibt dabei grundsätzlich die Zufälligkeit der Daten. Eine hohe Entropie oder auch ein hoher Informationsgehalt, deutet dabei oft auf komprimierte oder verschlüsselte Inhalte hin.

Mithilfe des in Abbildung 17 dargestellten Graphen, lassen sich die relevanten Abschnitte der Firmware identifizieren und in der Datei zur näheren Betrachtung exakt lokalisieren. Abgesehen vom Speicherbereich 0 - 1 MB weisen alle erkennbaren Datenbereiche aufgrund von Komprimierung hohe Entropiewerte auf (Abbildung 17).

Mit diesen Informationen erhält man einen genauen Überblick über die Struktur der Firmware. Die dabei identifizierten Bereiche werden durch Padding mit 0-Bytes voneinander getrennt. Die Firmware enthält darüberhinaus zwei IPL-Header, die auch schon bei der Betrachtung des Recovery-Mode in den Statusnachrichten vorgekommen sind.

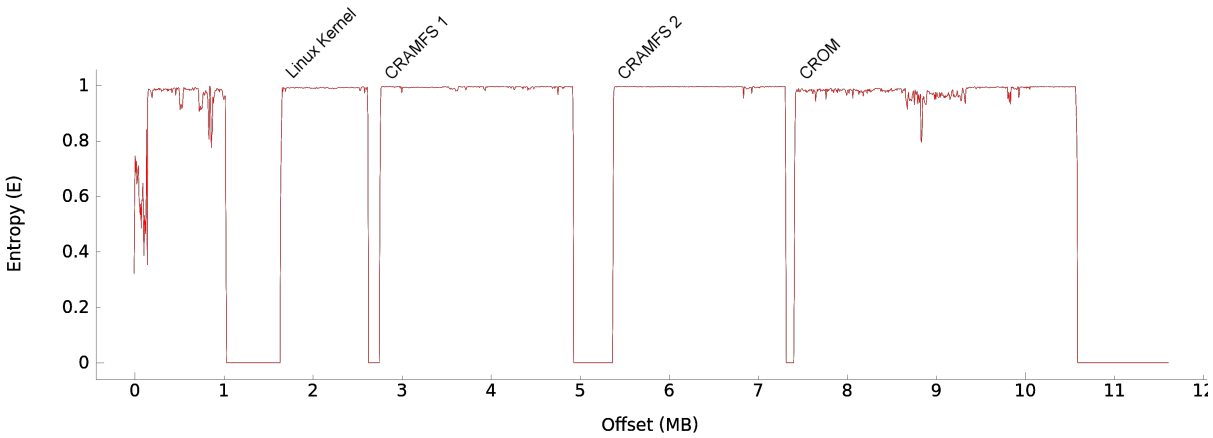

Abbildung 17: Entropie Analyse der LJ05DC Firmware des WF-2540

Der Entropie Graph der Firmware beschreibt für jede Position der Datei die Zufälligkeit der Daten. Ein hoher Entropiewert deutet dabei oft auf komprimierte oder verschlüsselte Inhalte hin. Mit diesen Informationen kann man Teilbereiche identifizieren und einfacher die Struktur analysieren.

4.3.2 IPL Header

Die IPL-Header beschreiben den eigentlichen Aufbau der Firmware. Ein Header beschreibt dabei, welche Daten aus der Firmware wie auf einen Speicherbaustein geflasht werden sollen. Die untersuchte Firmware enthält für jeden genutzten Speicherbaustein jeweils einen Header. Durch die Analysen diverser Firmware-Dateien konnten zwei verschiedene Arten von IPL-Headern mit strukturellen Gemeinsamkeiten identifiziert werden.

Der überwiegend eingesetzte Header beginnt, wie in Abbildung 19 zu sehen, mit dem Magic Byte String “EPSON IPL”. Im Header ist jeweils ein Klartext Prefix als 2 Byte Null-terminierter String enthalten. Beispielsweise “LJ” aus der Firmware-Version “LJ05DC_48_48”. Auf das Prefix, folgt die Länge des Headers in Bytes. Der restliche Header teilt sich dann in verschiedene Records auf, wobei jeder Record einen eigenen Bereich der Firmware beschreibt. Records beginnen mit einem Record-Type gefolgt von einer Prüfsumme für den vom Record beschriebenen Datenbereich.

Die Position der Daten des ersten Records eines Headers beginnt implizit 4kB d.h. 0x1000 hinter dem Beginn des IPL-Headers. Die Länge des Datenbereiches, der vom Record beschrieben wird, ist durch das Längenfeld eines jeden Records bestimmt. Hinter den Daten der einzelnen Records werden 0-Bytes als Padding bis zum nächsten Datenbereich eingesetzt. Das Ende der Daten eines Records ist der Anfang der Daten des nächsten Records. Enthält die Firmware mehr als einen IPL-Header muss das Ende des letzten Datenbereiches eines Headers der Anfang des nächsten IPL-Headers sein. Je nach Ausführung des IPL-Headers können auf die Länge eines Records noch 20 Byte (160 Bit) Daten fol-

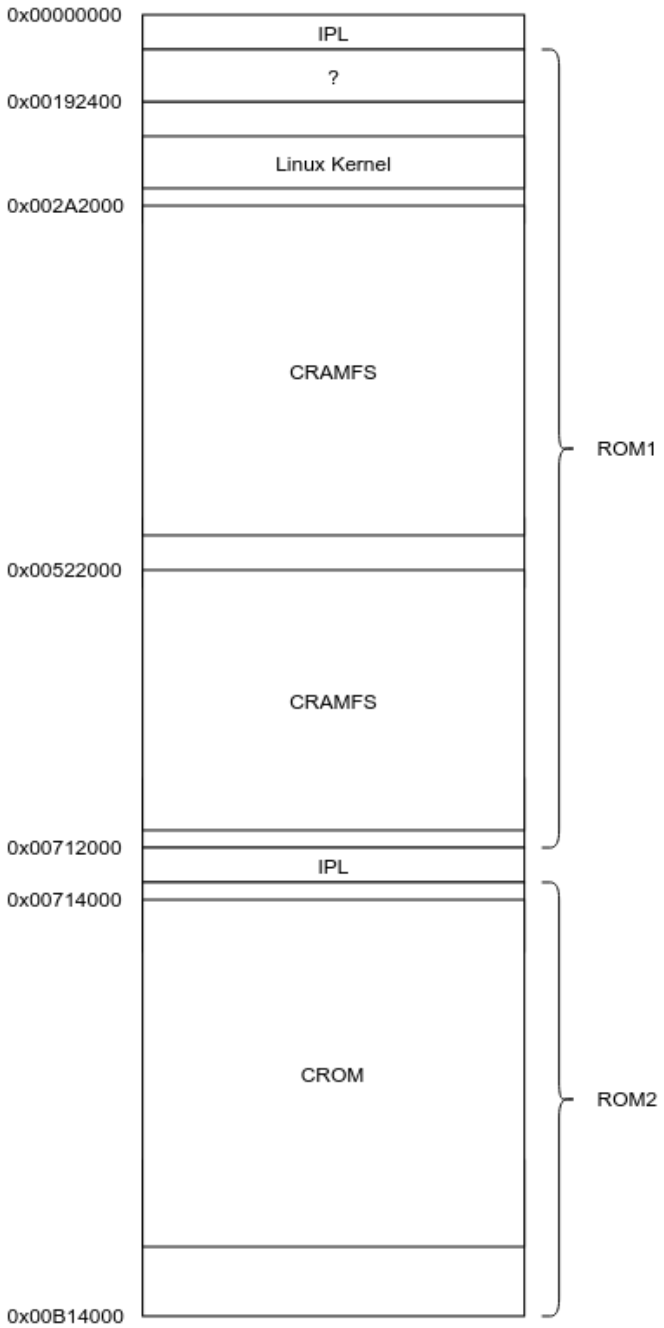

Abbildung 18: Struktur der LJ05DC Firmware des WF-2540

Auf Basis der durchgeführten Entropie-Analyse und des resultierenden Graphen aus Abbildung 17, können die einzelnen Bestandteile der Firmware manuell identifiziert und untersucht werden.

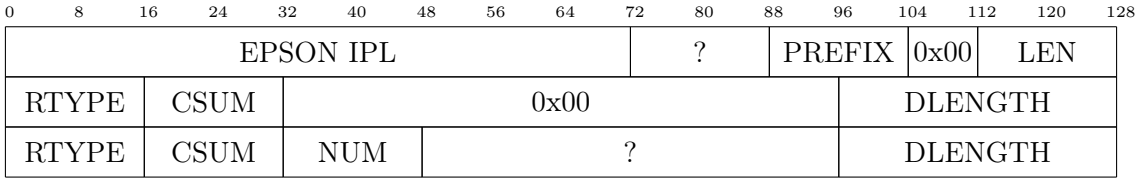

Abbildung 19: Strukturübersicht IPL-Header

Der überwiegend auftretende Header setzt sich aus Magic-Bytes, dem Firmware-Prefix und der Header-Länge sowie Records zusammen. Diese Records bestehen aus Record-Type RTYPE, einer Prüfsumme des vom Record beschriebenen Datenbereichs CSUM, der Länge des Datenbereiches DLENGTH und einer Headernummer im letzten Record eines Headers NUM.

gen. Die Form der Records wird dabei nicht allein nur durch den Record-Type, sondern auch durch den IPL-Header bestimmt. Dies ergibt sich aus dem Umstand, dass identische Record-Typen mit und ohne 160 Bit Datenfeld existieren (vgl. Abbildung 19 und 20).

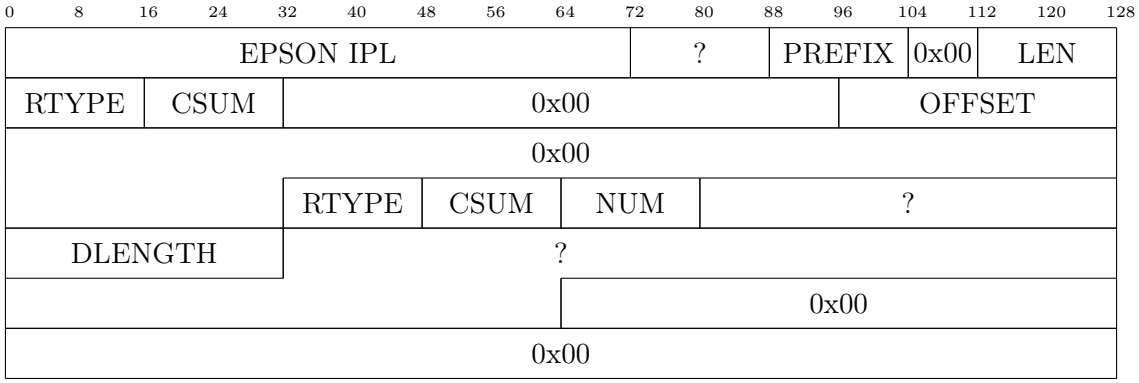

Abbildung 20: Strukturübersicht IPL-Header mit 160Bit Datenfeldern

Der Header mit Datenfeldern ist im Aufbau mit Abb. 19 nahezu identisch. Er enthält nur zusätzlich in jedem Record 160 Bit Datenfelder, die auf die Länge der Daten DLENGTH folgen. Bei unseren Untersuchungen war das Datenfeld des ersten Records dabei immer mit Null-Bytes gefüllt.

Betrachtet man die Header mit 160 Bit Einträgen hinter den Längenfeldern, so fällt auf, dass für den ersten Record des Headers statt Daten immer 20 Nullbytes eingefügt werden. Eine Länge von 160 Bit weisen üblicherweise SHA1 Prüfsummen auf. Es ist jedoch nicht gelungen Datenbereiche zu finden die zu diesen Prüfsummen passen. Die in Abbildung 19 zu sehenden unbekannten Bereiche des Headers sind vermutlich Flags für den Header und jeweils Flags für die einzelnen Records. Der jeweils letzte Record eines IPL-Headers enthält nach der Prüfsumme die Nummer des IPL-Headers in der Firmware. Diese Durchnummerierung der Header beginnt dabei mit 0. Eine Besonderheit dieser Header ist, dass die Daten, die durch den ersten Record eines jeden Headers beschrieben werden, zwischen den Headern einer Firmware immer identisch sind.

Die zweite aber strukturell ähnliche Ausprägung des IPL-Headers konnte bei den Analysen nur ein einziges mal in der Firmware des WF-R8590 gefunden werden. Dieser Header beginnt mit einem geänderten Magic-Byte String und das terminierende Null-Byte des Prefix wurde im Vergleich zum Header in Abbildung 19 entfernt. Dafür wurde ein Byte vor dem Prefix hinzugefügt. Der Header setzt sich scheinbar ebenfalls aus Records zusammen. Es konnten jedoch keine Längenfelder oder Offsets in diesen Records identifiziert werden (siehe Abbildung 21).

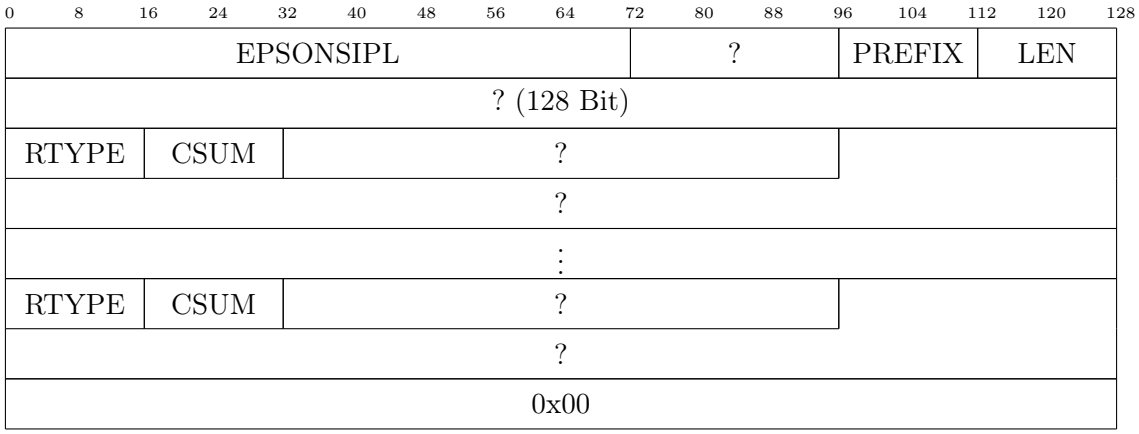

Abbildung 21: Strukturübersicht erweiterter IPL-Headers

Diese Form des IPL-Headers konnte nur einmal in der Firmware des WF-R8590 nachgewiesen werden. In dieser Form wurde das 0-Byte hinter dem Prefix entfernt und der Aufbau der Records geändert. Das erste üblicherweise mit 0-Bytes gefüllte 160 Bit Datenfeld, ist hier 128 Bit lang und enthält Daten.

In Kombination mit den Speicherabzügen der Flash-Bausteine konnte bestimmt werden, welche von den IPL-Headern beschriebenen Datenbereiche durch ein Update auf welche Speicherbausteine geschrieben werden (siehe Abbildung 22). Dabei fällt auf, dass von den zwei Records pro Header immer der letzte auf einen Speicher-Baustein geschrieben wird. Die ersten 65kB des Bootspeichers scheinen dabei für Bootcode und Recovery-Mode reserviert zu sein. Das JFFS2 Dateisystem am Ende des Bausteins ist nicht in der Firmware enthalten (siehe 4.5).

4.3.3 Prüfsummen

Wie in 4.3.2 gezeigt, kann ein einzelner IPL-Header mehrere Records mit eigenen Prüfsummen enthalten. Die Prüfsummen werden dabei über den ganzen Datenbereich der Records durch einfaches Summieren der Bytes als 2 Byte Integer ohne spezielle Behandlung des Überlaufes gebildet.

$$s = \left(\sum_{i=0}^{N} f_i \right) \mod 2^{16} \tag{1}$$

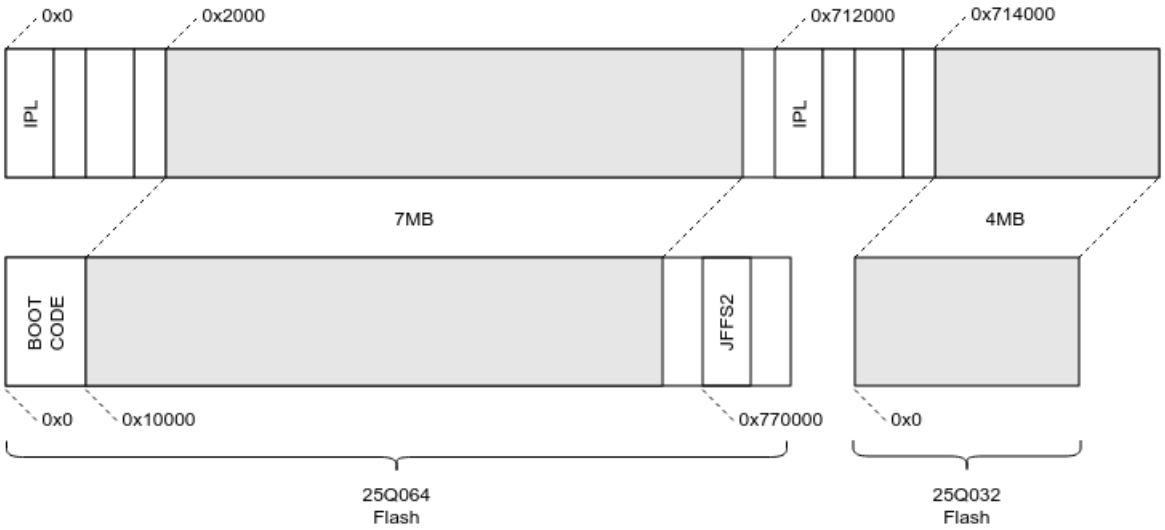

Abbildung 22: Übergang der LJ05DC Firmware in den Flash des WF-2540

Die IPL-Header beschreiben, welche Datenbereiche aus der Firmware auf die Speicherbausteine geschrieben werden.

Der Inhalt der Datenbereiche wird mit 0-Bytes auf die gewünschten Längen gefüllt und hat daher auch keinen Einfluss auf die Prüfsummen. Welche Bereiche der Firmware von den einzelnen Prüfsummen abgedeckt werden, ist in Abbildung 23 zu sehen.
Prüfsummen für die Header oder einzelne Records der Header sind nicht vorhanden. Vergleicht man die Prüfsummen der Records im IPL-Header mit den Prüfsummen, die nach einem erfolgreichen Update durch den Recovery-Mode angezeigt werden, so fällt auf, dass die Prüfsumme des ersten ROM abweicht (siehe Abbildung 12). Das liegt daran, das der Recovery-Mode nur Prüfsummen über ganze Speicherbausteine bildet und anzeigt. Da der zweite Speicherbaustein exakt die gleichen Daten enthält wie vom IPL-Header beschrieben, wird hier auch die erwartete Prüfsumme angezeigt.

Mit diesen Informationen über die Prüfsummen können nun alle Teile der Firmware beliebig modifiziert werden. Tests haben gezeigt, dass es scheinbar keinen weiteren Mechanismus gibt, der Veränderungen an der Firmware registriert. Der Einsatz einer einfachen Summe über Bytes als Prüfsumme in Verbindung mit dem Padding durch 0-Bytes macht es einem Angreifer ausgesprochen einfach, unbemerkt Modifikationen an der Firmware vorzunehmen. Ein Angreifer könnte sogar beliebige Modifikationen vornehmen und durch einfaches Anpassen des 0-Byte Padding, jede beliebige Prüfsumme erzeugen.

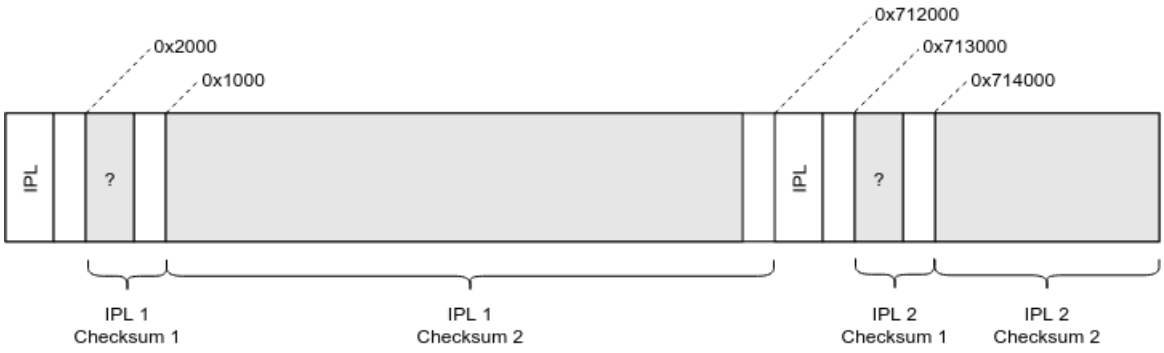

Abbildung 23: Prüfsummen in der LJ05DC Firmware

Die LJ05DC Firmware des WF-2540 enthält zwei IPL-Header mit jeweils zwei Records. Jeder Record beschreibt einen Datenbereich mit eigener Prüfsumme.

4.4 Bootprozess

Der Bootloader des Druckers befindet sich zusammen mit dem Code für den Recovery-Mode in den ersten 64kB des 25Q064 Flash-Bausteins (siehe Abbildung 22) und wird durch die Firmware-Updates nicht überschrieben. Der Bootloader konnte bei den Analysen keinem öffentlich verfügbaren Bootloader für ARM Platformen zugeordnet werden. Daher handlet es sich in Verbindung mit dem Recovery Mode (siehe 4.1.1) um einen proprietären Bootloader. Der eigentliche Code zum Laden des Linux-Kernels vom ROM in den RAM scheint vom Rest des Bootloaders getrennt zu sein und befindet sich 8kB vor dem eigentlichen Kernel in der Firmware. So kann kernelspezifischer Code für jeden Kernel separat bereitgestellt werden und erlaubt somit auch das Laden anderer sich vom Linux-Kernel unterscheidender Kernel. Sofern der Anwender nicht den Recovery Mode auslöst, lädt der Bootloader nach der Initialisierung der Hardware den Linux-Kernel. Der Kernel wurde dazu über Parameter mit einem festen Pfad für ein Boot-Skript ausgestattet.

```
root=/dev/mtdblock1 console=ttyS0 mem=25M init=/root/PreBoot
```

Listing 6: Kernel-Parameter der LJ05DC Firmware

Neben der Firmware des WF-2540 wurden noch weitere Firmware-Dateien für verschiedene andere Durcker überprüft. Alle geprüften Drucker enthalten Reste von Dateien und Skripten für einen Runlevel-basierten Start. Dieses System wurde jedoch scheinbar aufgegeben und durch ein einzelnes Boot-Skript ersetzt.

Das über die Kernel-Parameter festgelegte Speicherlimit von 25 MB deutet darauf hin, dass beim Systemstart Echtzeitkomponenten geladen werden, die neben dem Linux existieren. Dabei soll vermutlich verhindert werden, dass diese gleichzeitig auf dieselben Speicherbereiche zugreifen. Da jedoch 64 MB Hauptspeicher verbaut wurden, scheint ein Limit von 25 MB für das Linux-System als ausgesprochen niedrig.

4.4.1 Boots-Skript

Das Boot-Skript des Gerätes sorgt für die Einrichtung des Dateisystems, setzt Systemeinstellungen, lädt Kernelmodule und startet den größten Teil der Anwendungen auf dem System. Schlussendlich wird ein zweites Skript gestartet, welches die zentrale Anwendung des Systems startet (siehe Abbildung 24).

```
#!/bin/sh
#
# PreBoot
#
#

# PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/local/bin
PATH=/sbin:/usr/sbin:/bin:/usr/bin:/usr/local/bin
export PATH

#

mount -t proc   proc           /proc
mount -t sysfs  sysfs          /sys
mount -t tmpfs  tmpfs          /tmp
mount -t usbfs  usbfs          /proc/bus/usb
mount -t devpts devpts         /dev/pts
mount -t tmpfs  none           /var/run
mount -t tmpfs  none           /tmp
mount -t cramfs /dev/mtdblock2 /opt/nwsoc
mount -t jffs2  /dev/mtdblock3 /opt/nwsoc_data

#unaligned access "User␣faults"
#0: "ignored"
#1: "warn"
#2: "fixup" fixup in kernel handler
#3: "fixup+warn"
#4: "signal"
#5: "signal+warn"
echo 3 > /proc/cpu/alignment

# console log level change

echo 3 3 1 7 > /proc/sys/kernel/printk
#echo 7 6 1 7 > /proc/sys/kernel/printk
#echo 16 > /proc/sys/net/ipv4/tcp_max_syn_backlog

echo "version␣infomation"
echo -n "System␣"
cat /opt/version/k
echo "␣"
echo -n "Apprication␣"
cat /opt/version/a
echo "␣"
echo "␣"
```

```
echo "Load␣modules␣......."
#/usr/sbin/ipaccel_load.sh
/usr/sbin/idc_load.sh

/bin/mknod /tmp/ttyAGS3 c 62 67
/sbin/insmod /lib/modules/lsimodem.ko
/sbin/insmod /lib/modules/lsiserial.ko
/usr/sbin/faxdrv 1 &

echo "Starting␣NWDomain..."

if [ -f /opt/nwsoc/NWControl ]; then
        /etc/rc3.d/S99NWControl
echo "nomal␣mode␣finish."
else
echo "failed␣!!"
fi


/bin/sh

# end of script
```

Listing 7: WF-2540 Boot-Skript aus der LJ05DC Firmware

4.5 Dateisysteme

Die für den WF-2540 erhältliche Firmware enthält zwei CRAMFS Dateisysteme. CRAMFS ist ein einfaches komprimiertes RAM Dateisystem, welches lediglich Lesevorgänge implementiert und keine Unterstützung für Schreibvorgänge besitzt. Eines der CRAMFS Dateisysteme wird über die Kernel Parameter als Wurzelverzeichnis zum Booten eingehängt und enthält hauptsächlich alle zum Betrieb des Linux benötigten Skripte, Kernelmodule, Programme und Bibliotheken. Das zweite CRAMFS Dateisystem wird unter /opt/nwsoc in das Dateisystem eingehängt und enthält Konfigurationsskripte und Firmware für das WiFi-Modul. Zusätzlich enthält es ein Startskript für Epsons proprietäre Software und die vom Skript gestartete Anwendung, welche nahezu alle Systemfunktionalität in sich vereint.

Betrachtet man nicht nur die Firmware, sondern auch die Abzüge der Speicherbausteine, so fällt auf, dass es noch ein drittes Dateisystem gibt, welches auch im Boot-Skript des Gerätes gemountet wird. Dabei handelt es sich um ein JFFS2 Dateiystem, welches gerätespezifische Konfigurationen wie z.B. MAC-Adresse, Gerätenummer und WLAN-Konfigurationsdaten enthält. Dieses Dateisystem scheint nicht in der Firmware enthalten zu sein. Das legt nahe, dass es vom Hersteller bei der initialen Installation mit der Gerätenummer und anderen Daten befüllt wird.

Um an den Inhalt der CRAMFS-Dateisysteme zu gelangen, können diese mit den entsprechenden CRAMFS-Tools normalerweise direkt gemountet oder auch entpackt wer-

den. Versuche mit verschiedenster Firmware zeigten jedoch, dass für viele der CRAMFS-Dateisysteme keine der beiden Methoden funktioniert. Es konnten zunächst aufgrund doppelter Dateisystemeinträge und anderer Anomalien in den Dateisystemen nie alle Dateien extrahiert werden. Um an alle Inhalte zu gelangen, wurden Modifikationen am cramfschk Tool vorgenommen, die das Entpacken der Dateisysteme ermöglichen (siehe Appendix A.3).

Wie in Abbildung 18 zu sehen ist, gibt es auf dem zweiten Speicherbaustein eine Art Dateisystem vom Typ CROM. Der Inhalt dieses Datenbereiches konnte jedoch nicht extrahiert werden.

4.6 Software

Epson setzt neben einem 2.6.18 Linux-Kernel weitere freie Software für den Betrieb des Systems ein. Für die Grundfunktionalität des Systems kommt ein BusyBox v1.7.2 aus dem Jahr 2012 zum Einsatz. Busybox ist ein Projekt, dass eine Vielzahl von Programmen, die für den Betrieb eines Linux-Systems benötigt werden, in minimalistischer Form in einer einzigen Anwendung vereint. Um die Größe und Komplexität weiter zu reduzieren, wurde die leichtere uClibc in der Version 0.9.29 von 2008 statt der deutlich komplexen glibc Bibliothek eingesetzt. uClibc auch μClibc als Kurzform von microcontroller C library, ist eine Bibliothek, die ursprünglich für den Einsatz auf Microcontrollern ohne MMU entstanden ist. uClibc ist darauf ausgelegt, so viel Funktionalität wie möglich auf möglichst kleinem Platz zu bieten. Um Platz zu sparen, werden im Vergleich zur glibc dabei Features entfernt und die Größe auf Kosten der Performance optimiert (siehe [21]).

Die zentrale Anwendung des Systems ist die /opt/nwsoc/nwsoc Anwendung. Dieses proprietäre Programm scheint alle nach außen sichtbaren Funktionen des Gerätes zu implementieren. Es startet alle auf dem System erreichbaren Dienste (siehe 4). Somit ist das Programm zuständig für alle vom Gerät gesprochenen Protokolle, die Druckvorgänge, FAX, Cloud-Funktionalität, Firmware-Updates und vieles mehr. Durchsucht man die nwsoc-Anwendung nach Strings, findet man eine Art Kommandozeile für das Programm (Listing 8). Versuche diese Schnittstelle zu nutzen waren nicht erfolgreich und hatten entweder keine Reaktion oder Abstürze der Anwendung zur Folge. Wenn Systemeinstellungen z.B. an Netzwerkschnittstellen vor dem Start von nwsoc verändert werden, stürzt die Anwendung ab oder das Gerät schaltet sich aus. In beiden Fällen ist das Gerät erst nach dem Trennen der Stromversorgung wieder nutzbar.

```
Launching Console Menu.
Input     'r' : Reboot.
          'R' : Reset settings and reboot.
          'a' : display current IP address.
          'm' : display current MAC address.
          'f' : show /proc/meminfo.
          '' : run shell command'l' : List current module status's' : statussheet
              output'1' : wcif debug mode
```

Listing 8: nwsoc Kommandos

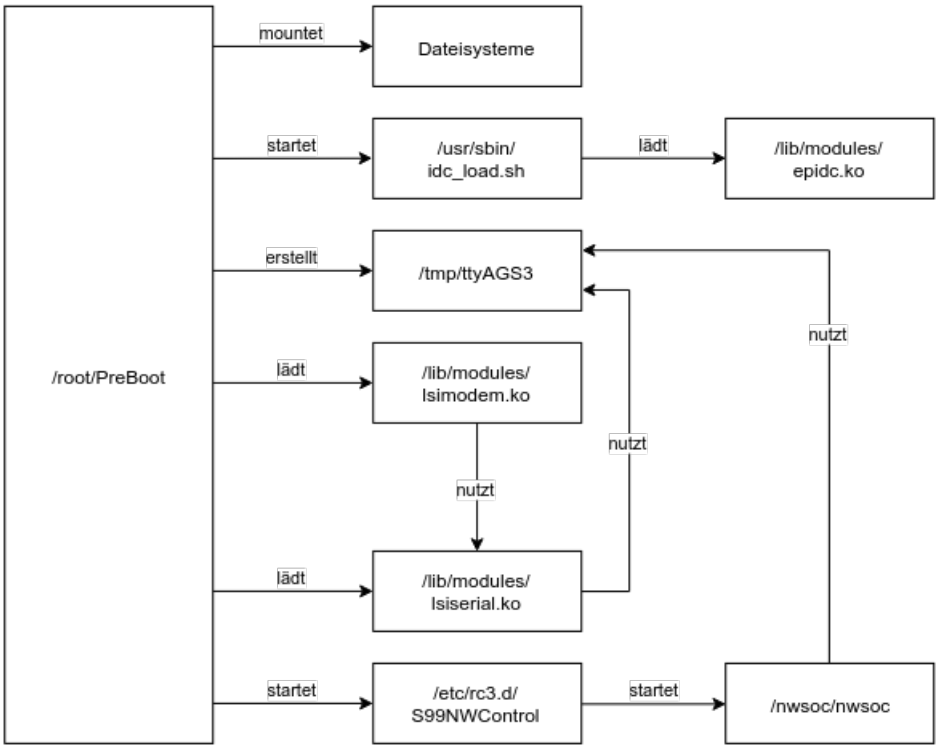

Abbildung 24: Übersicht der Softwarekomponenten

Ausgehend vom Boot-Skript werden alle Softwarekomponenten des Systems geladen. Alle relevanten Dienste werden dabei durch die nwsoc Anwendung bereitgestellt, die durch das NWControl Skript gestartet wird.

nwsoc scheint eine Reihe von SSL-Zertifikaten zu nutzen, die neben der Anwendung unter /nwsoc/nwsoc_RootCert.pem platziert wurden. Welche dieser Zertifikate von der Anwendung wofür genutzt werden, konnte nicht genau bestimmt werden. Die Auswertung zeigte jedoch, dass Zertifikate enthalten sind, die von 1996 bis 2036 gültig sind und teilweise auf die SHA1 Hashfunktion mit 1024 Bit RSA setzen. Neben der nwsoc Anwendung gibt es noch die faxdrv-Anwendung, die scheinbar dafür sorgt dass das Modem vor der Nutzung richtig eingerichtet wird.

Das System lädt beim Startvorgang drei Kernelmodule. Zwei dieser Kernelmodule sind für die FAX-Funktionalität des Gerätes zuständig. Das Modul lsimodem.ko stellt den Modem-Treiber bereit und das Modul lsiserial.ko sorgt dafür, dass dieses Modem als serielle-Konsole nutzbar gemacht wird. Die Funktion des dritten Kernelmodules ist uns unbekannt. Es handelt sich dabei um epidc.ko und meldet sich beim Laden über den Kernel-Ringpuffer mit "Epson Interdomain Communication Driver".

5 Packen

Zum Erstellen eigener Firmware wurden Tools entwickelt und eine Cross-Compiler Toolchain erstellt, damit zusätzliche Software für das Testsystem erzeugt werden kann. Aufgrund der komplexen Einrichtung einer Cross-Compilation-Umgebung und aller damit verbundenen Tools und Bibliotheken, wurde diese unter Einsatz des Buildroot-Projektes erstellt. Versuche das Gerät brauchbar zu virtualisieren, sind aufgrund der starken Anbindung an die Hardware gescheitert.

5.1 Buildroot

Buildroot ist eine Sammlung von Skripten und Makefiles, die es erlauben ein eigenes embedded Linux System über ein Kommandozeilen-Interface zusammenzustellen und zu generieren. Mit Buildroot ist es dabei möglich, nahezu alle benötigten Cross-Compiler Toolchains für diese Systeme zu erzeugen, sowie automatisiert Kernel, Bootloader und das Root-Dateisystem erstellen zu lassen. Buildroot stellt dabei für viele Benutzer den bevorzugten Weg dar, um die Toolchain für uClibc zu erstellen, die von den gleichen Entwicklern gepflegt wird, wie Buildroot selbst.

5.2 Firmware

Für das Erstellen und modifizieren von Firmware wurde eigens entwickelte Software eingesetzt. Mit dieser Software kann eine beliebige Firmware entpackt, nach eigenen Wünschen modifiziert und wieder gepackt werden. Dabei muss besonders auf die Größenrestriktionen der einzelnen Geräte acht gegeben werden, damit die CRAMFS Dateisysteme in den Hauptspeicher passen und nicht zu groß für die Flash-Bausteine werden. Werden eigene Kernel erstellt, können diese sich an der Kopie der Konfigurationsdatei zum Erstellen

des Kernels aus dem original Dateisystem des Druckers orientieren (siehe Appendix A.6). Ein angepasster Kernel kann dann mit der Toolchain compiliert werden. Wird ein eigener Kernel genutzt muss dieser die gleichen Ladeaddressen enthalten, wie der ursprüngliche Druckerkernel. Versucht man den Kernel auszutauschen, kann dies jedoch zu starken Konflikten mit den Kernelmodulen und Treibern im System führen.

Mit den in der Analyse gewonnen Kenntnissen über die IPL-Header (Kapitel 4.3.2) kann Firmware nach eigenen Wünschen neu strukturiert werden. So könnte beispielsweise durch einen Angreifer eine sehr kleine Firmware erstellt werden, die nur einen einzelnen Speicherbaustein überschreibt und aufgrund der geringen Größe schnell verteilt und eingespielt ist.

5.3 Programme

Epson setzt für den Betrieb des Druckers auf ein funktional sehr eingeschränktes Busybox in Kombination mit einzelnen separaten Binärprogrammen auf Basis der uClibc-Bibliothek (siehe 4.6 Software). Mit Hilfe des Buildroot Projektes, dessen Entwickler ebenfalls das uClibc Projekt pflegen, wurde eine uClibc basierte Cross-Compilation Toolchain erzeugt. Diese Toolchain ist auf das Testsystem zugeschnitten und erlaubt das compilieren eigener Anwendungen. Damit konnte für das System ein neues Busybox mit mehr Funktionen und eigene Kernelmodule erstellt werden. Versuche, die auf dem Drucker genutzten Bibliotheken durch neuere eigene mit mehr Funktionen zu ersetzen, scheiterten jedoch an der starken Bindung der proprietären Anwendungen auf dem System. Möchte man alle auf dem System befindlichen Bibliotheken ersetzen, so kann man die proprietären Softwarebausteine von Epson nicht beibehalten und den Funktionsumfang des Gerätes nicht erhalten.

6 Angriffe

Die durchgeführten Analysen der Firmware und der Update-Mechanismen haben gezeigt, dass seitens des Herstellers keine Schutzmaßnahmen gegen Angriffe getroffen wurden. Die genutzten Prüfsummen sind schwach und erlauben es dem Angreifer Firmware mit beliebigen Prüfsummen zu erstellen. Mit den gezeigten Methoden für Firmware-Updates kann ein Angreifer unabhängig vom direkten physikalischen Zugriff direkt oder indirekt über das Netzwerk Geräte angreifen. Es kann entweder direkt über USB oder HTTP, oder von außerhalb des Netzwerkes mit XSS eigene Firmware auf das Gerät aufgespielt werden. Das Testgerät konnte so übernommen und beliebig Software nachladen oder modifiziert werden.

6.1 Angreifer

Da gezeigt werden konnte, dass eine Infektion des ausgewählten Systems möglich ist, wird nun geprüft, welche Angreifer dazu in der Lage sind. Die technischen Fähigkeiten für einen solchen Angriff sind dabei erschreckend niedrig. Angriffe, wie die demonstrierten, sind mit den richtigen Tools auch von Angreifern ohne technisches Verständnis durchführbar. Die gezeigten Schwachstellen können von Angreifern hochautomatisiert und im großen Stil ausgenutzt werden. Einfache Angriffsskripte oder Firmware mit vorgefertigten Hintertüren

kann dabei schnell auch aus kleinen Angreifern ohne Mittel eine große Bedrohung machen.

Für professionelle Angreifer bedeutet die Ausnutzbarkeit der Geräte eine einfache und verlässliche Möglichkeit zum Eindringen in Systeme eines Opfers. Mit entsprechenden technischen Fähigkeiten sind die Geräte wahre Goldgruben für Wirtschaftsspione und Geheimdienste. Verschlüsselt übertragene Dokumente werden beispielsweise vom Drucker für den Druck entschlüsselt und können abgegriffen werden. Die Anwender des Gerätes setzen möglicherweise, Fingerabdrucksensoren, Smart-Cards oder ähnliches am Gerät ein, die von einem Angreifer ausgelesen werden können. Diese Angreifer sind in der Lage sich wie mit dem Bootkit demonstriert, tief in einem System einzunisten, um für lange Zeiträume unbemerkt in den Systemen eines Opfers zu agieren. Dabei profitieren sie passiv von der Rolle der Geräte als zentrale Informationsknotenpunkte und können wie demonstriert Informationen mit den eingebauten Modems unbemerkt aus dem System schleusen. Multifunktionsgeräte und Drucker sollten daher als klare Ziele für Advanced Persistent Threat (APT)-Angriffe angesehen werden und es ist wahrscheinlich das mächtige Angreifer wie Geheimdienste die Geräte bereits für zielgerichtete Angriffe einsetzen.

Es scheint daher sehr wahrscheinlich, dass diese Geräte zukünftig im großen Stil zum Ziel professioneller Malware, Würmern und Botnetzen werden.

6.2 Versuchsaufbau

Für die Tests und Analysen wurde um den WF-2540 ein Testsystem aufgebaut. In diesem Testsystem werden die üblichen Konfigurationen in denen das Gerät eingesetzt und betrieben wird nachgebildet. Um auch die FAX-Funktionalität des Gerätes näher untersuchen zu können, wurde zusätzlich ein eigenes kleines Telefonnetz errichtet. Alle demonstrierten Angriffe wurden an diesem System entwickelt und getestet (Abbildung 25). Die aufgebaute Testumgebung ist in Abbildung 26 zu sehen.

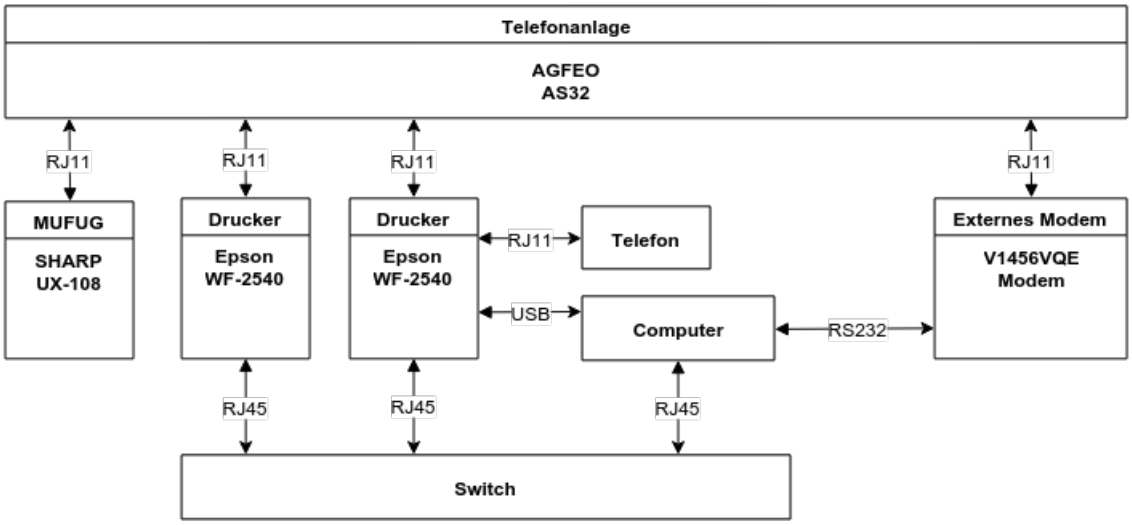

Abbildung 25: Architekturübersicht des Testsystems

Für die Analyse des WF-2540 Multifunktionsdruckers und die nötigen Tests im Laufe der Analyse wurde eine Testumgebung eingerichtet. Untersuchungen wurden an zwei baugleichen WF-2540 mit und ohne angeschlossenem Telefon, sowie über USB und LAN durchgeführt. Im Zuge Tests mit den Modems der Geräte wurde zudem ein eigenes Telefonnetz mit Telekommunikationsanlage eingerichtet.

Abbildung 26: Aufbau des Testsystems

6.3 Firmware-Updates durch CSRF

Direkte Angriffe auf Geräte durch Firmware-Updates sind wie in der Analyse gezeigt ohne weiteres möglich (siehe 4.1.3). Ein Angreifer kann aber nicht nur Systeme angreifen die er direkt erreichen kann, sondern ist in der Lage durch CSRF indirekt alle Geräte anzugreifen, die an ein Netzwerk angeschlossen sind (siehe Abbildung 27).

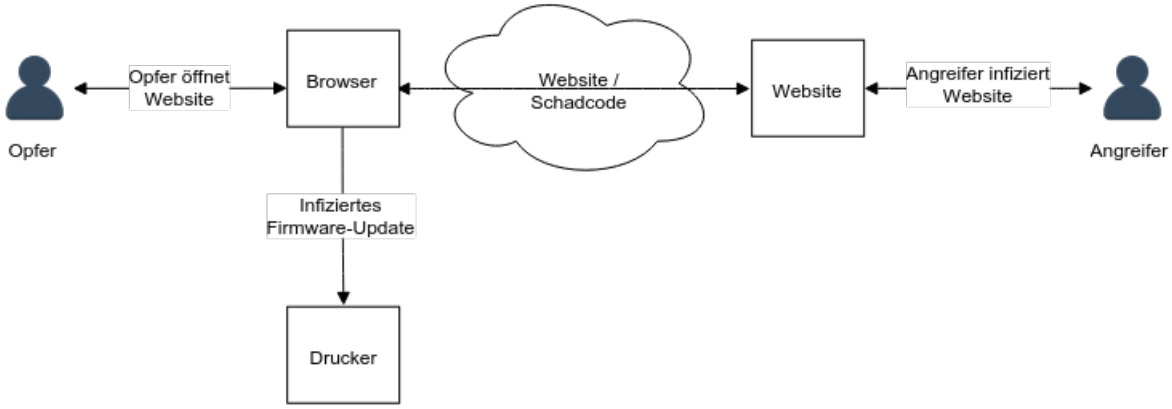

Abbildung 27: Angriff auf einen netzwerkfähigen Druckers mit CSRF durch XSS

Hat ein Angreifer eine Website mit Schadcode infiziert, kann er die Opfer für tiefer gehende Angriffe auf netzwerkfähige Geräte im gleichen Netz nutzen. So kann er den ausgeführten Code nutzen, um wie in Kapitel 4.1.3 beschrieben mit CSRF Firmware auf einen Drucker aufzuspielen.

Mit CSRF bringt ein Angreifer ein Opfer dazu ungewollt bösartige Anfragen zu versenden. Dazu wird dem Opfer im einfachsten Fall ein Link untergeschoben, der eine bösartige Veränderung auf einem Zielsystem hervorruft. Das Zielsystem kann dabei nicht feststellen ob es sich um eine bösartige Anfrage handelt, da sie von einem bekannten und berechtigten Nutzer abgesendet wird ([22]). Um den Update-Mechanismus zu Nutzen, müssen eine GET und eine POST Anfrage durch ein Opfer versendet werden. Das Opfer kann dabei ein beliebiger Netzwerkteilnehmer sein, der sich im gleichen lokalen Netzwerk wie das anzugreifende Gerät befindet. Damit Anfragen in diesem Netzwerk versendet werden, wird das Opfer mittels XSS dazu gebracht Schadcode auszuführen. CSRF Anfragen die durch den Schadcode abgesendet werden, führen so zur Installation von bösartiger Firmware.

XSS ist eine Angriffsart, bei der Schadcode in ansonsten vertrauenswürdige Internetseiten injiziert wird. Der Schadcode wird von dort an die Aufrufer der Internetseite ausgeliefert und in deren Browser ausgeführt. So ist ein Angreifer in der Lage durch das Infizieren von Internetseiten andere Benutzer anzugreifen. Dabei macht er sich zunutze, dass den Inhalten der aufgerufenen Seite voll vertraut wird und nicht zwischen den eigentlichen Inhalten der Seite und dem Schadcode des Angreifers unterschieden werden kann. Da der Browser den Schadcode für vertrauenswürdig hält, kann der Angreifer sensible Informationen wie Cookies und Session-Tokes auslesen, die von der Seite genutzt werden ([23]).

Die Möglichkeit Schadcode bei einem Nutzer auszuführen erlaubt es einem Angreifer, diesen als Sprungbrett für Angriffe auf Geräte im selben Intranet zu Nutzen. Geräte die normalerweise von z.B. Firewalls durch Zugriffe von außen geschützt werden (siehe Abbildung 28), sind so angreifbar. Der Schutzmechanismus Same-Origin-Policy (SOP) bietet dabei für den gezeigten Weg der Firmware-Updates über das Netzwerk keinen Schutz. SOP soll verhindern, dass Skripte einer Website, die beim Benutzer ausgeführt werden, Zugriff auf Objekte haben, die nicht von dieser Website stammen. Diese Webseiten definieren sogenannte Origins, die sich aus Protokoll, Domäne und Port einer URL zusammensetzen. Nur wenn diese drei Komponenten der Origin zur Origin des Skripts passen, dürfen Inhalten nachgeladen werden. SOP verhindert aber nur, dass Informationen von einer anderen Origin gelesen werden können. Das Senden von Informationen an andere Origins insbesondere durch HTTP-Requests ohne eigene Request-Header ist aber typischerweise erlaubt ([24]). Da der untersuchte Update-Mechanismus auf HTTP basiert und lediglich das Senden und nicht das Empfangen von HTTP-Anfragen erfordert, kann ein Angreifer wie demonstriert, die Geräte mittels XSS übernehmen. (siehe Appendix A.4).

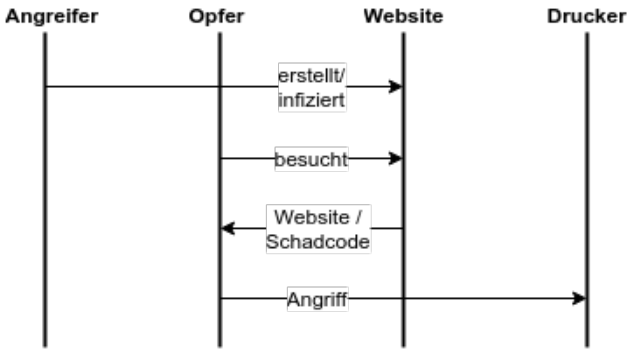

Abbildung 28: CSRF Angriffsverlauf über XSS

Der demonstrierte CSRF Angriff wurde über XSS durchgeführt. Zur Durchführung muss zunächst eine Website infiziert oder selbst hosten werden. Ruft ein Opfer, d.h. Ein Nutzer im gleichen Netzwerk wie der Drucker diese auf, werden die Website zusammen mit dem Schadcode des Angreifers ausgeliefert. Da das Opfer die Inhalte der Website, der es vertraut, und den Schadcode des Angreifers nicht auseinanderhalten kann, wird dieser ausgeführt und kann Drucker im Netzwerk angreifen.

6.4 Bootkit

Durch die Kontrolle der Firmware, ist ein Angreifer in der Lage nahezu alle Teile der Hardware in seinem Sinne zu kontrollieren. Um diesen Zugang zum infizierten System auch über Firmware-Updates hinweg zu halten oder um Erkennungsversuchen zu entgehen, kann ein Bootkit eingesetzt werden. Ein Bootkit ist Schadsoftware, die beim Bootvorgang also noch vor dem eigentlichen Betriebssystem aktiv wird. So wird direkt nach dem Einschalten die

volle Kontrolle über das System und über alle später laufende Software erlangt. Wurde Schadcode auf dieser tiefen Ebene eingeschleust, ist eine Entdeckung der Infizierung ausgesprochen schwer. Im Falle des Testsystems kann sich ein Angreifer insbesondere die ersten 64kB des Bootflash zu Nutze machen, da sich in diesem Abschnitt Bootloader und Recovery-Mode befinden, die durch Firmware-Updates nicht modifiziert werden.

Der Drucker wird von einem ARM9-Prozessor gesteuert und bootet indem ein Reset-Interrupt ausgelöst wird, der zur Ausführung des entsprechenden Codes für den Bootprozess führt. Ein Interrupt ist ein Unterbrechungssignal, dass dem Prozessor das Eintreten eines Ereignisses signalisiert. Die entsprechende Interrupt Service Routine (ISR) die den Code enthält, der beim Erhalt eines Interrupts ausgeführt werden soll, wird dabei durch den Interrupt Vector Table (IVT) bestimmt. Dieser befindet sich in den ersten Bytes des Bootflash und referenziert für die Interrupts des ARM Prozessor entsprechende Interrupt Service Routinen. Der zum Booten des WF-2540 vom Prozessor genutzte Reset-Interrupt befindet sich beispielsweise an der Stelle 0x0 im IVT und zeigt auf eine ISR an der Stelle 0x114 im Speicher.

```
0x0000  ldr pc, [pc, 0x1c]  ; vec_reset               pc = 0x114
0x0004  ldr pc, [pc, 0x1c]  ; vec_undef_instruction   pc = 0x44
0x0008  ldr pc, [pc, 0x1c]  ; vec_superv_call         pc = 0x48
0x000c  ldr pc, [pc, 0x1c]  ; vec_pref_abort          pc = 0x4c
0x0010  ldr pc, [pc, 0x1c]  ; vec_data_abort          pc = 0x50
0x0014  mov r0, r0          ; not used (nop)
0x0018  ldr pc, [pc, 0x1c]  ; vec_interrupt           pc = 0x80c
0x001c  ldr pc, [pc, 0x1c]  ; vec_fast_interrupt      pc = 0x54
0x0020  dd 0x12345678       ; padding
0x0024  dd 0x00000114       ; isr_reset
0x0028  dd 0x00000044       ; isr_undef_instr
0x002c  dd 0x00000048       ; isr_superv_call
0x0030  dd 0x0000004c       ; isr_pref_abort
0x0034  dd 0x00000050       ; isr_data_abort
0x0038  dd 0x00000000       ; (reserved)
0x003c  dd 0x0000080c       ; isr_interrupt
0x0040  dd 0x00000054       ; isr_fast_interrupt
0x0044  b 0x44              ; infinite loop
0x0048  b 0x48              ; infinite loop
0x004c  b 0x4c              ; infinite loop
0x0050  b 0x50              ; infinite loop
```

Listing 9: WF-2540 Interrupt Vector Table

Die Tests zeigen, dass der Code dieser Interrupt Service Routine von einem Angreifer ohne Schwierigkeiten so modifiziert werden kann, dass diese nach dem Einschalten des Systems, noch bevor der Linux-Kernel geladen wird, Schadcode ausführen. Der Angreifer ist also in der Lage, vollkommen unbemerkt vom Betriebssystem, das Gerät nach seinen Wünschen zu kontrollieren und kann dabei sogar Codepfade des Recovery-Mode für sich zweckentfrem-

den. Der so platzierte Schadcode, ist für das Betriebssystem unsichtbar und ermöglicht es dem Angreifer beliebige Speicherbereiche zu lesen und zu verändern. Wird nach der Infektion ein Firmware-Update auf dem Gerät durchgeführt, wird das Bootkit nicht überschrieben und kann das Gerät weiterhin kontrollieren. Sollte Software aus dem Linux-System heraus doch versuchen den vom Bootcode genutzten Speicherbereich zu überschreiben, kann der Angreifer dies theoretisch verhindern, da er durch das Bootkit volle Kontrolle über den Prozessor besitzt.

6.5 Datenübertragung über Modems

In diesem Abschnitt wird gezeigt, wie ein Angreifer nach erfolgreichem Eindringen in ein System das integrierte Modem nutzen kann um eine Datenverbindung nach außen zu aufzubauen. Der WF-2540 verfügt über ein Modem mit dem die FAX-Funktionalität des Gerätes realisiert wird. Bei dem Modem handelt es sich um ein Soft-Modem. Das bedeutet, dass ein Großteil der Funktionalität in Software realisiert worden ist. Ein Angreifer kann diese Software natürlich zu seinen Gunsten modifizieren. Um ohne Patches in der Software neben der normalen FAX-Funktion des Gerätes einen Datenkanal zum Angreifer zu öffnen, muss in die bestehende FAX-Architektur eingegriffen werden.

6.5.1 FAX-Architektur

Der physikalische Teil des Modems wird durch das Kernelmodul lsimodem.ko angesteuert. Durch ein zweites Kernelmodul lsiserial.ko kann das Modem als serielle-Konsole im Dateisystem angesprochen werden. Diese Schnittstelle wird von zwei Anwendungen verwendet, dessen Aufgaben aber nur grob bekannt sind. Zum Einen existiert die Anwendung “faxdrv”, die das Modem für den Betrieb einrichtet und diverse Einstellungen an der seriellen-Konsole vornimmt. Zum Anderen nwsoc das große Binärprogramm des Systems, dass scheinbar für das Empfangen und Senden von FAX zuständig ist (siehe Abbildung 29).

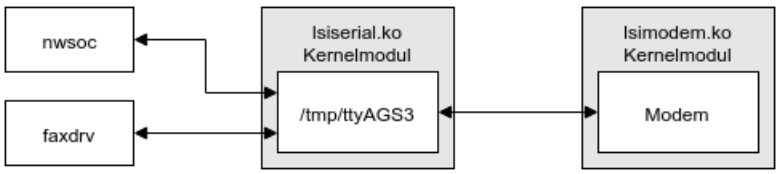

Abbildung 29: FAX Architektur

Die Anwendungen nwsoc und faxdrv kommunizieren über die serielle-Konsole /tmp/ttyAGS3 mit dem Modem. Auf diesem Weg werden FAX-Daten empfangen und versendet.

Zu diesem Zweck wird ein Kernelmodul implementiert, dass als Mittelsmann die Kommunikation zwischen Modem und Anwendung mitschneiden und modifizieren kann. Damit kann das Modem genutzten werden, um ausgehend vom Opfer eine Datenverbindung zum Angreifer aufzubauen (siehe Abbildung 30), Inhalte aus Dokumenten zu löschen oder in diese einzufügen. Ein Angreifer kann sogar unbemerkt von den auf dem System laufenden

Anwendungen per FAX eingehende oder ausgehende Dokumente duplizieren und an sich weiterleiten.

Die Kommunikation mit dem Modem könnte zwar auch direkt über /tmp/ttyAGS3 erfolgen, damit wäre es aber auch für die anderen Anwendungen auf dem System sichtbar und könnte diese stören. Da die Anwendungen sich als sehr instabil bei unvorhergesehenen Ereignissen erwiesen haben, wird ein Umweg über ein Kernelmodul gewählt. Dieses Kernelmodul implementiert weitestgehend nur eine Pipe-Funktionalität. Inhalte die durch die Pipe gehen, können unbemerkt mitgelesen und modifiziert werden. Die ursprüngliche serielle-Konsole /tmp/ttyAGS3 wird mit Hilfe des Boot-Skripts umbenannt und durch eine Datei ersetzt, welche die Kommunikation durch das Kernelmodul leitet. Die Anwendungen des Systems greifen nun über /tmp/ttyAGS3 lesend und schreibend auf die Pipe zu.

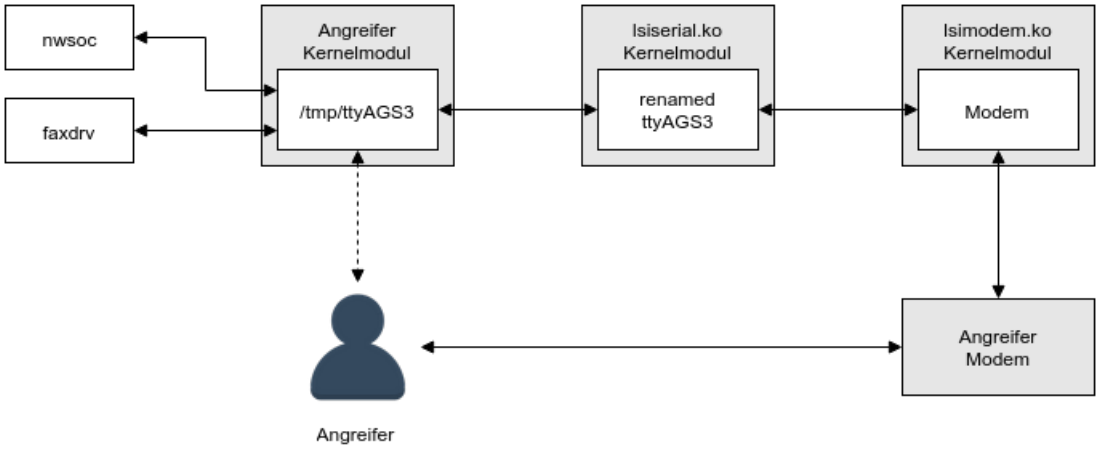

Abbildung 30: FAX Angriffsmodell

Im beispielhaften Angriff wurde mit einem eigenen Kernelmodul die ursprüngliche serielle-Konsole /tmp/ttyAGS3 durch eine eigene ersetzt. Das ursprüngliche /tmp/ttyAGS3 wird mittels des Boots-Skripts umbenannt. So können unbemerkt von den Anwendungen Daten in der Kommunikation gelesen und geschrieben werden, ohne dabei die Grundfunktionalität des Systems zu stören.

6.5.2 Hayes-Kommandos

Die Kommunikation mit Modems wird mit Hilfe der Hayes-Kommandos durchgeführt. Diese wurden 1981 eingeführt und machen seitdem für fast alle Hersteller die Basisfunktionalität von Modems steuerbar. Diese Klartextkommandos erlauben Konfiguration und Nutzung des Modems durch einfache menschenlesbare Eingaben und Ausgaben. Hayes-Kommandos werden auch von den Anwendungen auf dem Drucker genutzt um die FAX-Funktionalität bereitzustellen. Mit diesen Kommandos können nahezu alle Aspekte des Modems kontrolliert werden. Sie erlauben es zum Einen das Modem in einen lautlosen Modus zu versetzen, in dem die normalerweise so markanten Geräusche nicht zu hören

sind und zum Anderen ermöglichen sie es dem Angreifer auf dem Modem gespeicherte Informationen, wie beispielsweise Telefon und FAX-Nummern auszulesen.

Jedes Hayes-Kommando muss mit dem “Attention” Prefix “AT” beginnen, welches den Anfang eines neuen Kommandos markiert. Danach kann eine beliebige Anzahl an Operationen und Parametern folgen, die je nach Implementierung optional noch durch einen Zeilenumbruch abgeschlossen werden müssen. (siehe Appendix A.5).

6.5.3 Datenübertragung

Um eine Datenverbindung zwischen dem Opfer und dem Angreifer aufzubauen, müssen zunächst serielle-Konsole und Modem eingerichtet werden. Daher sollte vor der Kommunikation mit dem Modem zunächst die faxdrv-Anwendung einmal gestartet werden. Die Anwendung sendet eine Reihe von Hayes-Kommandos zur initialen Einrichtung an das Modem und setzt Optionen an der seriellen-Konsole. Anschließend können die Vorbereitungen für den Aufbau der Verbindung getroffen werden. Mit dem Kommando M0, kann die Tonausgabe des Modems auf dem Gerät deaktiviert werden, um unbemerkt Verbindungen aufzubauen und Daten zu übertragen. Durch Setzen des S0 Registers des Modems auf den Wert 1, kann der Angreifer erreichen, dass der Drucker nach einem Klingelzeichen automatisch eine eingehende Verbindung entgegennimmt. Kennt er die Rufnummer des Opfers, so kann er damit von außen eine Verbindung zum Gerät aufbauen. Der eigentliche Verbindungsaufbau, kann durch das Opfer oder den Angreifer mit dem DT Kommando zur jeweiligen Rufnummer durchgeführt werden (siehe Abbildung 31 und 32). Wird eine Verbindung von außen zum Gerät aufgebaut und automatisch angenommen ist dies für den Benutzer nicht erkennbar, da das Gerät weder Geräusche von sich gibt noch eine Meldung anzeigt. Wird an der zweiten RJ11 Dose des Druckers ein Telefon betrieben, so lassen externe Verbindungen das Telefon einmal Klingeln bis der Drucker die Verbindung automatisch angenommen hat. Nachdem die Verbindung so aufgebaut wurde, kann der Angreifer über /tmp/ttyAGS3 Daten übertragen.

7 Auswertung

Es konnte gezeigt werden, dass eine Kompromittierung von Multifuktionsgeräten bereits mit einfachen Mitteln möglich ist. Angriffe sind nicht nur durch hochspezialisierte und professionelle Angreifer möglich, sondern sind mit einfachen Skripten und vorgefertigter Firmware auch von Angreifern ohne tieferes technisches Verständnis durchführbar. Die gesammelten Erkenntnisse zeigen, dass ein Angreifer einfach und hochautomatisiert Angriffe auf große Mengen von Geräten durchführen kann und drüber nahezu unbemerkt tief in die Systeme eines Opfers eindringen kann.

Durch die Untersuchungen des Firmware-Dateiformates konnte gezeigt werden, dass ein Angreifer beliebig Firmware verändern oder selbst erstellen kann. Schutzmechanismen, die Modifikationen durch Unbefugte verhindern könnten, existieren nicht. Ein Angreifer kann,

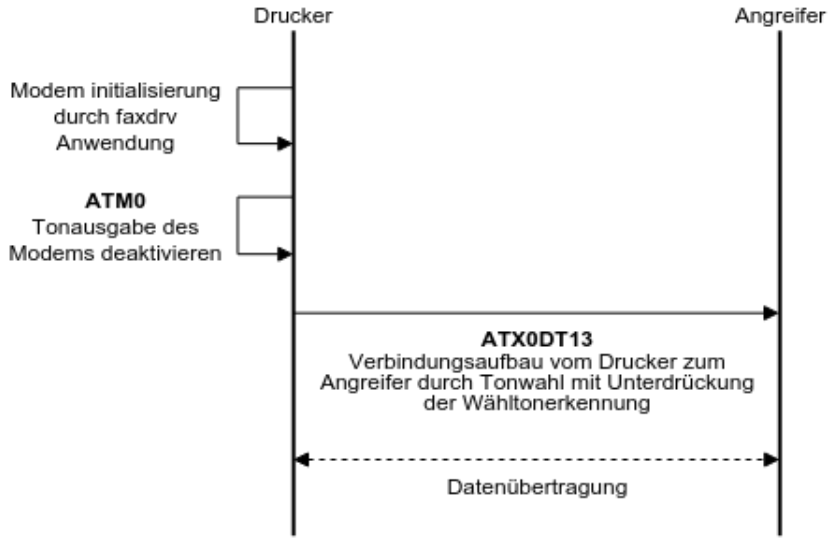

Abbildung 31: Modem Verbindungsaufbau vom Drucker zum Angreifer

Der Drucker deaktiviert die Tonausgabe des Modems um die Interaktion der Schadsoftware mit dem Modem zu verstecken. Anschließend kann das Gerät eine Datenverbindung zum Angreifer mit der Rufnummer 13 aufbauen und Daten übertragen.

wie gezeigt, beliebig eigene Firmware erstellen und dabei sogar die Prüfsumme selbst bestimmen. Die Analysen des Update-Mechanismus haben gezeigt, dass keinerlei Autorisierung benötigt wird, um eigene Firmware aufzuspielen. Updates können von jedem anderen netzwerkfähigen Gerät aus durchgeführt werden. Sogar Geräte die nach außen beispielsweise durch Firewalls geschützt sind, können von einem Angreifer mittels XSS durch Firmware-Updates angegriffen werden. Eine sichere Authentifizierung gegenüber dem System ist scheinbar auf keiner Ebene umgesetzt. Lediglich das EpsonNet-Konfigurations-Tool, das Einstellungen über SNMP verändern kann, bietet eine Passwortabfrage. Da das Passwort aber im Klartext übertragen wird und nur von diesem einen Tool geprüft zu werden scheint, ist eine Sicherung administrativer Aufgaben faktisch nicht gegeben.

Mit der erstellten Toolchain kann beliebig eigene Software und Firmware für Geräte erstellt und nachgeladen werden. Damit ist es gelungen Daten unbemerkt über das eingebaute Modem eines Druckers auszuleiten, ohne dabei die Grundfunktionen des Gerätes zu beeinträchtigen. Über diesen Kanal ist es möglich, mit Geräten zu kommunizieren, die keinerlei Anbindung an ein IP-basiertes Netzwerk haben. Dokumente können dabei durch einen Angreifer nicht nur ausgeleitet, sondern auch unbemerkt modifiziert und gefälscht werden. Wurde ein Gerät derart infiziert, ist von außen nicht feststellbar, dass es übernommen wurde. Durch die Kontrolle der Firmware ist ein Angreifer sogar in der Lage, einen Drucker physikalisch unbrauchbar zu machen, indem er zum Beispiel alle vorhandenen Flash-Bausteine löscht.

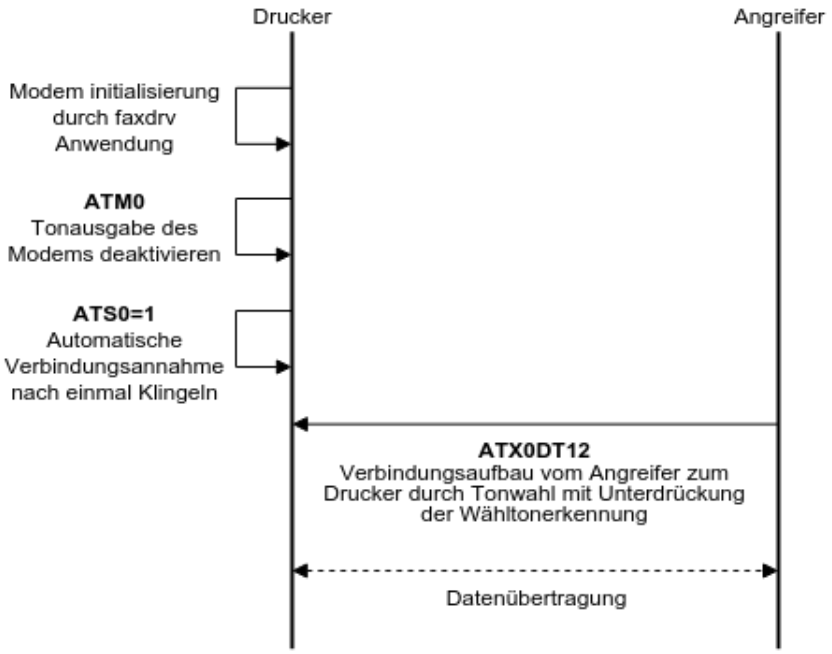

Abbildung 32: Modem Verbindungsaufbau vom Angreifer zum Drucker

Der Drucker deaktiviert die Tonausgabe des Modems um die Interaktion der Schadsoftware mit dem Modem zu verstecken. Anschließend wird das Modem durch setzen des S0 Registers angewiesen automatisch eingehende Verbindungen anzunehmen. Nun kann der Angreifer von außen eine Verbindung zum Gerät mit der Rufnummer 12 aufbauen und das Gerät wird die Verbindung automatisch annehmen.

7.1 Bedeutung

Epson gehört zu den größten Druckerherstellern und verkauft Drucker millionenfach in alle Teile der Welt. Mit den gezeigten Schwachstellen im Firmware-Update-Mechanismus die sogar indirekt über z.B XSS ausgenutzt werden können (siehe 6.3), ist davon auszugehen, dass etliche Modelle verschiedener Baureihen anfällig sind. Anhand der POST-Header (siehe 4.1.3) und den Gültigkeitszeiträumen der im Dateisystem gefundenen SSL-Zertifikate (siehe 4.6) kann gemutmaßt werden, dass der Update-Mechanismus mindestens seit 1998/1999 existiert. Während der Analysen wurde Firmware diverser Geräte und Baureihen entpackt, dabei konnte kein alternativer Firmware-Update-Mechanismus identifiziert werden. Daher ist naheliegend, dass ein großer Teil der produzierten Drucker auf diesem Mechanismus aufbaut und somit gegen die gezeigten Angriffe anfällig ist.

7.2 Ausmaß

Um zumindest eine Einschätzung über die direkt angreifbaren Geräte im Internet zu bekommen, werden aktuelle Daten von scans.io für den gesamten IPv4-Adressraum auf Port 80 ausgewertet. Um die verwundbaren Geräte zu identifizieren, wird nach markanten Mustern gesucht die von diesen Geräten ausgehen. Angreifbare Geräte haben dabei beispielsweise in ihren Antworten das HTTP-Response-Header Server Feld mit folgendem Eintrag gesetzt.

```
SERVER: EPSON_Linux UPnP/1.0 Epson UPnP SDK/1.0
```

Listing 10: Epson HTTP-Server Response-Header

Die Auswertung der Project Sonar Daten vom 18.08.2015, ergab dabei etwa 5300 direkt angreifbare Geräte ([25]). Diese Zahl ist keinesfalls ein Maß für die Anzahl der weltweit verwundbaren Geräte, sondern zeigt nur die Anzahl der direkt angreifbaren Systeme. Die Zahl der indirekt über z.B. XSS angreifbaren Geräte mit Anbindung an ein Netzwerk dürfte deutlich höher sein und einen Großteil der verkauften Geräte mit diesem Update-Mechanismus betreffen.

Um mehr über Angriffe auf diese Geräte zu erfahren, wurden vier Honeypots aufgestellt, die sowohl die Weboberfläche als auch das Verhalten des Webservers auf HTTP HEAD, GET und POST Anfragen dem WF-2540 nachempfinden und protokollieren. Bei den Auswertungen der Logdateien wurden keine Angriffe gefunden, die auf die demonstrierten Angriffe hinweisen oder den emulierten MFP anderweitig gezielt angreifen. Versuchte Angriffe gegen die Honeypots waren überwiegend blinde Angriffe die versuchten Schadcode über CGI-Dateien einzuschleusen oder PHP-Dateien zu finden. Derartige Dienste sind aber weder auf den Geräten noch auf den Honeypots vorhanden.

7.3 Bedrohungen

In falsch konfigurierten Netzwerken, in denen Geräte von außen angesprochen werden können, besteht eine sehr hohe Gefahr durch Bots und Crawler die, die Geräte automatisch finden und infizieren. Selbst in Netzwerken mit einem Schutz der Geräte vor Zugriffen von außen, kann ein Angreifer über XSS die Geräte eines Opfers kompromittieren. Ein unerkanntes kompromittiertes Gerät, stellt eine enorme Bedrohung für dessen Umfeld dar. Es wird nicht nur die Vertraulichkeit und Integrität aller Dokumente untergraben, da ein Angreifer diese lesen und modifizieren kann, sondern das gesamte Netzwerk ist angreifbar. Angreifer können ein solches Gerät als unsichtbaren Brückenkopf in die Systeme eines Opfers nutzen. Darüber sind die in der Lage, die Schutzmaßnahmen der Netze zu umgehen und noch tiefer einzudringen. Wird ein Netzwerkfähiges Gerät zum Gateway eines Angreifers, können damit die Netzwerke hinter den Firewalls durch Netzwerkscanner erkundet und beliebig weiter angegriffen werden.

Die Möglichkeit ein Gerät bei einem Opfer zu platzieren und damit unbemerkt Zugriff auf dessen Netze zu bekommen ist insbesondere für sehr gezielte Angriffe relevant. Hochspezialisierte Angreifer wie Nachrichtendienste müssen nicht direkt angreifen und dabei Gefahr laufen entdeckt zu werden, sondern können Geräte unbemerkt abfangen und modifizieren. Wird Schadcode so durch Zwischenhändler, Reparaturen oder das Abfangen der Geräte platziert, sind alle getroffenen Sicherheitsvorkehrungen zunichte gemacht worden. Auch für Wirtschaftsspione sind Angriffe äußerst lukrativ. Diese Angreifer schrecken nicht vor direkten physikalischen Zugriffen auf die USB-Schnittstellen oder modifizierten USB-Geräten zurück.

Angriffe sind nicht komplex, erfordern keine Privilegien und ermöglichen es trotzdem die Schutzziele Vertraulichkeit, Integrität und Verfügbarkeit ganz auszuschalten. Systeme die direkte IP-Kommunikation zulassen, sind dabei am meisten gefährdet und erhalten die höchstmögliche Common Vulnerability Scoring System (CVSS)-Wertung von 10, da sie jederzeit übernommen werden können. Ein über XSS eingeleitetes Firmware-Update, erfordert Social Engineering um ein Opfer auf eine infizierte Website zu locken und Kenntnis der lokalen IP-Adresse des Gerätes. Verbringt ein Opfer genug Zeit auf der infizierten Website, kann durch einfache Scans oder sogar simples raten von Adressen ein Gerät infiziert werden. Da für diesen Angriffsweg die Interaktion eines Benutzers erforderlich ist, sind Angriffe aufwändiger, aber dennoch hoch kritisch. Auch Angriffe die einen physikalischen Zugang zu einem Gerät voraussetzen, stellen eine hohe Bedrohung dar (siehe Tabelle 5).

8 Fazit

Es konnte demonstriert werden, dass auch Multifunktionsdrucker durch Angreifer übernommen werden können. Durch oft identische Software der Geräte eines Herstellers und deren starke Verbreitung können Angriffe für ein Gerät auch auf anderen Geräten eingesetzt werden. Dadurch ergeben sich schnell große Mengen an verwundbaren Geräten. Eine

Update-Methode	Voraussetzungen	Angreifer	CVSS-Wertung
HTTP direkt	IP-Kommunikation	Bots Script-Kiddies	10 (CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
HTTP XSS	Kenntnis der IP-Adresse Social Engineering	Wirtschaftsspione Geheimdienste	9.6 (CVSS:3.0/AV:N/AC:L/PR:N/UI:R/S:C/C:H/I:H/A:H)
USB	physikalischer Zugriff	Wartungspersonal Insider	7.6 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)
Flash-Speicher	physikalischer Zugriff	kriminelle Zwischenhändler Geheimdienste	7.6 (CVSS:3.0/AV:P/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H)

Tabelle 5: CVSS-Bewertung der Angriffswege

Die Angriffswege über die Firmware auf einem Gerät installiert werden kann, wurden mit dem CVSS Bewertungssystem bewertet.

Erkennung infizierter Systeme ist ausgesprochen schwer und teilweise nur durch das Zerlegen einzelner Geräte möglich. Wurde ein System einmal infiziert ist eine Desinfektion, wenn überhaupt möglich, sehr schwer und kostenintensiv. Es konnte gezeigt werden, dass Angriffe keineswegs nur von hochprofessionellen Angreifern durchgeführt werden können und sich nur auf APT-Angriffe beschränken. Angreifer ohne tieferes Verständnis der Technik können mit einfachen Tools schnell zu einer großen Bedrohung werden und großangelegte Angriffe durchführen. Ein einziges kompromittiertes Gerät kann einem Angreifer als versteckter Zugangspunkt in ein Netzwerk dienen und dabei die Vertraulichkeit und Integrität nahezu aller in diesem Netzwerk ausgetauschten Daten untergraben.

Die erste Einschätzung der Bedrohung durch die Sicherheitslücke mit einem CVSS-Wert von 10 (siehe 3.4), konnte durch die Analysen bestätigt werden. Die Möglichkeiten einzelner Angreifer um ein System zu kompromittieren, sind hoch kritisch. Die Angriffe sind von geringer Komplexität, erfordern keine Privilegien und ermöglichen es trotzdem Geräte vollständig zu übernehmen.

Die Fähigkeiten der Geräte werden unterschätzt und die damit verbundenen Bedrohungen übersehen oder ignoriert. Es ist wichtig zu erkennen, dass eingebettete Geräte wie Drucker oder auch Router vollständige Computer mit allen technischen Möglichkeiten sind. Diese Geräte werden mit einer Vielzahl sensibler Informationen und Aufgaben betraut und müssen daher stärker denn je Teil von Sicherheitsbetrachtungen zum Schutz der eigenen Infrastruktur sein. Trotz der Veröffentlichungen und den gefundenen Sicherheitslücken der letzten Jahre, werden die Probleme von einigen Herstellern scheinbar immer noch nicht ernst genommen. Bedrohungen werden dabei fahrlässig auf Kosten der Kunden ignoriert.

9 Ausblick

9.1 Empfehlungen

Im Folgenden wird von konkreten technischen Lösungsvorschlägen absehen, da eine Reparatur der untersuchten Mechanismen nicht sinnvoll erscheint. Es ist zu empfehlen, in Kooperation mit anderen Herstellern ein offenes und sicheres Verfahren für Firmware-Updates

zu entwickeln oder zumindest gemeinsam Implementierungen für zentrale Komponenten, wie eingebettete HTTP-Server und andere Protokolle zu fördern oder ggf. zu schaffen. Aktive Untersuchungen der eigenen Systeme auf Schwachstellen und Untersuchungen, ob eigene Produkte schon Ziel von Angriffen und Missbrauch waren oder sind sollten permanent durchgeführt werden. Zu diesem Zweck können beispielsweise Honeypots für eigene Systeme eingerichtet werden. Es ist ratsam eine kompetente Kontaktstelle zu schaffen, die Hinweise entgegennehmen kann. Das Einrichten von Bug-Bounty-Programmen, kann Anreize geben gefundene Fehler zu melden, damit diese möglichst früh behoben werden.
Für größere Systeme kann die Implementierung von guten Logging-Schnittstellen und die Zusammenarbeit mit Intrusion Detection Systemen ein gutes Verkaufsargument sein und den Kunden gleichzeitig bei seinen Bemühungen unterstützen seine Systeme zu schützen.

9.2 Weiterführend

Multifunktionsdrucker bieten schon aufgrund ihrer technischen Ausstattung viele weitere Möglichkeiten für Angriffe. Neben dem von Shamir gezeigten Weg, Daten über das Licht eines Scanners zu übertragen und dem demonstrierten Ansatz, Daten über das Modem auszuleiten (siehe 6.3, ergeben sich viele weitere Möglichkeiten. So könnten beispielsweise Daten über die Geräusche der Motoren, das elektrische Laden und Entladen der Tintenpatronen oder das LCD exfiltriert werden.

Betreffend des untersuchten WF-2540 und aller baugleichen Geräte bleiben neben den untersuchten Firmware-Updates auch zukünftig viele weitere Angriffswege, die genauer betrachtet werden sollten. Die Kernelmodule des Soft-Modems auf dem WF-2540, erlauben Updates des verbauten Modem-Chipsatzes. Ein Angreifer könnte den Modem-Chipsatz nutzen, um darauf Daten und Schadcode abzulegen. Bei zukünftigen Betrachtungen dieser Geräte könnte sich eine genauere Untersuchung der nwsoc-Anwendung lohnen. Werden dabei Fehler in der HTTP-Implementierung oder den Druckerprotokollen gefunden, die dazu führen das Code ausgeführt werden kann, könnten sich die Geräte darüber übernehmen lassen. Außerdem gibt es eine ganze Reihe von offenen Ports, denen keinerlei Funktion zuordnet werden konnte. Einige der auf dem System gefundenen SSL-Zertifikate, stammen zum Teil von 1996 und setzen auf die schon lange als schwach geltende SHA1 Hashfunktion und RSA mit 1024 Bit. Diese Zertifikate sind teilweise noch bis zum Jahr 2036 gültig und sollten sie im System noch Anwendung finden, könnte dies zu weiteren Schwachstellen führen (siehe [26]).

A Appendix

A.1 WINBOND 25Q32FVSIG Datenblatt

Das Datenblatt des WINBOND 25Q32FVSIG Flash-Speicher ist als Datei unter `appendix/winbond.pdf` zu finden ([27]).

A.2 HTTP Firmware-Update Sniff

Der Mitschnitt eines Firmware-Updates über das Netzwerk ist als PCAP-Datei unter `appendix/http_firmware_update.pcap` beigelegt.

A.3 CRAMFSCHK Patch

Eine modifizierte Version des Quelltextes von cramfschk wurde unter `appendix/cramfs-1.1` beigefügt.

A.4 CSRF Firmware-Update Demo

Eine Demonstrationsanwendung für Firmware-Updates durch CSRF, wurde unter `appendix/csrf_demo` beigefügt.

A.5 Modem Handbuch

Das Handbuch für ein agere systems Modem ist als Datei unter `appendix/modem_manual.pdf` beigelegt ([28]).

A.6 Kernel Make Config

Die automatisch generierte make config des Kernels ist unter `appendix/kernel_config` beigelegt.

A.7 Risikobewertung der Systemschnittstellen

Zugang	Beschreibung	soll Zugriffe	mögliche Zugriffe	Anmerkungen
TCP / 80	Startseite des Webinterface	Alle	Alle	-
	Konfigurationsseite für Epson Connect-Services	Benutzer	Alle	keine Verschlüsselung, keine Authentifizierung
	Konfigurationsseite für Google Cloud Print-Services			
	Konfigurationsseite für DNS und Proxy			
	Firmware-Update Seite, (Automatisches Firmware-Updates von Epson Servern)			
	Konfigurationsseite für AirPrint			
	Seite für Geräte Informationsübersicht			
	Firmware-Updates durch Update-Tools			
	SOAP/XML Service für Konfiguration durch externe Tools			
TCP / 445	CIFS Netzwerkfreigabe	Besitzer, Gast, Angreifer	Alle	-
TCP / 515	Line Printer Daemon	Alle	Alle	keine Verschlüsselung
TCP / 631	Internet Printing Protocol	Alle	Alle	keine Verschlüsselung
TCP / 1865	unbekannt	-	-	-
TCP / 9100	Jetdirect Print Service	Alle	Alle	-
NetBT Ports	SMB über NetBIOS	Besitzer, Gast, Angreifer	Alle	-
UDP / 137	NetBIOS Name Service			
UDP / 138	NetBIOS Datagram Service			
TCP / 139	NetBIOS Session Service			
UDP / 161	Simple Network Management Protocol	Besitzer	Alle	keine Verschlüsselung
UDP / 427	Service Location Protocol	Alle	Alle	-
UDP / 1022	unbekannt	-	-	-
UDP / 1023				
UDP / 3072				
UDP / 3073				
UDP / 3075				
UDP / 3078				
UDP / 3289	(ENPC) proprietäres Binärprotokoll von Epson, um Geräteinformationen abzufragen und zu verändern.	Besitzer	Alle	keine Verschlüsselung, keine Authentifizierung
UDP / 3702	Web Service Dynamic Discovery	Alle	Alle	-
UDP / 5353	Zeroconf	Alle	Alle	-
UDP / 5355	Link-Local Multicast Name Resolution	Alle	Alle	-
LCD-Display	LCD-Display und Konfiguration	Besitzer	Besitzer, Gast, Angreifer	-
	Kopieren, FAX, Scannen	Besitzer, Gast Angreifer	Besitzer, Gast, Angreifer	-
	Diverse Systemkonfigurationen	Besitzer	Besitzer, Gast, Angreifer	keine Authentifizierung
USB Typ A	USB Kommunikation mit Computern	Besitzer, Gast Angreifer	Besitzer, Gast, Angreifer	-
	Drucken, FAX, Scannnen, Dateiübertragung	Besitzer, Gast Angreifer	Besitzer, Gast, Angreifer	-
	Systemeinstellungen durch Konfigurationstools verändern	Besitzer	Besitzer, Gast, Angreifer	keine Authentifizierung
	Firmware-Updates durch Update-Tools	Besitzer	Besitzer, Gast, Angreifer	keine Authentifizierung
USB Typ B	USB-Massenspeicher	Besitzer, Gast, Angreifer	Besitzer, Gast, Angreifer	-
Modem	FAX Versand und Empfang	Besitzer, Gast, Angreifer	Besitzer, Gast, Angreifer	-
Cloud-Dienste	Druckaufträge und Faxversand über Internet und Mobilgeräte	Besitzer	Besitzer	-

Tabelle 6: Identifizierte Systemschnittstellen

Für die identifizierten Schnittstellen zum System werden den erlaubten die tatsächlichen Zugriffsrechte durch Akteure gegenübergestellt.

Literatur

[1] BSI. Beschränkung der Zugriffe auf Drucker, Kopierer und Multifunktionsgeräte. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m04/m04301.html , 2013. [Online; accessed 01-09-2015 12:57].

[2] BSI. Netztrennung beim Einsatz von Multifunktionsgeräten. https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/Inhalt/_content/m/m05/m05146.html , 2013. [Online; accessed 01-09-2015 13:00].

[3] Popular Science. Spies in the Xerox Machine. https://books.google.de/books?id=KIEIX2X-na8C&lpg=PA68&dq=Spies%20in%20the%20Xerox%20Machine&hl=de&pg=PA68#v=onepage&q=Spies%20in%20the%20Xerox%20Machine&f=false, 1997. [Online; accessed 21-07-2015 15:16].

[4] FX/pH. Attacking Networked Embedded Systems. http://www.phenoelit-us.org/stuff/BHLV.pdf, 2002. [Online; accessed 30-07-2015 12:26].

[5] Irongeek. Network Printer Hacking. http://www.irongeek.com/i.php?page=videos/notacon2006printerhacking, 2006. [Online; accessed 30-07-2015 12:34].

[6] Irongeek. Hacking Network Printers. http://www.irongeek.com/i.php?page=security/networkprinterhacking, 2006. [Online; accessed 4-08-2015 16:04].

[7] Wikipedia. PostScript. https://de.wikipedia.org/wiki/PostScript, 2015. [Online; accessed 23-08-2015 12:00].

[8] Andrei Costin. PostScript - Danger Ahead - Hacking MFPs, PCs and Beyond. https://www.cupfighter.net/2012/05/hitb2012ams-postscript-danger, 2015. [Online; accessed 23-08-2015 12:03].

[9] Ang Cui/Sal Stolfo. Print Me If You Dare. http://www.redballoonsecurity.com/pdf/print-me-if-you-dare-2011.pdf, 2011. [Online; accessed 30-07-2015 14:38].

[10] Deral Heiland. From Patched to Pwned. http://foofus.net/goons/percx/Xerox_hack.pdf, 2013. [Online; accessed 30-07-2015 13:10].

[11] Sal Stolfo/Ang Cui/Michael Costello. When Firmware Modifications Attack: A Case Study of Embedded Exploitation.

http://ids.cs.columbia.edu/sites/default/files/ndss-2013.pdf , 2011. [Online; accessed 14-08-2015 13:47].

[12] Mitre Corporation. CVE Listings for Keyword „printer“. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=printer, 2015. [Online; accessed 18-07-2015 9:55].

[13] Adi Shamir. Side Channel Attacks Past Present And Future. https://www.blackhat.com/eu-14/briefings.html#side-channel-attacks-past-present-and-future, 2014. [Online; accessed 30-07-2015 15:08].

[14] statista. Marktanteile der Hersteller am Absatz von Druckern, Kopierern und Multifunktionsgeräten weltweit vom 1. Quartal 2009 bis zum 1. Quartal 2015. http://de.statista.com/statistik/daten/studie/160909/umfrage/weltweite-marktanteile-der-hersteller-von-druckern-und-multifunktionsgeraeten/, 2015. [Online; accessed 24-08-2015 13:51].

[15] multifunktionsdruckertest 24. Entwicklung des Anteils von Druckern und Scannern in deutschen Haushalten. http://multifunktionsdruckertest-24.de/entwicklung-des-anteils-von-druckern-und-scannern-in-deutschen-haushalten/, 2015. [Online; accessed 24-08-2015 13:48].

[16] Christian Büch. SPI –Serial Peripheral Interface. http://www.uni-koblenz.de/~physik/informatik/MCU/SPI.pdf, 2006. [Online; accessed 31-08-2015 22:55].

[17] Wikipedia. SPI-Sternverbindung. https://upload.wikimedia.org/wikipedia/commons/thumb/f/fc/SPI_three_slaves.svg/2000px-SPI_three_slaves.svg.png, 2006. [Online; accessed 07-09-2015 14:20].

[18] www.mikrocontroller.net. Serial Peripheral Interface. http://www.mikrocontroller.net/articles/Serial_Peripheral_Interface. [Online; accessed 31-08-2015 23:00].

[19] L. Masinter. RFC7578 multipart/form-data. https://tools.ietf.org/html/rfc7578, 2015. [Online; accessed 30-08-2015 13:50].

[20] IETF. RFC2616 Hypertext Transfer Protocol – HTTP/1.1. https://www.ietf.org/rfc/rfc2616.txt, 1999. [Online; accessed 30-08-2015 13:55].

[21] uClibc. uClibc FAQ. http://www.uclibc.org/FAQ.html, 2015. [Online; accessed 30-08-2015 19:50].

[22] OWASP. Cross-Site Request Forgery (CSRF). https://www.owasp.org/index.php/Cross-Site_Request_Forgery_(CSRF), 2015. [Online; accessed 16-09-2015 12:03].

[23] OWASP. Cross-Site Scripting (XSS). https://www.owasp.org/index.php/Cross-site_Scripting_(XSS), 2014. [Online; accessed 31-08-2015 10:44].

[24] IETF. RFC6454 The Web Origin Concept. https://tools.ietf.org/html/rfc6454#section-3.4.2, 2011. [Online; accessed 31-08-2015 10:46].

[25] Rapid7 Labs. Project Sonar. https://scans.io/data/rapid7/sonar.http/20150818-http.gz, 2015. [Online; accessed 01-09-2015 20:45].

[26] BSI. Kryptographische Verfahren: Empfehlungen und Schlussellängen. https://www.bsi.bund.de/cae/servlet/contentblob/477256/publicationFile/30924/BSI-TR-02102_V1_0_pdf.pdf, 2015. [Online; accessed 16-09-2015 13:52].

[27] Winbond. W25Q32FV Datasheet. http://pdf.datasheetarchive.com/indexerfiles/Datasheets-IS46/DSA00916759.pdf, 2012. [Online; accessed 08-09-2015 15:21].

[28] agere systems. Soft Modem AT Command Reference Manual. http://www.produktinfo.conrad.com/datenblaetter/950000-974999/955662-an-01-en-Befehlsliste_ANALOG_USB_MINI_MODEM.pdf, 2005. [Online; accessed 08-09-2015 15:29].