Fraunhofer
FKIE

FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE FKIE

HARDWARE- UND HARDWARENAHE TROJANER

Überblick und Bedrohungslage

HARDWARE-TROJANER

Überblick und Bedrohungslage (08/17)

Peter Weidenbach, Raphael Ernst

Dr. Elmar Padilla

Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie, FKIE
in Wachtberg und Bonn.

Dieser Bericht wurde in Teilen finanziell gefördert durch das Bundesamt für Sicherheit in der Informationstechnik.

Inhalt

1
Vorwort

51 Milliarden Euro – das ist der geschätzte Schaden, den allein deutsche Unternehmen jährlich durch Cyberattacken erleiden. Gleichzeitig sind auch etwa 51% aller deutschen Unternehmen Opfer von Cyberattacken geworden. Die Bedrohungslage durch Cyberangriffe ist real – und sie wächst.

In einer zunehmend vernetzten und digitalisierten Welt wird die Angriffsfläche für Cyberattacken zwangsläufig größer. Wo sich 1985 noch eine Handvoll Viren & Würmer verantwortlich für punktierten Schaden zeigten, sind im Jahr 2016 ganze Bot-Netzwerke zusammengeschaltet und bringen hunderttausende Kunden oder ganze Regierungsnetze offline. Diese wachsende Angriffsoberfläche durch die steigende IT-Durchdringung erhöht das Risiko von Angriffen. Zudem ist eine zunehmende Professionalität der Hacker-Community (organisiert und zielgerichtet) erkennbar, was gleichzeitig das Ausmaß an potentiellem Schaden erhöht. So werden auch Schwachstellen schnell (mitunter schon wenige Stunden nach Veröffentlichung) und vollautomatisch ausgenutzt.

Natürlich kann niemand hundertprozentige Sicherheit garantieren: Kein Hersteller von Hardware-Komponenten wie Routern, kein Netzbetreiber und – neu – auch kein Hersteller von Internet-of-Things (IoT)-Geräten wie Smartphones und Tablets – aber auch inzwischen Kühlschränken, Kaffeemaschinen oder TV-Geräten. So verfügt beispielsweise ein moderner Fernseher über ein eigenes Betriebssystem sowie Internetschnittstellen und somit über etliche Programmzeilen, die mehr als den Programmwechsel oder die Lautstärke regeln. Neben Programminformationen können auch Bewertungen zu Sendungen abgegeben werden. Gleichzeitig kann auch mit TVs inzwischen Videotelefonie betrieben werden. Was passiert, wenn hier die Kamera gekapert und ferngesteuert wird? Oder wenn scheinbar durch »Geisterhand« kostenpflichtige Inhalte ohne Zustimmung des Eigentümers erfolgen?

Trotz umfangreicher Tests ist niemals ausgeschlossen, dass darin Fehler enthalten sind. Aber es muss sichergestellt sein, dass Schwachstellen unverzüglich beseitigt werden, wenn sie bekannt werden. Dann läuft nämlich der Countdown: Es ist nur eine Frage der Zeit, bis Kriminelle diese Lücke ausnutzen und so z.B. gekaperte Kühlschränke zu einem Bot-Netz verbinden und Attacken starten.

Der vorliegende Bericht liefert einen guten Überblick über die Bedrohungslage im Kontext hardwarenaher Trojaner und schafft somit dringend notwendige Transparenz. Diese Transparenz hilft neue Testmethoden entwickeln zu können. Nur wenn wir verstehen, wie die Angreifer arbeiten und welcher Schwachstellen sie sich bedienen, können wir als Industrie wirksame Gegenmaßnahmen entwickeln und Boden im Kampf um die Sicherheit unserer Kunden und aller Nutzer gut machen.

Der Countdown läuft…

Thomas Tschersich
Senior Vice President Internal Security and Cyber Defense
T-Systems

2
Lesehinweise

Dieser Bericht muss nicht von vorne nach hinten gelesen werden. Es wird allerdings empfohlen das Grundlagenkapitel 4 vor den Kapiteln 5 bis 7 zu lesen, da an diversen Stellen der Kapitel 5 bis 7 auf Informationen aus den Grundlagen verwiesen wird.
Die Kapitel 5 bis 7, die sich mit den einzelnen Hardware-Trojaner Kategorien beschäftigen, sind ähnlich aufgebaut. Nach einer kurzen allgemeinen Einführung folgt jeweils ein Abschnitt zu Infektionsvektoren und zu möglichen Schutzmechanismen. Im Kapitel 7 IC-Trojaner gibt es einen zusätzlichen Abschnitt über Trigger, die eine Aktion auslösen. Im Anschluss werden in allen drei Kapiteln die einzelnen Geräteklassen betrachtet und in Form von einheitlichen Steckbriefen ausgewertet. In diesen werden Quick-Read-Icons verwendet, die dem Leser die jeweils wichtigsten Informationen vermitteln ohne den gesamten Steckbrief lesen zu müssen.

2.1
Quick-Read-Icons

Es folgt eine kurze Erläuterung der einzelnen Quick-Read-Icons.

2.1.1
Status Icons

Hardware-Trojaner für diese Geräteklasse sind nachweislich im aktiven Einsatz bei Kriminellen, Behörden oder Geheimdiensten.

Es gibt funktionierende Proof-of-Concepts (PoC) von Hardware-Trojanern für diese Geräteklasse.

2.1.2
Icons zu möglichen Angriffsvektoren

Denial of Service (DoS) Angriffe sind möglich. Siehe dazu Abschnitt 4.3.2.1.

Ermöglicht Remote Zugang. Siehe dazu Abschnitt 4.3.2.2.

Das Gerät kann als Brückenkopf ins interne Netzwerk genutzt werden. Siehe dazu Abschnitt 4.3.2.3.

Geräte dieser Klasse ermöglichen Man in the Middle (MitM) Angriffe. Siehe dazu Abschnitt 4.3.2.4.

Bei Geräteklassen mit diesem Symbol sind Angriffe über den Direct Memory Access (DMA) möglich. Siehe dazu Abschnitt 4.3.3.1.

3 Einleitung

Anhand der Medienberichterstattung der letzten Jahre lässt sich ein Trend erkennen, dass Hardware- und hardwarenahe Trojaner eine immer größere Verbreitung finden.
Auf Sicherheitskonferenzen sind Themen zu Hardware- und hardwarenahen-Trojanern ein fester Bestandteil. So zeigten zwei Forscher aus den USA einen Proof-of-Concept (PoC), bei dem sie die Firmware des Multimedia Systems eines Autos aus der Ferne manipulierten, sodass sie direkten Zugriff auf den Kommunikations-Bus des Fahrzeugs erhalten konnten. Diesen Zugriff konnten sie nutzen, um wichtige Fahrzeugfunktionen zu manipulieren. So ist es ihnen u.a. gelungen, die Bremsen des Fahrzeugs zu deaktivieren (1).
Hardware- und hardwarenahe Trojaner sind nicht nur ein akademisches Forschungsfeld, sondern befinden sich bereits seit Jahren im produktiven Einsatz bei Geheimdiensten. Einer der bekanntesten Vorfälle ist Stuxnet, der bereits seit mindestens 2007 von Geheimdiensten eingesetzt wurde, um das iranische Atomprogramm zu sabotieren. Stuxnet hat die Steuereinheiten von Zentrifugen befallen, die zur Urananreicherung gebraucht werden. Dabei hat Stuxnet die Zentrifugen so angesteuert, dass sie unbrauchbares Material erzeugen und sich selber beschädigen.
Mittlerweile sind Hardware- und hardwarenahe Trojaner günstig zu beschaffen bzw. einfach zu implementieren, sodass sie auch von Kriminellen vielfach eingesetzt werden. So installierten 2013 Kriminelle Hardware-Keylogger und Display-Cloner in einer Bank, um auf diese Weise an Zugangsdaten zu gelangen (2).
Eine immer größere Bedeutung gewinnen auch Bot-Netze bestehend aus Embedded Devices, wie z.B. Home Router oder auch Geräten, die man gemeinhin dem Internet-of-Things (IoT) zuschreibt. Eines dieser Botnetze wurde 2016 genutzt, um den größten bisher gemessenen Distributed Denial of Service-Angriff (DDoS) auszuführen. Dieser erreichte fast die doppelte Bandbreite wie der bis dato größte gemessene DDoS (3).

Wie die obigen Beispiele aus den Medien zeigen, sind klassische IT-Szenarien nicht die einzigen Anwendungsfelder für Hardware- und hardwarenahe Trojaner. So ist potentiell fast jedes elektronische Gerät anfällig. Auch Geräte in sensiblen Bereichen wie der Medizintechnik oder kritischen Infrastrukturen wie Strom- und Wasserwerke können Ziele von Hardware-Trojanern sein. Dies verdeutlicht, dass der Einsatz von Hardware- und hardwarenahen Trojanern weitreichende Folgen im privaten Leben, der Wirtschaft und der Landessicherheit haben kann.
Obendrein sind klassische Sicherheitskonzepte wie Intrusion Detection Systeme (IDS), Firewalls und Virenscanner wenig effektiv gegen eine solche Bedrohung.
Zusammenfassend muss man Hardware- und hardwarenahe Trojaner als eine der größten Bedrohungen dieses Jahrzehnts ansehen.

Der vorliegende Bericht vermittelt zunächst einige Grundlagen und geht anschließend in den Kapiteln 5 bis 7 sowohl auf das theoretische Gefahrenpotential in den einzelnen Bereichen als auch reale Vorfälle sowie im akademischen Bereich publizierte PoCs ein. Des Weiteren wird auf mögliche Schutztechniken eingegangen, die zum Teil allerdings wenig verbreitet sind und zudem in vielen Fällen keinen umfassenden Schutz bieten.

4
Grundlagen

In diesem Kapitel werden einige Grundlagen, die zum Verständnis des weiteren Berichtes nötig sind, erläutert. Zunächst werden die verschiedenen Arten der Hardware-Trojaner eingeführt und auf deren mögliche Verbreitungswege eingegangen. Darauf folgen Abschnitte über grundsätzliche Gefahrenpotentiale sowie mögliche Kommunikationskanäle der Trojaner.

4.1
Klassifizierung von Hardware- und hardwarenahen Trojanern

Der Begriff Hardware-Trojaner ist in verschiedenen Bereichen unterschiedlich definiert. Im Ingenieurwesen werden Hardware-Trojaner meist auf »bösartige« Funktionalitäten beschränkt, die auf Schaltkreisebene implementiert sind (4). Im gängigen Sprachgebrauch erstreckt sich der Begriff auch auf Embedded Devices, Computer-Komponenten sowie spezielle Hardware wie z.B. externe Keylogger.
Um Missverständnisse zu vermeiden, werden in der Folge drei Arten von Hardware- bzw. hardwarenahen Trojanern unterschieden:

- **Firmware-Trojaner:** Als Firmware-Trojaner werden Geräte definiert, bei denen die Firmware manipuliert oder ausgetauscht wurde. Hierzu zählen auch »bösartige« Programme, die auf der Firmware laufen. Im eigentlichen Sinne sind dies keine Hardware- sondern hardwarenahe Trojaner, denn die Hardware selbst ist identisch zu derer nicht kompromittierter Geräte.
- **Malicious Hardware:** Malicious Hardware sind Geräte, die entweder nur zu ihrem bösartigen Zweck konstruiert wurden oder gutartige Geräte, die mit zusätzlicher bösartiger Hardware ausgestattet sind. Je nach Komplexität enthalten diese Geräte eine eigene anpassbare Firmware. Das bekannteste Beispiel für Malicious Hardware sind externe Keylogger, die zwischen Tastatur und Computer gesteckt werden.
- **Integrated Circuit Trojaner (IC-Trojaner):** Als IC-Trojaner werden »böse« Funktionalitäten auf Schaltkreisebene bezeichnet. Ein bekanntes Beispiel sind Kill-Switches, die bei einem bestimmten Trigger die Funktion des Integrated Circuits (IC) zerstören. Dies schließt nicht aus, dass Kill-Switches legitime Anwendungen haben können.

In der Folge werden alle drei Arten als Hardware-Trojaner zusammengefasst. Die einzelnen Trojanerarten und ihre Ausprägungen werden in den Kapiteln 5 bis 7 näher betrachtet.

4.2
Verbreitungswege

Abhängig von der Art des Hardware-Trojaners gibt es unterschiedliche mögliche Verbreitungswege, die in der Folge vorgestellt werden.

4.2.1
Entwicklungs-/Designphase

Bei der Entwicklung bzw. beim Design eines Produktes werden bereits bösartige Funktionen eingeplant. Dies ist vor allem bei IC-Trojanern verbreitet, da Schaltkreise in einem IC nicht nachträglich manipulierbar sind. (4).

Aber auch bei Firmware-Trojanern werden bereits bei der Entwicklung Hintertüren eingebaut. So hat z.B. ein chinesischer Hersteller Bootkits in UEFI eingebaut, welche Software des Herstellers auch bei einer Neuinstallation des Systems mit unabhängigen Installationsmedien automatisiert installiert (5).
In vielen Fällen ist jedoch nicht unterscheidbar, ob eine Hintertür absichtlich oder versehentlich eingebaut wurde. So wurde im Jahr 2014 ein nicht dokumentierter offener Port in zahlreichen Home-Routern diverser Hersteller entdeckt, über welchen man unter anderem die Konfiguration inklusive Passwörtern auslesen kann (6). Ob es sich hierbei um einen legitimen Debug-Port handelte, dessen Entfernung im finalen Produkt lediglich vergessen wurde, oder ob es eine absichtlich platzierte Hintertür ist, ist nicht bekannt. Dass so viele Hersteller von diesem Fall betroffen waren, liegt vermutlich daran, dass die Hersteller die Hintertür nicht selbst eingebaut haben, sondern diese bereits in einer zugekauften Komponente enthalten war.

4.2.2 Produktionsphase

Während der Produktion werden Geräte bzw. ICs kompromittiert. Neben der Designphase ist dies der einzige Weg IC-Trojaner zu verbreiten. Dazu wird beispielsweise die Lithografiemaske, die bei der Herstellung die Strukturen auf dem Chip bestimmt, gegen eine manipulierte Version ersetzt.

Des Weiteren lassen sich bei der Produktion Firmware-Trojaner einschleusen, was diverse Vorfälle aus der Vergangenheit belegen. Exemplarisch sei hier ein Vorfall aus dem Jahr 2013 erwähnt, bei dem E-Plus Smartphones mit vorinstalliertem Virus verschickt hat (7). Dabei wurde zwar nicht die Firmware selbst manipuliert, aber der Infektionsweg ist äquivalent nutzbar - in diesem Falle das Kompromittieren der Masterkopie des Datenspeichers in der Fabrik.

Der Einbau von Malicious Hardware während der Produktion ist zwar grundsätzlich möglich, aber wachsame Mitarbeiter könnten eine zusätzliche Komponente, die verbaut wird, bemerken. Das Risiko, dass die Manipulation frühzeitig entdeckt wird, ist in diesem Fall wesentlich höher.

4.2.3 Transportweg

Geräte werden während des Transports zum Händler oder zum Endabnehmer manipuliert. Hierbei kann sowohl die Firmware manipuliert als auch zusätzliche Malicious Hardware verbaut werden. Besonders lukrativ ist diese Infektionsmethode, da gezielt Unternehmen oder sogar einzelne Personen angegriffen werden können.
Laut den Dokumenten von Edward Snowden ist das Abfangen und Manipulieren von Ware auf dem Transportweg gängige Praxis bei der NSA (8).

4.2.4 Remote Infektion

Geräte aus der Ferne (Remote) zu infizieren ist nur mit Firmware-Trojanern möglich. In der Regel werden hier Schwachstellen in der Firmware oder dem Firmware-Update-Prozess ausgenutzt, um eigenen Code einzuschleusen oder die Firmware komplett zu ersetzen.
Ein bekanntes Beispiel für einen solchen Angriff ist ein im Jahr 2013 entdecktes Botnetz aus Home-Routern, dessen Schadsoftware selbständig neue Opfer im Internet sucht und infiziert (9). Dabei wurde eine Schwachstelle genutzt, die im integrierten http-Server der Geräte enthalten war.

Als Übertragungsweg können jedoch nicht nur Netzwerke dienen, sondern auch Wechseldatenträger wie USB-Sticks. Ein entsprechender PoC wurde 2014 präsentiert (10).

4.2.5 Vor Ort

Am finalen Standort der Geräte lassen sich sowohl Firmware-Trojaner einspielen, als auch Malicious Hardware installieren.
Laut Edward Snowden ist es gängige Praxis bei der NSA, Agenten in Unternehmen einzuschleusen, um vor Ort Überwachungstechnik zu installieren (11). Dies umfasst vermutlich sowohl klassische Computer-Trojaner, als auch Firmware-Trojaner sowie Malicious Hardware in diversen Ausführungen.
Des Weiteren gibt es diverse dokumentierte Vorfälle zu Vor-Ort-Installation von Malicious Hardware. Beispielsweise installierten 2013 Kriminelle Hardware Keylogger in einer Bank, um Passwörter zu stehlen (2).

4.3 Angriffsmöglichkeiten

Der erste Teil dieses Abschnitts geht auf die allgemeinen Schutzziele ein, die durch Hardware-Trojaner gefährdet werden. Der zweite Teil beschreibt einige gängige Angriffe, die von Hardware-Trojanern sowie anderer Malware genutzt werden, um Schutzziele zu untergraben. Im dritten Teil wird auf Angriffe eingegangen, die Hardware-Trojaner-spezifisch sind.

4.3.1 Allgemeine Schutzziele

Hardware-Trojaner können genutzt werden, um alle wesentlichen IT-Schutzziele auszuhebeln: Verfügbarkeit (Availability), Geheimhaltung (Confidentiality) und Integrität (Integrity).

4.3.1.1 Verfügbarkeit (Availability)

Verfügbarkeit beschreibt den Zustand, dass ein Service erreichbar ist und dass dieser ordnungsgemäß funktioniert. Angriffe auf die Verfügbarkeit können die Produktivität mindern oder gar zum Totalausfall von Systemen führen. Dies kann hohe finanzielle Auswirkungen haben.

4.3.1.2 Geheimhaltung (Confidentiality)

Geheimhaltung beschreibt den Schutz von Informationen vor dem Zugriff unautorisierter Parteien. Schadsoftware und Hardware-Trojaner können Daten stehlen und diese anschließend über einen Kommunikationskanal zum Angreifer übertragen. Im Abschnitt 4.4 wird näher auf die möglichen Kommunikationswege eingegangen. Dieser Datendiebstahl kann als Mittel zum Zweck der Spionage und des Betruges dienen.

4.3.1.3 Integrität (Integrity)

Integrität bedeutet, dass Informationen nicht verändert bzw. manipuliert wurden. Die Manipulation oder auch das Fälschen von Daten kann diverse Formen annehmen. Es

geht hierbei nicht nur um inhaltliche Daten, sondern auch um Metadaten, Protokoll-Dateien und Kommunikation. So können beispielsweise Spuren verwischt oder falsche Fährten gelegt werden. Anderseits können so auch Sicherheitssysteme lahmgelegt werden. Z.B. kann ein IDS, das an einem Mirror-Port eines Switches angeschlossen ist, getäuscht werden, wenn alle Merkmale für »böse« Aktivitäten vom kompromittierten Switch vorab gefiltert werden.

4.3.2 Allgemeine Angriffe

In diesem Abschnitt werden gängige Angriffe erläutert, die von Hardware-Trojanern genutzt werden, um die Schutzziele zu untergraben. Hierbei sind die Techniken zum großen Teil äquivalent zu Strategien, die von Malware und insbesondere Remote Access Tools (RAT) und Bots verwendet werden.

4.3.2.1 Denial of Service (DoS)

Bei Denial of Service Angriffen wird versucht den Betrieb von Diensten zu stören oder gar die Verfügbarkeit komplett zu eliminieren. Dabei gibt es verschiedene Ansätze. Am bekanntesten sind Überlastungsangriffe, bei denen versucht wird eine große Zahl von Anfragen an ein System zu senden, um dieses zu überlasten. Eine Unterform dieses Überlastungsangriffs ist der Distributed Denial-of-Service (DDoS) Angriff, bei welchem mehrere angreifende Systeme versuchen ein System durch viele Anfragen zu überlasten.
Es gibt aber auch andere Arten von DoS Angriffen. Zum Beispiel kann man Geräte mit fehlerhaften Konfigurationen versehen.

4.3.2.2 Remote Zugang (Backdoor)

Mit Remote Zugang bezeichnet man die Fähigkeit aus der Ferne Code auf Maschinen ausführen zu können. Meist ist dies sogar in Echtzeit möglich.
Remote Zugänge gefährden sowohl die Verfügbarkeit als auch die Geheimhaltung und Integrität. Dementsprechend bietet ein Remote-Zugang den Angreifern weitreichende Möglichkeiten. Wenn der Remote Zugang dauerhaft besteht, spricht man von einem *persistenten* Remote Zugang.

4.3.2.3 Brückenkopf

Remote Zugänge können in der Regel auch als »Brückenköpfe« in ein internes Netzwerk dienen und so bestehende Sicherheitsmaßnahmen an der Netzperipherie umgehen. Teilweise brauchen interne Nutzer für Dienste keine Authentifizierung und es gibt weniger Beschränkungen durch Firewalls für intern angebotene Dienste.
Brückenköpfe können insbesondere genutzt werden, um weitere Geräte im internen Netzwerk zu infizieren. Dieses Vorgehen wird auch als »Lateral Movement« bezeichnet.

4.3.2.4 Man-in-the-Middle (MitM)

Bei Man-in-the-Middle Angriffen befindet sich der Angreifer auf dem Kommunikationsweg zwischen zwei Kommunikationspartnern. Je nachdem, ob und welche Sicher-

heitsmaßnahmen bei der Kommunikation getroffen wurden, kann ein Angreifer die Geheimhaltung und Integrität aufheben oder die Kommunikation komplett verhindern (Verfügbarkeit).
Selbst bei verschlüsselten Verbindungen können unter Umständen Daten gestohlen oder manipuliert werden, falls die Überprüfung des Kommunikationspartners unzureichend ist. In diesem Fall würde der Sender beim Versuch eine verschlüsselte Verbindung zum Empfänger aufzubauen unbewusst eine verschlüsselte Verbindung zum Angreifer aufbauen. Anschließend baut dieser eine weitere verschlüsselte Verbindung zum Empfänger auf. Somit werden beim Angreifer alle Daten entschlüsselt und anschließend wieder verschlüsselt.

4.3.3
Hardware-Trojaner spezifische Angriffe

In diesem Abschnitt wird auf Angriffe eingegangen, die spezifisch für Hardware-Trojaner sind.

4.3.3.1
Direct Memory Access (DMA) Angriffe

Bei Direct Memory Access (DMA) Angriffen wird das DMA Feature, das bei vielen Schnittstellen in einem Computer zum Einsatz kommt, ausgenutzt. Hierbei sind PC-Komponenten in der Lage ohne Umweg über Betriebssystem oder Prozessor auf den Arbeitsspeicher zuzugreifen. Einerseits beschleunigt dies interne Datentransfers um ein Vielfaches, andererseits ist ein Angreifer somit in der Lage beliebige Daten aus dem Arbeitsspeicher zu stehlen oder zu manipulieren. So kann er z.B. geheime kryptographische Schlüssel aus dem Speicher stehlen oder in die Ausführung eines Programms eingreifen, um beispielsweise eine Authentifizierung zu umgehen. DMA enthält von Haus aus keine Sicherheitsfunktionen, die auch nachträglich nur schwer zu realisieren wären.

4.3.3.2
Option ROM Angriffe

Option ROMs sind Bestandteile der Firmware von Erweiterungskarten, die beim Booten des PCs vom BIOS bzw. UEFI in den Arbeitsspeicher kopiert und dort aufgerufen werden. Option ROMs werden normalerweise dazu verwendet, um Erweiterungskarten über die normale BUS Initialisierung hinaus in einen betriebsbereiten Zustand zu versetzen. Zu den am weitesten verbreiteten Option ROMs gehören das Video-ROM der Grafikkarte, ohne das kein BIOS/UEFI-Screen auf dem Monitor erscheinen würde, und das PXE-ROM von Netzwerkkarten, das zum Booten von Netzwerkmedien nötig ist.
Option ROMs können Hooks auf Interrupts setzen und somit bei jedem Eintreten des Interrupt-Events Code ausführen. Dies ermöglicht weitreichende Angriffsmöglichkeiten, zumal der Option-ROM-Code unabhängig vom Betriebssystem ausgeführt wird.

4.4
Kommunikationskanäle

Hardware-Trojaner können auf verschiedene Weise untereinander, mit dem Angreifer in Person oder auch mit einem Command and Control Server (C2S) kommunizieren. Diese Kommunikation kann sowohl zum Ausleiten von Daten, als auch zum Übermitteln von Befehlen genutzt werden.

4.4.1 Wechseldatenträger

Disketten, Speicherkarten, USB-Sticks und externe Festplatten sind mögliche Kommunikationsmedien. Dabei gibt es für den Datenfluss verschiedene Szenarien. Zum einen könnte ein Agent am Gerät vor Ort gezielt Daten vom Gerät kopieren bzw. aufspielen. Zum anderen gibt es einen Best-Effort Ansatz, bei dem jedes verbundene Speichergerät mit den zu übertragenen Informationen versehen wird. Dabei werden die Daten im Hintergrund und womöglich versteckt auf den Wechseldatenträger geschrieben. Andere infizierte Geräte können diese dann wieder auslesen und ggf. auch über andere Kommunikationskanäle weiterleiten. So können auch Geräte ohne Netzwerkanschluss kontinuierlich aus der Ferne ausspioniert werden.

4.4.2 Netzwerk

Kommunikationskanäle über Netzwerke lassen sich in drei Kategorien einteilen:
Offene Kanäle, getarnte Kanäle und versteckte Kanäle. Jeder dieser Kanäle kann zusätzlich verschlüsselt sein.

4.4.2.1 Offene Kanäle

Offene Kanäle bedienen sich proprietären Protokollen oder Standardprotokollen wie FTP oder SSH. Diese Kanäle sind meist schnell zu identifizieren, da die entsprechende Kombination aus Protokoll und Gegenstelle normalerweise nicht vorkommen sollte. Daher lassen sie sich wirkungsvoll durch IDS erkennen bzw. durch Firewalls unterbinden.

4.4.2.2 Getarnte Kanäle (Protocol Tunneling / Translation)

Im Gegensatz zu offenen Kanälen wirken getarnte Kanäle wie legitime Kommunikation. Am häufigsten wird diese Kommunikation als verschlüsselter http-Traffic getarnt, der den Standard https-Port verwendet und auch die Header des originalen Protokolls nachbildet. Von außen ist dies nur schwer von einem normalen Benutzer zu unterscheiden, der im Internet surft. Somit ist diese Art Kommunikation von IDS-Systemen und Firewalls nur schwer zu erkennen bzw. zu unterbinden.

4.4.2.3 Versteckte Kanäle (Covert Channels)

Im Vergleich zu getarnten Kanälen wird bei versteckten Kanälen keine eigene Verbindung verwendet, sondern die Informationen werden in einer anderen legitimen Verbindung versteckt. Demensprechend sind diese Kanäle sehr schwer aufzuspüren.
Ein bekanntes Beispiel sind Timing Channels, bei denen beispielsweise der zeitliche Abstand von Datenpaketen zur Codierung von Informationen verwendet wird.
Covert Channels sind ein idealer Kommunikationsweg für Hardware-Trojaner, da sie sich generisch in das Konzept der angestrebten »Unsichtbarkeit« von Hardware-Trojanern einfügen. Einige Covert Channels funktionieren nur in lokalen Netzen, da viele Eigenschaften, in denen sich Informationen verstecken lassen, nicht eins-zu-eins durch einen Router weitergeleitet werden. Covert Channels lassen sich jedoch auch auf andere Arten realisieren. So können sie z.B. in Datei-Attributen versteckt werden, die dann als E-Mail verschickt oder über physische Datenträger verbreitet werden.

4.4.3 Funk

Funk bezieht sich hierbei nicht auf Standard Netzwerk-Übertragungen wie WLAN oder Bluetooth, sondern auf Übertragungen auf anderen Frequenzbereichen und Protokollen. Funkübertragungen können daher lediglich bei Malicious Hardware und einigen Embedded Devices genutzt werden, die Funk-Module für andere Zwecke haben. Dieser Kommunikationskanal ist relativ aufwendig und teuer, da auch ein Empfänger in Funkreichweite deponiert werden muss.

4.4.4 Schall

Geräte, die mit Mikrofonen und Lautsprechern ausgestattet sind, erfüllen alle Voraussetzungen, um Daten per Schall zu übertragen. 2013 gab es einen entsprechenden PoC durch Mitarbeiter des Fraunhofer FKIE (12). Bei diesem wurden fünf Computer über Schall in einem nicht hörbaren Bereich vernetzt. Die Reichweite unter Laborbedingungen Betrug bis zu 20 Meter. Im realen Umfeld in Gebäuden ist die Reichweite vermutlich deutlich geringer. Nichtsdestotrotz ist es möglich über Schall auch Geräte zu vernetzen und remote zu erreichen, die eigentlich keine Netzwerkverbindung aufweisen. Angeblich soll der BIOS-Trojaner BadBIOS über solche Fähigkeiten verfügen. Die Existenz dieses Trojaners konnte aber bisher nicht zweifelsfrei nachgewiesen werden (13).

4.4.5 Geteilter Speicher

Geteilter Speicher in einem System kann zur internen Kommunikation zwischen System-Komponenten genutzt werden. Dabei kann es sich sowohl um flüchtigen Speicher wie dem RAM oder um nicht flüchtigen Speicher wie eine Festplatte handeln. Am effizientesten kommunizieren die Geräte über DMA, bei dem Geräte direkten Zugriff auf den Arbeitsspeicher haben, ohne einen Umweg über das Betriebssystem oder den Prozessor gehen zu müssen. Diese Art der Kommunikation ist für das Betriebssystem unsichtbar.

5
Firmware-Trojaner

Firmware-Trojaner lassen sich in zwei Kategorien teilen:

- **Embedded Device Trojaner** sind bösartige Programme, die auf einem Embedded Device laufen. Dabei gilt als Embedded Device ein geschlossenes System mit eigenem Betriebssystem (engl. Operating System) (OS), das ohne andere Systeme lauffähig ist. Des Weiteren gilt für Embedded Devices, dass sie einen festgelegten Funktionsumfang haben, der nur geringfügig durch Software Updates geändert werden kann.[1]
- **Firmware Rootkits** sind bösartige Programme oder Funktionalitäten, die in Systemkomponenten integriert sind. Im Gegensatz zu Embedded Devices sind Systemkomponenten Teil eines Gesamtsystems, wobei die einzelnen Komponenten nicht ohne andere Komponenten des Systems lauffähig sind. Solche Komponenten sind z.B. Computerkomponenten wie Festplatten, Grafikkarten, Netzwerkkarten oder auch UEFI.
  Die Bezeichnung als Rootkit stammt von der Ähnlichkeit zu Software Rootkits, bei denen »böse« Aktivitäten sowie die Existenz der Malware selbst effektiv vor dem Benutzer als auch Virenscannern und anderer Sicherheits-Tools versteckt werden.

Obwohl sich Embedded Devices und Systemkomponenten technisch stark unterscheiden, sind die generischen Infektionswege und Schutzmechanismen sehr ähnlich.

5.1
Infektion

Grundsätzlich lassen sich Firmware-Trojaner in allen Phasen, die in Kapitel 4.2 aufgeführt werden, einschleusen. In der Folge werden die konkreten Methoden beschrieben.

5.1.1
Firmware Update

Viele Geräte bieten von Haus aus die Möglichkeit eines Firmware-Updates. Oft ist dieser Update-Prozess nicht oder nur unzureichend geschützt, sodass eine kompromittierte Firmware eingespielt werden kann. In vielen Fällen muss man sich weder vor dem Update authentifizieren noch gibt es eine Signaturprüfung, ob das Update wirklich vom Hersteller stammt.

5.1.2
Exploit

Bei einem Exploit wird die Firmware nicht während eines Updates, sondern über Schwachstellen zur Laufzeit kompromittiert. Exploits sind besonders gut für Remote-Infektionen geeignet und bei Geräten, die im Dauerbetrieb arbeiten.

[1] Smartphones, Tablets und klassische Computer sowie Notebooks fallen nicht unter die Embedded Devices, da sie universell einsetzbar sind.

Bei gezielten Angriffen helfen dabei Webseiten, wie z.B. routerpwn (14), den passenden Exploit zum Gerät zu finden. Hierbei sind diverse Faktoren hilfreich. Support und somit auch Firmware Updates für Embedded Devices gibt es meist nur innerhalb eines relativ kurzen Zeitraums von wenigen Jahren. Viele Geräte sind aber noch weit über diesen Support-Zeitraum hinaus im Einsatz und somit bleiben viele Schwachstellen offen, die erst nach dem Support-Zeitraum entdeckt werden. Zum Beispiel warnte das ICS-CERT im Jahr 2016 vor dem Einsatz eines Medikamentenverteilers für Krankenhäuser, welcher über 1400 Sicherheitslücken enthält, die aufgrund des abgelaufenen Support-Zeitraums nicht mehr behoben werden. Davon sind 715 Lücken als kritisch eingestuft (15). Zudem werden Firmware Updates oft nicht flächendeckend eingespielt, da es nicht wie bei PC-Software eine ausgereifte zum Teil vollautomatisierte Update-Infrastruktur gibt. Des Weiteren wird auch heute noch teilweise explizit vor einem Update der Firmware gewarnt wird, weil dieses beispielsweise zu einem Datenverlust führen kann.
Zusammenfassend: Wenn man eine Schwachstelle in einem Gerät findet, dann kann man diese oft viele Jahre einsetzen, um Geräte erfolgreich zu infizieren.
Lediglich bei Home-Routern scheint es einen Trend zu geben, diesen Zustand zu ändern. So integrierte AVM 2014 eine automatische Updatefunktion in seinen Routern (16).
Ein weiteres großes Problem ist der Einsatz von Drittanbieter-Software in Firmware. Diese führt dazu, dass oft nicht nur ein Gerät von einer Lücke betroffen ist, sondern eine ganze Reihe an Geräten aus unterschiedlichen Geräteklassen. So schätzt man, dass der Heartbleed-Bug in OpenSSL mehr als 100 Hersteller betroffen hat (17). Ein weiteres Beispiel ist ein GlibC-Bug der Anfang 2016 allein bei Cisco fast 100 Produkte betroffen hat (18).

5.1.3
Ausnutzen von Standardpasswörtern

Viele Embedded Devices werden mit Standardpasswörtern ausgeliefert, die man sehr leicht über öffentlich zugängliche Quellen (19) heraus finden kann.
Diese Standardpasswörter kann man nicht nur nutzen, um eine manipulierte Firmware einzuspielen (siehe 5.1.1), sondern auch zum Ändern der Konfiguration. So kann man z.B. in Routern statische Routen ändern oder Proxy-Server eintragen, die einen Angreifer in eine MitM Position versetzen. In manchen Fällen bieten Geräte auch einen Konsolenzugang, der mit einem Standardpasswort geschützt ist. In diesem Fall lassen sich auf einfache Weise eigene (Schad-) Programme ausführen.
In extremen Fällen sind Standardpasswörter in der Software hartkodiert, sodass diese sich nicht vom Benutzer bzw. Administrator ändern lassen (20). Diese Notfalltüren für den Kundensupport sind im Grunde absichtliche Backdoors, die auch missbraucht werden können.

5.1.4
Manipulieren der Firmware im geteilten Speicher

Firmware kann sowohl auf geteiltem persistentem Speicher als auch auf geteiltem flüchtigem Speicher manipuliert werden. Ersteres kann vor allem bei Embedded Devices auftreten, bei denen die Firmware, also quasi das Betriebssystem, im selben Dateisystem wie die Daten der Programme liegen. Hierzu muss lediglich eine Schwachstelle genutzt werden, um Schreibzugriff auf die Betriebssystemdateien zu erlangen.
Überschreiben der Firmware im flüchtigen Arbeitsspeicher kann sowohl bei Embedded Devices als auch bei Systemkomponenten auftreten. Systemkomponenten haben zwar oft dedizierte Prozessoren und Arbeitsspeicher, auf denen ihre Firmware ausgeführt wird, allerdings ist dieser meist auch über das Hardware-Adress-Mapping adressierbar. Beim Hardware-Adress-Mapping handelt es sich um eindeutige binäre Adressen, bei der sowohl jede Stelle des Arbeitsspeichers, als auch Ressourcen von Erweiterungskar-

Firmware-Trojaner

ten und sonstiger Hardware explizit adressiert werden können. Potentiell kann man folglich die Firmware im Arbeitsspeicher manipulieren. Die Betriebssysteme und Firmwares haben zwar diverse Schutzmechanismen, die diese Bereiche des Arbeitsspeichers schützen, aber diese lassen sich vermutlich über Techniken wie DMA umgehen. Eine solche Manipulation der Firmware ist aus diversen Gründen erstrebenswert. Zum einen müssen keine Signaturen oder Prüfsummen gefälscht werden, da diese in der Regel nicht zur Laufzeit erneut geprüft werden. Dies macht eine Übernahme des Gerätes wesentlich leichter. Zum anderen ist die Modifikation nicht persistent. Wird das Gerät neu gestartet, verbleiben keine Hinweise auf die Kompromittierung.
Ein mögliches Szenario für einen solchen Angriff ist ein Festplatten-Firmware-Trojaner, der die Firmware einer Netzwerkkarte im Speicher manipuliert, um am Betriebssystem vorbei Daten ins Netzwerk schicken zu können. Auf diese Weise kann sich ein Firmware-Trojaner im System verbreiten und mehr funktionale Möglichkeiten erringen, als es die ursprünglich befallene Hardware zugelassen hätte.

5.2 Schutz

Es gibt proaktive und reaktive Schutzmechanismen. Proaktive Mechanismen sollen verhindern, dass die Firmware überhaupt manipuliert werden kann. Reaktive Mechanismen sollen manipulierte Firmware entdecken. In der Folge werden einige Sicherheitskonzepte kurz vorgestellt.

5.2.1 Prüfsummen (Checksum)

Prüfsummen sind eine proaktive Sicherheitsmaßnahme mit geringem Sicherheitsgewinn, da sie lediglich eine Integritätsprüfung bieten. Bei Firmware können Prüfsummen in drei Ausführungen vorkommen.
Zum einen sind Prüfsummen meistens Bestandteil des Firmware-Containers. Diese werden beim Update der Firmware oder auch bei jedem Start des Gerätes automatisch überprüft. Schlägt diese Prüfung fehl, sollte im Idealfall das Update nicht funktionieren bzw. das Gerät nicht starten. Diese Prüfsumme kann ein Angreifer aber ohne große Probleme manipulieren und gegen eine gültige Prüfsumme austauschen. Dazu muss er lediglich die Position und die Art der Prüfsumme im Container herausfinden.
Zum anderen ist eine leicht abgewandelte und etwas sicherere Form die Integritätsprüfung durch »unabhängige« Hardware. Bei diesem Ansatz wird ein zusätzlicher Chip, wie z.B. Trusted Platform Module (TPM) oder ME, genutzt, um vor dem Start der Firmware deren Checksumme zu prüfen. Entsprechend verlässliche Checksummen müssen allerdings zuvor in diese Chips programmiert werden. Außerdem muss sichergestellt werden, dass die Zusatzchips selbst vor unautorisierter Manipulation geschützt sind.
Die dritte Ausführung von Prüfsummen muss manuell geprüft werden. Oftmals werden neben den Firmware-Update-Dateien auch die Prüfsummen einer Datei auf den Update-Web-Seiten der Hersteller zur Verfügung gestellt. Diese können manuell vom Mitarbeiter vor dem Einspielen geprüft werden. Es ist allerdings zu beachten, dass auch die Webseiten manipuliert sein können. Dazu muss nicht zwangsläufig der Server des Herstellers kompromittiert sein, sondern es kann auch durch eine MitM Attacke geschehen. Begünstigt werden diese durch nicht SSL-gesicherte Download-Seiten der Hersteller.
Alle drei Ansätze schützen nicht vor Manipulationen, die zur Laufzeit durchgeführt werden.

5.2.2 Signaturen

Signaturen sind eine Verbindung aus Prüfsumme und Asymmetrischer Verschlüsselung, die proaktiv sowohl Integrität als auch Authentizität sicherstellt. Damit das Verfahren sicher ist, wird vorausgesetzt, dass das Gerät den öffentlichen Schlüssel (public key) des Herstellers integriert hat und dieser nicht ausgetauscht werden kann. Signaturen bei Firmware werden grundsätzlich automatisiert geprüft. Allerdings gibt es Unterschiede, wann eine Signatur geprüft wird. Bei manchen Geräten wird diese nur beim Update-Prozess geprüft und bei anderen Geräten während des Systemstarts. Die zweite Variante ist zu bevorzugen, da eine Prüfung nur beim Update oft leicht umgangen werden kann.

5.2.3 Authentifizierung beim Update

Bei dieser proaktiven Maßnahme wird ein Zugang mit erweiterten Rechten benötigt, um ein Update durchführen zu können. Dieser Zugang ist beispielsweise durch ein Passwort oder andere Maßnahmen geschützt.

5.2.4 Read-Only Speicher

Read-Only Speicher ist eine proaktive Maßnahme, bei der das nachträgliche Ändern der Firmware technisch unterbunden wird. Bei diesem Ansatz ist problematisch, dass Bugs in der Firmware nicht nachträglich verbessert werden können. Wird folglich eine Sicherheitslücke in der Firmware gefunden, die durch einen Exploit ausgenutzt werden kann, ist es während der gesamten Lebenszeit des Gerätes möglich nicht persistente Firmware-Trojaner in das Gerät einzuschleusen.

5.2.5 Malware- und Rootkit-Scanner

Malware- und Rootkit-Scanner können sowohl proaktiv auf die Update-Datei als auch reaktiv während des Betriebs eingesetzt werden. Allerdings sind entsprechende Signaturen Voraussetzung für den erfolgreichen Einsatz. Zurzeit gibt es derlei Signaturen und Scanner nur für Embedded Devices mit Unix-ähnlichem Betriebssystem und dies auch nur, wenn eine entsprechende Malware bereits von Analysten entdeckt und analysiert wurde. Somit lässt sich der Schutz vor gezielten Angriffen durch spezielle auf das Opfer angepasste Trojaner mit dieser Technik nicht gewährleisten.

5.2.6 Intrusion Detection System (IDS)

IDS ist eine reaktive Maßnahme, die ungewöhnliches Verhalten von Geräten feststellen soll. IDSs sind meist im Netzwerk verteilt und beobachten von »außen«, ob ein Gerät sich ungewöhnlich verhält. Dies kann ein Indiz für Trojaner-Aktivität sein.
Im akademischen Bereich gibt es Bestrebungen IDS auch geräteintern gegen DMA-Angriffe zu nutzen (21).

5.2.7 Integritätsprüfung zur Laufzeit

Red Balloon Security hat eine reaktive Technologie vorgestellt, um Änderungen des Firmware-Speichers in Embedded Devices zu überwachen. Auf diese Weise wird verhindert, dass zur Laufzeit beispielsweise durch einen Exploit die Firmware im Arbeitsspeicher manipuliert wird. Demonstrationen und Dokumentation des Programms legen nahe, dass Prüfsummen fixer Speicherbereiche erzeugt und wiederholt geprüft werden. Die Prüfsummen scheinen zu einem Server übertragen zu werden, der diese mit einer Datenbank abgleicht. Des Weiteren wird der Speicher der Geräte randomisiert, sodass es Angreifern erschwert wird Exploits erfolgreich einzusetzen. (22). Da die Prüfsummen auf dem Gerät berechnet werden, scheint dieses Verfahren keinen umfassenden Schutz bieten zu können, da die Berechnung selbst manipuliert werden kann.

5.2.8 Akademische Ansätze

An dieser Stelle soll auf einige Ansätze aus dem akademischen Bereich eingegangen werden. Allerdings wurde keiner dieser Ansätze bisher bis zur Marktreife verfolgt.

Speicherabgrenzung (IOMMU)
Forscher haben vorgeschlagen DMA- und Option Rom-Angriffe durch den Einsatz der Input / Output Memory Management Unit (IOMMU) von VT-d zu verhindern und somit den Speicher Hardware-gestützt vor DMA-Angriffen zu schützen (23) (24). Jedoch ist es bereits diversen anderen Forschern gelungen IOMMU selbst zu attackieren (25) (26).

Zeitmessung in Verbindung mit Integritätsprüfung
Auf der CCS 2011 wurde ein Verfahren vorgeschlagen, um die Manipulation von Firmware in Systemkomponenten zu verhindern (27). Dazu wird die Firmware angepasst, sodass sie eine Checksumme des Komponentenspeichers unter Berücksichtigung einer Challenge des Hosts berechnet wird. Unter der Voraussetzung, dass das Host-System über eine Kopie der nicht manipulierten Firmware verfügt, kann der Host die Checksumme des Gerätes verifizieren. Des Weiteren wird geprüft, ob die Checksumme innerhalb einer festen Zeitvorgabe erstellt wurde. Es gibt allerdings berechtigte Zweifel, ob Verfahren dieser Art sicher sind, da teilweise Berechnungen auch ohne Challenge vorab durchgeführt werden können und man nicht davon ausgehen kann, dass die ursprüngliche Berechnung der Checksumme optimal implementiert war. So kann es ein effizienteres Verfahren geben, dass die Prüfsumme in weniger Zeit berechnet und somit dem Angreifer genügend Zeit verschafft, die Prüfsumme beliebig zu fälschen (28).

5.3
Embedded Device Trojaner / IoT-Trojaner

Embedded Devices haben heutzutage eine sehr hohe Verbreitung und kommen nicht nur in der IT, sondern in nahezu jedem Bereich des täglichen Lebens zum Einsatz. Hier sei insbesondere auf die Untergruppe der Internet-of-Things (IoT)-Geräte hingewiesen, welche im Allgemeinen Geräte beschreibt, die mit dem Internet verbunden sind. Allen gemein ist, dass sie ein OS haben, auf welchem diverse zusätzliche Software installiert ist. Die meisten Hersteller programmieren OS und Software nicht von Grund auf selbst, sondern greifen auf bestehende Produkte zurück. Als OS kommen sowohl proprietäre Systeme wie VxWorks als auch offene Systeme wie Linux-Derivate zum Einsatz. Bei der zusätzlichen Software sieht es ähnlich aus. Die Hürde Software für Embedded Devices zu schreiben oder anzupassen ist dementsprechend nicht sonderlich hoch, da die Software teilweise sehr gut dokumentiert und in den meisten Fällen weit verbreitet ist. In vielen Fällen steht gegen Gebühr oder sogar kostenlos die Entwicklungsumgebung samt Tool-Chain zu Verfügung.
Diese »standardisierte« Software hat zur Folge, dass Malware und Exploits für Embedded Devices oft ohne große Anpassungen auf einer ganzen Reihe von teilweise sogar unterschiedlichen Geräteklassen lauffähig sind. So infizierte Linux/Flasher.A nicht nur Home-Router sondern auch DVB-Boxen (9).

5.3.1
Netzwerkinfrastruktur

In Netzwerken gibt es verschiedene Geräte, die an unterschiedlichen Stellen im Netzwerk zum Einsatz kommen und deswegen auch ein sehr unterschiedliches Bedrohungsszenario bieten. Deshalb wird dieser Punkt in weitere Unterpunkte gegliedert.

5.3.1.1 Router

Beschreibung:
Router sind zentrale Komponenten in jeder Netzwerkinfrastruktur
und werden benötigt, um unterschiedliche Netze oder -segmente zu verbinden. Alle Informationen, die von einem Rechnernetz in ein anderes Rechnernetz gelangen sollen, werden durch einen Router weitergeleitet. Viele Embedded Router sind mit zahlreichen weiteren Funktionen ausgestattet wie z.B. DHCP-, DNS- und NTP-Server. Home-Router enthalten oft weitaus mehr Dienste wie z.B. File-, Print- und Medien-Server sowie Telefon- und Fax-Funktionen.

Angriffsmöglichkeiten:
Grundsätzlich sind alle in 4.3.2 aufgeführten Angriffe möglich. Insbesondere kann sämtlicher Internet-Verkehr mitgeschnitten werden. Bei Home-Routern können zusätzlich alle Dateien des Dateiservers gestohlen sowie manipuliert und Druckaufträge kopiert werden. Falls eine Telefonanlage integriert ist, kann diese abgehört werden.

Kommunikationskanäle:
Wechseldatenträger und Netzwerke sind mögliche Kommunikationskanäle.

Mögliche Erkennungsmethoden:
Angriffe, bei denen der Router als Brückenkopf ins interne Netz genutzt wird, lassen sich prinzipiell von IDS erkennen, sofern ungewöhnliche Kommunikation auftritt. MitM Attacken jedoch lassen sich nur bei verschlüsselten Verbindungen erkennen, sofern eine eindeutige Überprüfung der Kommunikationspartner stattfindet. Das Abgreifen und Manipulieren von Daten auf dem Router hingegen selbst lässt sich mit lokalen Maßnahmen, wie z.B. IDS, weder detektieren noch verhindern. Dies gilt auch für Angriffe, die durch den Router auf andere Ziele im Internet durchgeführt werden.

Vorfälle / PoC:
Es gab bereits mehrere Bot-Netze bestehend aus Home-Routern, u.a.:

- Linux/Flasher.A (9)
- The Moon (29)
- Lizard Stresser (30)
- Moose (31)
- Linux/Mirai (32)
- Linux.Wifatch (33)

Die ersten vier genannten Bot-Netze wurden sowohl zum Datendiebstahl als auch für DDoS Angriffe auf Internet-Dienste genutzt.
Das Mirai Botnetz ist das bekannteste dieser Botnetze. Es umfasst nicht nur Router, sondern auch eine ganze Reihe anderer Geräteklassen. Mirai wird ebenfalls für den bisher größten gemessenen DDoS-Angriff mit 1,1 Terabit pro Sekunde verantwortlich gemacht (34). Es verbreitet sich dabei sowohl über Sicherheitslücken als auch über Standardpasswörter (35).
Linux.Wifatch wurde bisher nicht nachweißlich für böse Aktivitäten verwendet und scheint gegenteilig sogar die befallenen Geräte gegen andere Angreifer abzusichern. Die Intention der Autoren ist nicht bekannt. Ob sie wirklich Gutes tun wollen oder aber mit ihren bösen Aktivitäten noch nicht angefangen haben, ist offen.
Des Weiteren findet man mindestens vier Produkte im NSA ANT Katalog, die auf Router abzielen:

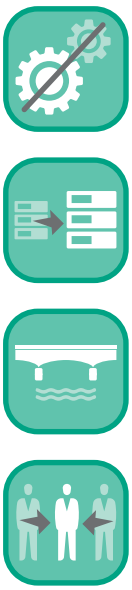
- Headwater
- Schoolmontana

- Sierramontana
- Stuccomontana

Die NSA Produkte sind hauptsächlich für Spionagezwecke konzipiert. Seit 2015 gibt es außerdem ein Exploit-Kit speziell für Router (36).
Ebenfalls 2015 macht ein amerikanischer Hersteller seine Kunden darauf aufmerksam, dass vermehrt Angriffe registriert wurden, bei denen die Firmware von Routern gegen manipulierte Versionen ersetzt wurde. Dabei loggen sich Angreifer in die Router ein und nutzen die normale Update-Funktion des Gerätes. Wie die Angreifer an die Zugangsdaten der Router gekommen sind, ist unklar (37). Es könnte sich um nicht geänderte Standardpasswörter gehandelt haben oder die Router wurden bereits auf dem Transportweg kompromittiert (vgl. Abschnitt 4.2.3).
2016 fand ein Sicherheitsforscher heraus, dass in LTE-Routern von Quanta gleich mehrere Backdoors vorhanden sind (38). Es ist nicht bekannt, ob diese vom Hersteller aus Unachtsamkeit oder absichtlich von einer dritten Partei eingebaut wurden. Perfide ist, dass Quanta auch Geräte für andere Hersteller produziert, die ähnliche Backdoors enthalten (39).

5.3.1.2 Switches

PoC



Beschreibung:
Switches sind die Verbindungsglieder zwischen einzelnen Netzwerkkomponenten und damit in nahezu jedem Netzwerk vorhanden. Zudem implementieren professionelle Switches viele wichtige Sicherheitsmaßnahmen in Netzwerken. Dazu zählen unter anderem V-LANs, die zur logischen Trennung von Netzwerken und deren Daten bestimmt sind, Access Control Listen (ACL), die beispielsweise dafür sorgen, dass sich nur bestimmte Geräte zu gewissen Ports verbinden können oder DHCP-Antwortpakete nur von einem Port weitergeleitetet werden (DHCP-Snooping). Des Weiteren können an Switches Mirror-Ports konfiguriert werden, an denen alle über den Switch laufenden Datenpakete geklont werden. Diese werden üblicherweise für IDS genutzt.

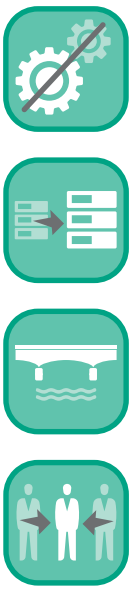
Angriffsmöglichkeiten:
Ein Fernzugang zu einem Switch kann genutzt werden, um Informationen über die Netzwerktopologie zu sammeln. Diese können als Grundlage für weitere Brückenkopfaktivitäten durch den Switch dienen.
Auch für DoS oder Bruteforce-Angriffe auf interne Netzwerkdienste sind Switches geeignet. Hierbei ist zu beachten, dass der Switch sich als jedes beliebige Gerät im Netzwerk ausgeben kann, was aufgrund der Position der Switches im Netzwerk nur in seltenen Fällen überhaupt detektierbar ist.
Des Weiteren sind Dank der zentralen Lage MitM Angriffe möglich. Zusätzlich können V-LANs und ACLs umgangen sowie IDS-Syteme ausgeschaltet werden, sofern diese an einem Mirror-Port des Switches hängen.

Kommunikationskanäle:
Netzwerke sind in der Regel der einzige Kommunikationskanal.

Mögliche Erkennungsmethoden:
Manche Angriffe können von IDS-Systemen, die an anderen Stellen des Netzwerks installiert sind, erkannt werden. Allerdings kann sich der Switch als jedes beliebige Netzwerkgerät im Netzwerk ausgeben, sodass es fast unmöglich ist, den Switch als Angreifer zu erkennen.
Außerdem ist eine Datenexfiltration am Switch kaum detektierbar. Da sich der Switch als jedes beliebige Gerät ausgeben kann, ist es theoretisch möglich sogar bestimmte Firewall-Regeln zu umgehen.

Vorfälle / PoC:
Auf dem 31C3 wurde in einem PoC gezeigt, dass Schwachstellen in der Firmware von Switches nicht nur genutzt werden können, um deren Konfigurationen auszulesen und zu ändern, sondern auch um die Firmware selbst zu manipulieren (40).

5.3.1.3 Firewalls



IN USE

Beschreibung:
Firewalls sind dazu gedacht (Sub-)Netze oder einzelne Geräte voneinander abzuschirmen und nicht autorisierte Kommunikation zu unterbinden.

Angriffsmöglichkeiten:
Firewalls können als Brückenköpfe und für MitM Angriffe genutzt werden. Außerdem können sie benutzt werden, um nicht autorisierte Kommunikation zwischen den (Sub-) Netzen zu ermöglichen und somit Sicherheitskonzepte wirkungslos zu machen. Im Umkehrschluss können sie auch genutzt werden, um erlaubte Kommunikation zwischen Netzen zu unterbinden, was einem DoS Angriff entspricht.

Kommunikationskanäle:
Netzwerke sind in der Regel der einzige Kommunikationskanal.

Mögliche Erkennungsmethoden:
IDS können die meisten Angriffe erkennen. MitM Angriffe können nicht erkannt werden.

Vorfälle / PoC:
Im NSA ANT Katalog gibt es mindestens fünf Produkte, die auf Firewalls abzielen:

- Feedtrough
- Gourmettrogh
- Jetplow
- Suffletrough
- Halluxwater

Halluxwater stellt einen persistenten Remote Zugang zur Firewall her, der zur Datenexfiltration gedacht ist. Die anderen Produkte sind Installer für Bananaglee, einer Backdoor Software von Digital Network Technologies (DNT), die von Haus aus nicht persistent zu sein scheint. Die genannten ANT-Produkte installieren Bananaglee bei jedem Neustart der Firewall. Teilweise bieten die Produkte auch eigene Backdoor-Funktionalitäten.
Außerdem fand im Jahr 2015 der Netzwerkausrüster Juniper offensichtlich absichtlich eingebaute Hintertüren im Source-Code seines hauseigenen Betriebssystems ScreenOS, welches auf Firewalls und VPN-Appliances zum Einsatz kommt (41). Außergewöhnlich ist, dass hier die Geräte im großen Stil bereits ab Werk manipuliert wurden.

5.3.2
IP-Telefone und Videokonferenzsysteme

Beschreibung:
IP-Telefone und Videokonferenzsysteme sind für audio- und visuelle Kommunikation zwischen Personen gedacht. Sie sind an ein Netzwerk angeschlossen und verfügen über Lautsprecher, Mikrofone und teilweise über Kameras sowie Bluetooth zum Anbinden von Headsets.

Angriffsmöglichkeiten:
Neben der Möglichkeit diese Systeme als Brückenköpfe zu benutzen, eignen sie sich durch ihre Mikrofone und Kameras auch als audio-visuelle Wanzen. Dies funktioniert grundsätzlich auch, wenn nicht telefoniert wird. Des Weiteren können Informationen wie Telefonbücher und Anruflisten gestohlen und manipuliert werden. Auch ein gezieltes Unterdrücken von Anrufen ist möglich.

Kommunikationskanäle:
Netzwerke sowie Schall sind mögliche Kommunikationskanäle.

Mögliche Erkennungsmethoden:
Brückenkopfaktivitäten lassen sich durch IDS erkennen. Eine Wanzenfunktion lässt sich evtl. über ein angepasstes IDS erkennen, das kontrolliert, ob größere Datenmengen von dem Telefon übertragen werden, obwohl kein Telefonat stattfindet.

Vorfälle / PoC:
Auf dem 29C3 gab es einen PoC, der zeigt, dass man die Firmware von IP-Telefonen manipulieren und diese zu Audiowanzen umfunktionieren kann (42).
Einen PoC zur Übernahme von Videokonferenzsystemen wurde auf der Blackhat Konferenz im Jahr 2013 präsentiert (43).
Außerdiesem gab es 2015 ein PoC, der demonstriert, dass Sicherheitslücken in Telefonen der Firma Snorm genutzt werden können, um diese komplett zu übernehmen (44).
2017 wurde im Rahmen der Vault 7 Leaks bekannt, dass die CIA Exploits für IP-Telefone entwickelt hat (45).

5.3.3
Drucker, Kopierer, Scanner und Fax

PoC

Beschreibung:
Drucker, Kopierer, Scanner und Fax findet man in fast jedem Büro. Oft sind diese Geräte in einem Gerät vereint. Ihnen gemein ist, dass sie mit sensiblen und teilweise geheimen Dokumenten in Berührung kommen und mit einem Netzwerk verbunden sind. Zudem werden Dokumente, die gedruckt gescannt und gefaxt werden, in einem internen Cache zwischengespeichert und sind oft noch eine ganze Weile nach Auftragsabschluss wiederherstellbar.

Angriffsmöglichkeiten:
Diese Geräte können als Brückenkopf genutzt werden. Außerdem ist es möglich jegliche Dokumente, die gedruckt, gescannt, kopiert oder gefaxt werden, zu stehlen oder zu manipulieren.

Kommunikationskanäle:
Als Kommunikationskanal steht das Netzwerk zur Verfügung. In manchen Fällen sind die Geräte per USB mit Computern verbunden, was auch für die Datenexfiltration genutzt werden kann. Vorhandene USB-Ports sowie Card-Reader können für eine Kommunikation mit Wechseldatenträgern benutzt werden. Im Falle von Geräten mit Faxfunktion kann zusätzlich die Telefonleitung als Kommunikationskanal genutzt werden.

Mögliche Erkennungsmethoden:
IDS Systeme können Brückenkopfaktivitäten und evtl. unerlaubte Verbindung, bei denen gestohlene Daten über das Netzwerk ausgeleitet werden, erkennen. Alle anderen Aktivitäten sind nur in Ausnahmefällen detektierbar.

Vorfälle / PoC:
Auf der 28C3 wurde im Rahmen eines PoC gezeigt, dass bei Xerox Druckern beliebiger Code, der in regulären Druckaufträgen integriert ist, ausgeführt werden kann, ohne die Firmware anpassen zu müssen. Dies schloss auch Memory Dumps und Dateisystemoperationen ein (46). Auf der NDSS 2013 gab es einen PoC, der zeigt, dass sich Firmware von HP-Druckern Remote per Druckauftrag austauschen lässt (47).

5.3.4
Home Entertainment

Beschreibung:
Fernseher sowie Set-Top-Boxen und Spielekonsolen fallen unter diese Kategorie. Diese Geräte stehen heutzutage nicht nur in privaten Haushalten, sondern auch in Büros und an öffentlichen Plätzen. Moderne Geräte dieser Klasse besitzen einen Netzwerkanschluss und zusätzlich verfügen viele Fernseher und Spielekonsolen über Mikrofone und Kameras. Teilweise weisen die Geräte auch USB-Anschlüsse auf.

Angriffsmöglichkeiten:
Home Entertainment-Geräte mit Netzwerkanschluss können als Brückenkopf genutzt werden. Wenn sie Mikrofon oder Kamera aufweisen, können sie auch als Wanze fungieren. Dies ist beispielsweise bei Geräten mit Sprach- oder Gestensteuerung der Fall.

Kommunikationskanäle:
Eine Kommunikation ist über das Netzwerk möglich. Theoretisch gäbe es auch einen Input-Kanal über ein TV- oder Radio-Signal. Dazu müsste ein Angreifer aber Zugriff auf die Sendestation oder die Hausverkabelung haben. Als Ausgangskanal können Schallwellen dienen. Sofern ein Mikrofon verbaut ist, kann Schall auch als Eingangskanal dienen. Falls USB-Ports verbaut sind, können auch diese zur Kommunikation über Wechseldatenträger genutzt werden.

Mögliche Erkennungsmethoden:
Brückenkopfangriffe können potentiell von IDS erkannt werden. Eine Wanzenfunktionalität ist nur in Ausnahmefällen nachweisbar.

Vorfälle / PoC:
Die Router-Malware Linux/Flasher.A befällt auch DVB-Boxen (9).
Ansonsten beweisen diverse PoCs, dass die Firmware von Spielekonsolen trotz ausgeklügelter Sicherheitskonzepte manipuliert werden kann. Die Spielekonsolenhersteller legen sehr viel Wert auf die Integrität der Firmware, da sie Raubkopierer fürchten, die mit einer Anpassung der Firmware Kopierschutzmaßnahmen umgehen könnten.
Samsung implementiert in seine Fernseher mit Sprachsteuerung eine Funktion, die alles Gesprochene an einen Service im Internet überträgt (48). Dies kommt einer in der Designphase eingebauten Wanze gleich, die auch von Geheimdiensten oder Kriminellen genutzt werden könnte.
Des Weiteren erläutert eine Webseite im Detail, wie man Root-Zugriff auf diverse Home-Entertainment-Geräte erlangt (49).
2017 wurde im Rahmen der Vault 7 Leaks bekannt, dass die CIA und der MI5 über ein Implant für Samsung Smart-TVs verfügen, das den Fernseher zur Audio- und Video-Wanze umfunktioniert (50).

5.3.5
Geldspielautomaten

Beschreibung:
Geldspielautomaten stehen oft in Kneipen, Spielhallen und Casinos. In der Regel haben sie keinen Netzwerkzugang und arbeiten isoliert.

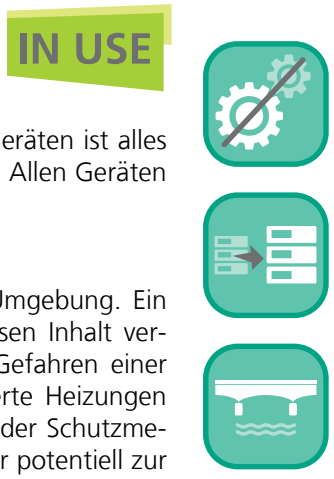
Angriffsmöglichkeiten:
Die Automaten können zum Betrug genutzt werden. Dabei werden sie so manipuliert, dass sie bei einer bestimmten Aktion einen hohen Gewinn ausschütten oder die Gewinnwahrscheinlichkeit wird zum Vorteil des Betreibers reduziert.

Kommunikationskanäle:
Keine.

Mögliche Erkennungsmethoden:
Aufmerksame Mitarbeiter könnten auf ein ungewöhnliches Gewinnausschüttungsverhalten aufmerksam werden, wenn die Kriminellen den Automaten regelmäßig plündern.

Vorfälle / PoC:
2015 wurde eine kriminelle Bande festgenommen, die gewerbsmäßig Geldspielautomaten manipuliert hat (51).

5.3.6
Smart Home / Gebäudetechnik



Beschreibung:
Smart Home / Gebäudetechnik umfasst eine ganze Reihe von Geräteklassen. Angefangen von fernsteuerbaren Steckdosen und Lampen über fernsteuerbare Heizungen bis hin zu fernsteuerbaren Küchengeräten ist alles in dieser Kategorie abgedeckt. Auch Fenster- und Türöffner zählen dazu. Allen Geräten gemein ist der direkte oder indirekte Netzwerkzugang.

Angriffsmöglichkeiten:
Neben dem Brückenkopfszenario haben alle Geräte Einfluss auf ihre Umgebung. Ein smarter Kühlschrank beispielsweise kann missbraucht werden, um dessen Inhalt verderben zu lassen, indem man die Kühlung zeitweise deaktiviert. Die Gefahren einer manipulierten Tür oder Fenstersteuerung sind offensichtlich. Manipulierte Heizungen können noch weitaus schlimmere Folgen haben. Durch das Abschalten der Schutzmechanismen oder der Manipulation von Sensorwerten könnten diese sogar potentiell zur Explosion gebracht werden und somit direkt das Leben von Menschen gefährden.

Kommunikationskanäle:
Netzwerke sind in der Regel der einzige Kommunikationskanal. Bei Sensoren ist auch eine Einwegkommunikation über das sensorspezifische Medium möglich. So könnte man z.B. Anweisungen an IP-Kameras über Lichtsignale schicken. Bei Aktoren ist eine Kommunikation in die andere Richtung möglich.

Mögliche Erkennungsmethoden:
Das Brückenkopfszenario kann ggf. durch IDS erkannt werden. Ungewöhnliches Verhalten von Geräten sowie falsche Sensordaten können evtl. über eine manuelle Plausibilitätsprüfung sichtbar werden. Bei gefälschten Anzeigen dürfte sich dies in der Praxis aber oft als schwierig erweisen.

Vorfälle / PoC:
2014 wurde im Rahmen eines PoC demonstriert, dass die Firmware von schaltbaren Steckdosen sehr einfach manipulierbar ist (52).
Des Weiteren erläutert eine Webseite im Detail, wie man Root-Zugriff auf diverse Smart-Home-Geräte erlangt (49).
2016 wurde demonstriert, dass HUE-Leuchten benutzt werden können, um Daten per Licht zu übertragen. Die Forscher stellen des Weiteren die These auf, dass die Leuchten auch benutzt werden könnten, um durch den Effekt der Photosensibilität bei anfälligen Personen epileptische Anfälle auszulösen (53).
Ebenfalls 2016 demonstrierten Forscher, wie sie eine Erpressungs-Software auf ein Thermostat einspielen konnten. Die Malware setzt dabei alle 30 Sekunden einen neuen PIN, sodass der Benutzer quasi ausgeschlossen ist. Anschließend wird das Thermostat auf einen für den Benutzer »unangenehmen« Wert eingestellt (54).
2016 demonstrierte ein Forscher die Übernahme per Remote-Angriff eines digitalen Videorekorders für Videoüberwachungssysteme (55). Laut Aussage des Forschers funktioniert der Angriff bei 70 verschiedenen Herstellern.
Ebenfalls 2016 wurde das Linux/Mirai Botnet nicht nur auf Routern und Gateways, sondern auch auf IP-Kameras und Video-Rekordern nachgewiesen (32).
2016 wurde bekannt, dass vermutlich die NSA mindestens seit 2005 Backdoors ab Werk in die Überwachungssysteme der Firma NetBotz (heute: Schneider Electric) eingebaut hat (56).
2017 demonstrierten Forscher einen Wurm, der sich selbständig auf smarten Glühbirnen mit ZigBee Übertragungsstandard ausbreitet (57).

5.3.7
Medizintechnik

PoC

Beschreibung:
In der Medizin werden an vielen Stellen Embedded Devices eingesetzt, die mittlerweile sehr oft vernetzt sind. Das Portfolio reicht von Zuckermessgeräten für den privaten Gebrauch über diverse Monitoring-Systeme und Infusionspumpen bis hin zu komplexen Systemen wie Ultraschall- oder Röntgengeräten.

Angriffsmöglichkeiten:
Neben dem Brückenkopfszenario können diese Geräte genutzt werden, um Patientendaten zu stehlen oder dem Patienten direkt zu schaden. Dies kann passiv bei Mess- und Monitoring-Systeme geschehen, indem die Anzeige manipuliert wird. Eine aktive Schädigung ist zum Beispiel durch Manipulationen an Infusionspumpen möglich. Eine permanente Schädigung oder gar der Tod des Patienten sind nicht auszuschließen.

Kommunikationskanäle:
Netzwerke sind in den meisten Fällen der einzige Kommunikationskanal.

Mögliche Erkennungsmethoden:
Brückenköpfe können potentiell über IDS erkannt werden. Manipulationen an Anzeigen oder falscher Dosierung können evtl. von sehr aufmerksamen Mitarbeitern entdeckt werden.

Vorfälle / PoC:
2015 wurden diverse Sicherheitslücken in Infusionspumpen der Firma Hospira gefunden. Unter anderem war eine Root-Shell über den LAN-Port verfügbar, die genutzt werden kann, um beliebigen Code auszuführen. Auch ein Update der Firmware ist auf diese Weise möglich ohne Sicherheitsmaßnahmen umgehen zu müssen. Diese Lücken können potentiell genutzt werden, um Patienten zu töten (58; 59).

5.3.8
Fahrzeugtechnik

PoC



Beschreibung:
In Fahrzeugen gibt es oft mehr als 50 Embedded Devices, sogenannte Electronic Control Units (ECU), die über einen Can-Bus verbunden sind. Für fast jede Funktion im Fahrzeug gibt es eine ECU – von der Motorsteuerung über Assistenzsystem wie ESP bis hin zu Multimedia-Geräten. Alle diese Devices sind oft mit demselben Bus verbunden, dessen Spezifikation keinerlei Sicherheitsvorkehrungen aufweist. So kann jedes Gerät alle Nachrichten auf dem Bus lesen und sich als jedes andere ausgeben und Nachrichten fälschen.

Angriffsmöglichkeiten:
Die größte Gefahr bei Firmware-Trojanern in Fahrzeugen ist der Zugang zum Can-Bus. Bereits 2010 wurde gezeigt, dass ein Zugriff auf den Can-Bus genutzt werden kann, um die Bremsen auszulösen oder den Motor zu stoppen (60). Hierbei können nicht nur Fahrzeuge beschädigt, sondern auch Menschenleben gefährdet werden.
Des Weiteren können Freisprecheinrichtungen genutzt werden, um Gespräche im Fahrzeuginnenraum aufzuzeichnen. Kameras, wie sie beim Müdigkeitswarner zum Einsatz kommen, lassen sogar eine Videoüberwachung des Fahrzeuginnenraums zu.
Außerdem kann die GPS-Funktion des Navigationssystems genutzt werden, um das Fahrzeug zu tracken.

Kommunikationskanäle:
Alle Geräte haben den Can-Bus als gemeinsames Kommunikationsmedium. Es gibt Geräte mit weiteren Kommunikationskanälen. So haben manche Multimedia-Systeme Zugriff auf Bluetooth, Internet, Radio und USB-Sticks.
Ein weiterer Kommunikationskanal wird durch den eCall bald flächendeckend eingeführt.

Mögliche Erkennungsmethoden:
IDS ähnliche Systeme könnten theoretisch ungewöhnliches Verhalten auf dem Can-Bus erkennen. Da aber alle Teilnehmer des Can-Busses quasi anonym sind, kann die befallende Komponente nicht ohne weiteres zweifelsfrei identifiziert werden. Eine Separierung der Busses, wie sie bereits bei manchen Fahrzeugherstellern eingesetzt wird, kann das Problem entschärfen.

Vorfälle / PoC:
2010 demonstrierten Forscher, dass sie eine Telematik-Einheit mit Schadcode infizieren können. Von dort aus nutzen sie den Can-Bus um die Bremsen auszulösen (60).
Auf dem 30C3 gab es einen weiteren PoC, bei dem das Multimediasystem des Fahrzeugs mit eigener Software versehen wurde (61).
2013 wurde ein Framework für Sicherheitsanalysen in Fahrzeugen veröffentlicht und viele weitere erfolgreiche Eingriffe in die Fahrzeugsteuerung wurden demonstriert wie zum Beispiel Deaktivieren der Bremsen oder aktive Eingriffe in die Lenkung (62).
2014 ist ein Handbuch zum Hacken von Autos erschienen, das 2016 eine erste Aktualisierung erfuhr (63).
Ebenfalls 2014 gab es eine ausführliche Studie mit Fahrzeugen diverserer Hersteller, bei der die theoretische Anfälligkeit solcher Angriffe untersucht wurde (64).
Basierend auf dieser Studie ist es 2015 Forschern in einem PoC gelungen ein Auto über dessen Internetverbindung zu hacken. Dabei demonstrierten sie unter anderem, dass sie über das Internet die Bremsen und die Schaltung unbrauchbar machen können. Sie zeigten des weiteren Eingriffe ins Lenkrad, das Entertainment System sowie die Lüftung (1). Kurze Zeit später berichten britische Medien über Forscher, denen es gelungen ist über Digital Audio Broadcast (DAB), das Multimediasystem eines Fahrzeuges zu hacken (65).

Firmware-Trojaner

2016 demonstrieren Forscher wie sie einen Tesla Model S durch diverse Sicherheitslücken aus der Ferne kapern. Unter anderem zeigen sie das Öffnen von Dachluke, Türen und Kofferraum sowie unfreiwilliges Anhalten eines fahrenden Fahrzeugs (66).

5.3.9
Geldtransfersysteme

Beschreibung:
Diese Kategorie umfasst Bank-Terminals, Geldautomaten und elektronische Bezahlsysteme im Einzelhandel (PoS).

Angriffsmöglichkeiten:
In der Regel werden Geldtransfersysteme zum Zweck des Betrugs kompromittiert. Hierbei werden Bankautomaten manipuliert, damit sie Geld ausgeben oder Bezahlterminals werden genutzt, um Giro- oder Kreditkartendaten abzugreifen (Skimming). Bankautomaten können zusätzlich als Brückenköpfe genutzt werden, um Zugang zum internen Bankennetz zu erhalten. Somit könnten auch großflächige DoS Angriffe durchgeführt werden.

Kommunikationskanäle:
Netzwerke sind meist der einzige Kommunikationskanal. Bezahlterminals haben teilweise NFC integriert.

Mögliche Erkennungsmethoden:
Brückenkopfangriffe können potentiell von IDS erkannt werden. Betrug wird vermutlich erst viel später entdeckt.

Vorfälle / PoC:
2013 wurde auf dem 30C3 von einem Vorfall berichtet, bei dem Kriminelle Bankautomaten mit Hilfe eines USB-Sticks so manipuliert haben, dass dieser ohne Buchung Geld ausgab (67).
2016 wurden mehrere Fälle bekannt, bei denen Geld aus Geldautomaten in Taiwan gestohlen wurde. Man geht davon aus, dass die Automaten mit Malware infiziert wurden (68).
2014 warnte das US-CERT vor der ersten bekannten Point-of-Sale (PoS) Malware namens Backoff (69). Diese suchte nach Buchungsdaten im Speicher, protokollierte Tastatureingaben und kommunizierte über einen Command and Control Server. 2015 wurden mit Malaum-POS und PoSeidon zwei weitere PoS-Trojaner entdeckt (70) (71).

5.3.10
Industrieanalgen

IN USE

Beschreibung:
Industrieanlagen bestehen aus einem Sammelsurium an Embedded Devices, die komplexe Mess- und Regelaufgaben genauso abdecken wie die Steuerung von Robotern. Diese Geräte, sogenannte Programmable Logic Controler (PLC), sind bereits heute stark vernetzt, um mit möglichst wenigen Mitarbeitern komplexe Anlagen steuern und überwachen zu können. Zur Überwachung kommen dabei weitere Embedded Devices, die Human Machine Interfaces (HMI), zum Einsatz.
Im Rahmen der »Industrie 4.0«-Initiative ist zu erwarten, dass diese Vernetzung weiter zunimmt. Sie basiert häufig auf dem Modbus-Protokoll, das ähnlich wie der Can-Bus bei Fahrzeugen keinerlei Sicherheitsmaßnahmen implementiert.

Angriffsmöglichkeiten:
Die Geräte können als Brückenköpfe dienen. Viel verheerender können aber DoS Angriffe sein, die die Produktion beeinflussen. Dies kann zu mangelnder Qualität der produzierten Produkte, aber auch zu Ausfällen der Produktion bis hin zur Zerstörung einer Produktionsanlage führen.

Kommunikationskanäle:
Die Geräte sind in der Regel vernetzt und kommunizieren teilweise auch über Funk oder Infrarot.

Mögliche Erkennungsmethoden:
Brückenkopfaktivitäten können potentiell von IDS erkannt werden. DoS Angriffe werden vermutlich erst anhand der Auswirkungen sichtbar.

Vorfälle / PoC:
Der bekannteste Vorfall, Stuxnet, hat seine Anfänge vermutlich bereits im Jahr 2005 und wurde erst im Jahr 2010 entdeckt. Der Firmware-Trojaner befiel Zentrifugen, die zur Anreicherung von Uran verwendet werden. Den Trojaner gab es in zwei Versionen: Die erste Version sollte möglichst unauffällig arbeiten und die Ausfälle nach normalem Verschleiß aussehen lassen. Die zweite Version, die ab 2009 eingesetzt wurde, war wesentlich aggressiver, was vermutlich auch zu dessen Entdeckung führte. Stuxnet verbreitete sich ursprünglich über USB-Sticks, die zweite Version zusätzlich über Netzwerke (72).
2014 wurde ein Angriff auf ein deutsches Stahlwerk publik. Es ist nicht offiziell bestätigt, aber Ausfälle von Steuerungskomponenten und ganzen Anlagen legen den Einsatz von Firmware-Manipulationen nahe (73).

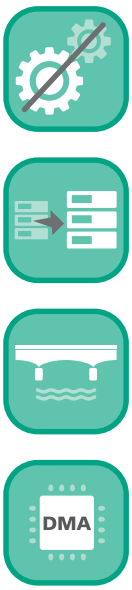
5.3.11 Militärtechnik

In militärischen Fahrzeugen und Anlagen sind ähnlich wie im zivilen Bereich diverse Embedded Systems verbaut. Diese bieten ähnliche Angriffsvektoren wie im zivilen Bereich und öffentlich gewordene Vorfälle zeigen, dass die Sicherheit dieser Systeme ähnlich stiefmütterlich behandelt wird (74) (75). An dieser Stelle sei im Besonderen auf den Data Distribution Service (DDS) hingewiesen, welcher momentan bereits im maritimen Bereich eingesetzt wird, um Systeme mit einander zu verbinden und später auch in Landfahrzeugen Verwendung finden soll. Dieser bietet eine ähnliche Funktionalität wie der Can-Bus bei Fahrzeugen und ist genau so wenig abgesichert.
Auf Grund der wenigen öffentlich verfügbaren Informationen wird an dieser Stelle auf eine genauere Betrachtung verzichtet.

5.4 Firmware Rootkits

Firmware Rootkits sind eine große Bedrohung für jeden Computer, da diese in der Lage sind, am Betriebssystem vorbei Daten zu manipulieren, abzugreifen und sie im Rahmen der Möglichkeiten der befallenden Komponente sogar auszuleiten. Auf dem Host selbst ist dieses bösartige Verhalten mit den heute zur Verfügung stehenden Mitteln meist nicht erkennbar.

5.4.1
BIOS / UEFI



IN USE

Beschreibung:
Das Basic Input Output System (BIOS) bzw. dessen Nachfolger
das Unified Extensible Firmware Interface (UEFI) ist dazu gedacht die Komponenten eines Computers soweit zu initialisieren, dass ein Betriebssystem gestartet werden kann. Im Gegensatz zum BIOS ist UEFI ein eigenes kleines Betriebssystem, das Treiber für Dateisysteme, Netzwerkkarten, Grafikkarten und vieles mehr mitbringt. UEFI ist gut dokumentiert und es gibt eine Open-Source Referenzimplementierung (76), die vielen UEFI Herstellern als Grundlage dient. Dank diverser frei verfügbarer Tools kann jeder technisch Versierte UEFI Images nach Belieben manipulieren. Daher ist das Erstellen von UEFI Trojanern besonders leicht und günstig, sofern man sie nicht Remote einschleusen möchte.

Angriffsmöglichkeiten:
BIOS und vor allem UEFI bieten vielfältige Angriffsmöglichkeiten. Das BIOS wird häufig missbraucht, um Malware insbesondere in den Bootsektoren der Festplatten zu persistieren. Wird die Malware zwischenzeitlich aus dem Bootsektor entfernt, so wird sie bei jedem Neustart neu installiert. So übersteht diese Malware auch den Austausch der Festplatte und anderer Komponenten.
UEFI ist noch um ein Vielfaches mächtiger als dessen Vorgänger und bringt Treiber für diverse Dateisysteme, Human Interface Devices (HID) wie z.B. Tastaturen und Mäuse und auch für Netzwerkkarten mit. Mit diesen Features eignet sich UEFI hervorragend für Remote-Zugänge mit umfangreichen Funktionen. So kann mittels der vorhandenen Treiber eine akustische Raumüberwachung erfolgen. Zu beachten ist hierbei, dass UEFI nicht nur beim Start des Rechners ausgeführt wird, sondern der sogenannte System Management Mode (SMM), der Bestandteil von UEFI ist, jedes Mal angestoßen wird, sobald ein Prozessorkern den Sleep-State wechselt. Dies kommt bei modernen Prozessoren sehr häufig vor. So lassen sich selbst Live-Linux-Systeme, die Read-Only von CD booten, ausspionieren.
Auch kann UEFI genutzt werden, um das OS per DMA zu manipulieren. So können z.B. Sicherheitsfeatures deaktiviert oder Prozessen mehr Rechte geben werden (privilege escalation).
Ein weiteres Angriffsszenario ist das Abschalten des UEFI Sicherheitsfeatures Secure Boot, welches dafür sorgt, dass nur signierte Bootloader gestartet werden können und einen integralen Bestandteil einiger Sicherheitskonzepte darstellt.
Des Weiteren können BIOS und UEFI für DoS Angriffe genutzt werden, um einzelne Komponenten oder ganze Systeme lahmzulegen.

Kommunikationskanäle:
Netzwerk, Wechseldatenträger und Schall sind mögliche Kommunikationskanäle. Intern kann über den Arbeitsspeicher mit anderen Systemkomponenten kommuniziert werden.

Mögliche Erkennungsmethoden:
Nicht normaler Netzwerkverkehr kann je nach Tarnung potentiell von IDS erkannt werden. Für alle weiteren Angriffsvektoren gibt es im Moment keine Erkennungsmethoden.

Vorfälle / PoC:
Drei Produkte des NSA ANT Katalogs nutzen das BIOS, um Malware, wie oben beschrieben, zu persistieren:

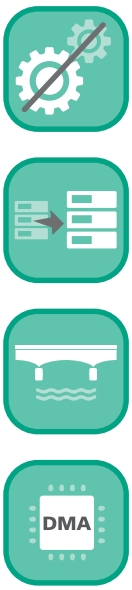
- Deitybounce
- Ironchef

- Swap

Teilweise bieten diese auch Backdoor Funktionalitäten. Im Jahr 2011 wurde mit »Mebromi« eine sehr ähnliche Software entdeckt, die von Kriminellen genutzt wurde (77).
2013 gab es einen PoC namens Dreamboot mit dessen Hilfe auf der Hack-in-the-Box-Conference demonstriert wurde, dass UEFI Rootkits genutzt werden können, um Windows 8 zu manipulieren. Konkret haben die Forscher eine Rechteausweitung und das Umgehen der Windows Authentifizierung gezeigt (78).
Auf der CanSecWest 2015 präsentierten Forscher ihren PoC LightEater, der das UEFI diverser Hersteller befallen kann und den SMM nutzt, um Code unabhängig vom Betriebssystem ausführen zu können (79).
2015 veröffentlichte ein Hacker Programmiertipps für UEFI Backdoors (80). Ebenfalls 2015 wurde bekannt, dass die auf Spionage-Software spezialisierte Firma Hacking Team ein Tool im Einsatz hat, das ähnlich wie Mebromi funktioniert (81).
2017 demonstrierten Forscher einen Erpressungstrojaner, der im UEFI implementiert ist und somit den Rechner bereits beim Bootvorgang sperrt (82).

5.4.2 Management Engine (ME) / System Management Unit (SMU)

PoC



Beschreibung:
Die Intel Management Engine (ME) ist eine Zusatzfunktion auf Intel Mainboard-Chips, die ursprünglich für die Fernwartung gedacht war. ME besitzt einen eigenen Prozessor, einen geschützten Speicherbereich im Hauptspeicher sowie einen direkten Zugang zur Netzwerkkarte. Somit ist ME nicht nur unabhängig von CPU oder einem Betriebssystem lauffähig, sondern kann auch am Betriebssystem vorbei im Netzwerk kommunizieren. Weiterhin unterstützt ME DMA. Die Firmware von ME ist zusammen mit dem BIOS im SPI-Flashchip enthalten und durch Signaturen vor Manipulationen geschützt. ME kann verschiedene Programme ausführen. Am häufigsten kommt die Active Management Technology zum Einsatz, die es Administratoren erlaubt, aus der Ferne Systeminformationen abzurufen oder das System neu zu booten. ME wird auch verwendet, um die Prozessortemperatur zu überwachen und Stromsparfunktionen des Prozessors zu steuern. Außerdem kann ME verwendet werden, um die Integrität des BIOS / UEFI vor der Ausführung zu prüfen. Das AMD Pendant zu ME ist die System Management Unit (SMU).

Angriffsmöglichkeiten:
ME/SMU kann für DMA Angriffe genutzt werden. Gestohlene Daten können am Betriebssystem vorbei direkt über die Netzwerkkarte gesendet werden. Da auch Stromsparfunktionen und Temperaturüberwachung des Prozessors über ME/SMU gesteuert werden, sind auch DoS Angriffe möglich, bei denen z.B. der Prozessor überhitzt wird.

Kommunikationskanäle:
Extern kann über das Netzwerk kommuniziert werden. Intern kann DMA zur Kommunikation mit Software oder anderen Komponenten genutzt werden.

Mögliche Erkennungsmethoden:
Gegen DMA Angriffe gibt es momentan nur diverse akademische Ansätze. Auf dem Markt verfügbar ist keine dieser Techniken.

Vorfälle / PoC:
Ein PoC auf der Blackhat USA 2009 demonstrierte, dass die ME Firmware manipulierbar ist und dass ME genutzt werden kann, um per DMA auf den RAM zuzugreifen (83). 2012 nutzten Forscher diese Erkenntnisse um einen Keylogger mit Netzwerkkommunikation namens DAGGER als PoC zu implementieren (84).
Auf dem 31C3 wurde im Rahmen eines PoCs demonstriert, dass auch die SMU von AMD manipulierbar ist (85).

5.4.3
Erweiterungskarten / Zusatzchips

Beschreibung:
Erweiterungskarten und zusätzliche Chips auf dem Mainboard sind meist über den PCI Express (PCIe) Bus angeschlossen. Weit verbreitet sind Netzwerk-, Grafik- und TV-Karten, sowie USB- und RAID-Controller. Erweiterungskarten und Zusatzchips verwenden oft Option ROMs (siehe 4.3.3.2).

Angriffsmöglichkeiten:
Neben DMA- und Option ROM-Angriffen können gerätespezifische Angriffe eingeleitet werden. So kann man z.B. auf einer Netzwerkkarte ein RAT implementieren und eine Grafikkarte könnte verwendet werden, um das Monitorbild periodisch zu speichern.

Kommunikationskanäle:
Direkte Kommunikationskanäle nach außen sind nur vorhanden, wenn die Karte über externe Anschlüsse verfügt. Netzwerkkarten beispielsweise können direkt über das Netzwerk kommunizieren. Alle Karten können aber auch intern mit anderen Komponenten oder Software per DMA kommunizieren.

Mögliche Erkennungsmethoden:
Derzeit gibt es keine auf dem Markt verfügbaren Erkennungsmethoden für DMA- oder Option ROM-Angriffe. Firmware Rootkits mit Netzwerkzugriff können evtl. per IDS erkannt werden.

Vorfälle / PoC:
Auf der Blackhat 2007 demonstrierte ein PoC, dass Option ROMs auf PCI-Karten genutzt werden können, um periodisch beliebigen Code ausführen zu können. Dazu werden Hooks auf Interupts gesetzt (86).
Ein PoC auf der PacSec 2008 demonstriert eine Remote Shell, die auf einer Netzwerkkarte in Verbindung mit einer Grafikkarte basiert. Dabei kommunizieren Netzwerk- und Grafikkarte direkt über den PCI-Bus, sodass das Betriebssystem außen vor bleibt. Die eigentliche Shell wurde auf der Grafikkarte implementiert, da diese im Gegensatz zur Netzwerkkarte viel eigenen Arbeitsspeicher und Rechenleistung mitbringt (87).
Auf der HITB Amsterdam 2010 zeigten Forscher einen PoC-DMA-Angriff, der demonstrierte, wie sich mit Hilfe einer PCMCIA Karte Windows 7 entsperren lässt (88).
Auf der RAID 2011 wurde im Rahmen eines PoC ein Netzwerkkarten-Rootkit gezeigt. Dieses war in der Lage Tastatureingaben aus dem Keyboard Buffer im Arbeitsspeicher zu lesen und anschließend über einen Covert Channel an ein anderes Gerät im Netzwerk zu übertragen (89).
Auf der Eurosec 2013 wurde ein Keylogger basierend auf einer Grafikkarte gezeigt (90). 2015 wurde der Source Code eines Rootkits und Keyloggers basierend auf dem PoC von der Eurosec 2013 veröffentlicht (91).

5.4.4
Datenspeicher

Beschreibung:
Datenspeicher decken sowohl interne Festplatten als auch Wechseldatenträger ab. Die Anschlüsse sind dabei sehr vielfältig (SATA, PCIe, SCSI, Thunderbolt, USB, Firewire usw.) Die meisten dieser Anschlussarten bieten DMA-Fähigkeiten.

Angriffsmöglichkeiten:
Neben DMA-Angriffen können bei Datenspeichern Daten manipuliert und abgegriffen werden. Das Abgreifen kann über einen Schattenspeicher geschehen, der für den Benutzer unsichtbar ist. Diese Daten im Schattenspeicher werden nicht gelöscht, wenn die eigentlichen Daten überschrieben werden. Des Weiteren ist es möglich Software Rootkits zu persistieren, indem man sie entweder vor Anfragen versteckt oder jedes Mal neu installiert, wenn sie gelöscht werden.
Eine weitere Angriffsmöglichkeit bezieht sich auf selbstverschlüsselnden Medien. Hier kann durch Manipulation der Firmware die Verschlüsselung abgeschaltet, abgeschwächt oder geknackt werden.

Kommunikationskanäle:
In der Regel ist DMA der einzige Kommunikationskanal. Bei Wechseldatenträgern ist der Datenträger selbst natürlich ebenfalls ein möglicher Kommunikationskanal.

Mögliche Erkennungsmethoden:
Momentan sind keine Erkennungsmethoden verfügbar.

Vorfälle / PoC:
Im NSA ANT Katalog befindet sich ein Firmware Rookit für Festplatten namens Iratemonk, das zur Persistierung von Malware benutzt wird.
Ein PoC auf der OHM2013 zeigt, dass Festplatten-Firmware manipuliert werden kann. Im PoC wurden Daten von der Festplatte manipuliert, bevor sie über den SATA-Bus ans System übertragen wurden (92).
Auf dem 30C3 wurde demonstriert, dass SD-Karten einen Micro Controller enthalten, dessen Software austauschbar ist (93).
Auf der Blackhat USA 2016 demonstrierte ein Forscher, wie man durch eine Firmware-Manipulation die Verschlüsselung einer Festplatte mit verbautem PIN-Pad knacken kann. Dabei wird nicht die Verschlüsselung ausgehebelt, sondern in der Firmware ein Bruteforce-Angriff implementiert, der innerhalb kurzer Zeit alle PIN Kombinationen durchgeht (94).

5.4.5
USB-Geräte

Beschreibung:
Geräte für den Universal Serial Bus (USB) gibt es für verschiedene Anwendungsfälle, die durch verschiedene Geräteklassen repräsentiert werden. Am verbreitetsten sind Human Interface Devices (HID) wie Tastatur und Maus sowie Speichergeräte wie USB-Stick und Festplatte. USB-Geräte können auch mehrere Geräteklassen in sich vereinen oder ihre Geräteklasse während des Betriebs wechseln.
USB funktioniert wie ein klassischer Bus, bei dem jedes Gerät alle Nachrichten auf dem Bus lesen kann. USB bringt zudem keinerlei Sicherheitsfunktionen mit, die die Authentizität von Nachrichten prüfen. Dementsprechend kann jedes Gerät sich als jedes andere Gerät am Bus ausgeben.
Die USB-Hostcontroller-Standards sehen DMA-Features vor, sodass USB-Geräte über den Controller DMA indirekt nutzen können.

Angriffsmöglichkeiten:
Am bekanntesten sind Angriffe, bei denen sich beliebige USB-Geräte als Tastatur ausgeben und so beispielsweise Programme auf dem Computer starten.
Ein beliebiges USB-Gerät kann sich als Netzwerkkarte ausgeben und somit einen MitM Angriff durchführen. Es ist auch möglich ein beliebiges USB-Gerät zum Sniffen auf dem USB-Port zu benutzen. So könnte man z.B. einen Keylogger implementieren, der allerdings nur funktioniert, wenn die Tastatur am selben USB-Controller angeschlossen. Auch das Abgreifen von Daten, die zu oder von einer USB-Festplatte kommen, ist denkbar.
Da DMA nur über den Host-Controller möglich ist, sind Angriffe über DMA schwierig, aber nicht auszuschließen.

Kommunikationskanäle:
Alle USB-Geräte haben den USB-Bus als Kommunikationskanal. Ansonsten gibt es gerätespezifische Kanäle. So haben Speichergeräte sich selbst, Netzwerkadapter Netzwerke und Multimedia-Geräte Schall als zusätzlichen Kommunikationskanal. 2016 demonstrierten Forscher, dass auch ein USB-Kabel zwischen Gerät und Host als Antenne zum Übertragen von Daten per Funk dienen kann (95).

Mögliche Erkennungsmethoden:
Geräte, die sich als andere Geräte ausgeben, können potentiell mit Bordmitteln des OS erkannt oder sogar unterbunden werden. So kann man z.B. in Windows per Gruppenrichtlinie ganze Geräteklassen verbieten oder eine Software nutzen, die zusätzliche USB-Tastaturen blockiert. Des Weiteren sind Eingaben einer emulierten Tastatur auf dem Bildschirm sichtbar.
Angriffe auf den USB-Bus (sniffen oder Nachrichten fälschen) können derweil nicht erkannt werden.

Vorfälle / PoC:
Bei der CanSec West 2005 wurde ein PoC eines DMA Angriffs vorgestellt, bei dem ein über USB verbundenes Handy genutzt wurde, um eine Shell-Skript in den Speicher des Hostsystems zu kopieren und zu starten (96).
Auf der Blackhat USA 2014 zeigten Forscher, dass sie die Firmware beliebiger USB-Sticks so manipulieren können, dass sie sich als HID oder Netzwerkgerät ausgeben. Auf diese Weise implementierten sie einen Dropper und einen Netzwerk-Proxy für MitM Angriffe (97). Wenige Monate später wurden Anleitung und Tools veröffentlicht, die jeden technisch versierten Nutzer in die Lage versetzen, böse USB-Geräte zu erstellen (98).

5.4.6
Thunderbolt-Kabel und -Geräte

PoC

Beschreibung:
Thunderbolt ist eine vornehmlich von Intel entwickelte Schnittstelle für externe Geräte. Technisch werden über die Thunderbolt Schnittstelle verschiedene Übertragungsprotokolle angeboten: PCIe, DiplayPort und seit Thunderbolt 3 auch USB3.1. Thunderbolt unterstützt dementsprechend DMA und, aufgrund der PCIe Kompatibilität, auch Option ROMs. Thunderbolt verfügt zudem über aktive Stecker mit mehreren Micro Controllern. Diese sind theoretisch selbst in der Lage böse Funktionalitäten zu implementieren.

Angriffsmöglichkeiten:
Thunderbolt kann für DMA- und Option ROM-Angriffe verwendet werden.

Mögliche Erkennungsmethoden:
Derzeit sind keine Erkennungstechniken gegen DMA- und Option ROM-Angriffe auf dem Markt verfügbar.

Vorfälle / PoC:
2014 wurde mit Thunderstrike eine Manipulation der Firmware eines Thunderbolt-Netzwerkadapters gezeigt, der über einen Option ROM-Angriff in der Lage ist, das EFI eines MacBooks auszutauschen. Dabei wurde die Signaturprüfung beim EFI-Update umgangen (99). 2015 wurde dieser PoC zu einem Wurm weiterentwickelt, der sich selbst repliziert (100).
Des Weiteren steht mit der Inception Software (101) ein Tool zu Verfügung, mit dem man mittels Thunderbolt von einem anderen PC oder möglicherweise auch von einem Embedded Device mit Linux System DMA Angriffe durchführen kann.
2016 wurde demonstriert, wie man über Thunderbolt das Anmeldepasswort eines Mac OS Benutzers auslesen kann, sofern die Festplattenverschlüsselung aktiviert ist (102).

5.4.7
IEEE 1394-Geräte (FireWire / i.Link)

Beschreibung:
IEEE 1394 ist eine Schnittstelle für externe Geräte, die ähnlich wie USB funktioniert. IEEE 1394 ist am Computer über das Open Host Controller Interface (OHCI) angebunden. Dieses sieht einen direkten Zugriff auf den Arbeitsspeicher vor, der allerdings nur 32Bit adressieren kann. Dadurch ist man mit FireWire in der Lage, nur die ersten 4GB RAM auszulesen und zu beschreiben.

Angriffsmöglichkeiten:
DMA-Angriffe auf die ersten 4GB Speicher sind möglich.

Mögliche Erkennungsmethoden:
Derzeit sind keine Erkennungsmethoden gegen DMA-Angriffe auf dem Markt verfügbar.

Vorfälle / PoC:
2005 wurde auf der CanSecWest ein PoC präsentiert, in welchem ein über Firewire angeschlossener iPod den Arbeitsspeicher eines PCs ausliest (103).
Auf der Ruxcon 2006 wurde demonstriert, dass über Firewire gezielt Passwörter gestohlen werden können (104). Ein Jahr später wurde auf der DIMVA ein ähnlicher PoC für SSL-Keys gezeigt (105).
Des Weiteren steht mit der Inception Software (101) ein Tool zu Verfügung, mit dem man mittels Firewire von einem anderen PC oder möglicherweise auch von einem Embedded Device mit Linux System DMA Angriffe durchführen kann.

5.5 Fazit

Firmware-Trojaner sind leicht zu implementieren und sehr einfach zu verbreiten. Zudem bieten sie weitreichende Funktionsmöglichkeiten.
Die proaktiven Schutzmechanismen gegen Firmware-Manipulationen sind sehr verbreitet und sinnvoll, um Manipulationen zu erschweren. Allerdings haben diverse PoCs gezeigt, dass auch vermeintlich sichere Verfahren, wie z.B. Signaturen, die bei jedem Systemstart geprüft werden, umgangen werden können. Ein bekanntes Beispiel ist Thunderstrike. Außerdem ist in den meisten Fällen weder vom Einkäufer noch vom Nutzer feststellbar, ob und welche proaktiven Sicherheitsmaßnahmen von den Herstellern zum Schutz der Firmware getroffen wurden. Auch Exploits, die zur Laufzeit des Gerätes ausgenutzt werden, werden durch die proaktiven Maßnahmen nicht geschützt. Erschwerend hinzu kommt hier die in 5.1.2 beschriebene Firmware-Update-Problematik.
Reaktive Sicherheitsmaßnamen sind bei Firmware wenig verbreitet. Lediglich IDSs kommen in Firmennetzwerken häufig zum Einsatz und können ungewöhnliches Verhalten von kompromittierten Geräten auf Netzwerkebene erkennen. Dies deckt aber bei weitem nicht alle Angriffsszenarien ab. Dementsprechend ist die Wahrscheinlichkeit einen Firmware-Trojaner zu entdecken sehr gering.
Zusammenfassend muss man die Firmware-Trojaner als die größte und akuteste Bedrohung unter den Hardware-Trojanern ansehen. Vor allem die mittlerweile weit verbreiteten Botnetze auf Embedded Devices zeigen, dass Firmware-Trojaner bereits im Malware-Massenmarkt angekommen sind.

6
Malicious Hardware

Schon seit dem zweiten Weltkrieg gehören versteckte Abhörgeräte zum Repertoire der meisten Geheimdienste. Malicious Hardware ist daher die vermutlich älteste Form der Hardware-Trojaner. Dieser Bericht beschränkt sich allerdings auf Malicious Hardware, die in IT-relevanten Geräten verbaut ist.
Dieses Kapitel beginnt mit der Erörterung von Infektionswegen und Schutzmechanismen. Anschließend werden Geräteklassen vorgestellt und in einheitlicher Form ausgewertet. Insbesondere wird auf reale Vorfälle und bereits implementierte PoCs eingegangen. Abschließend folgt ein Gesamtfazit zu Malicious Hardware.

6.1
Infektion

Die Verbreitung von Malicious Hardware kann nicht Remote erfolgen. Ansonsten sind grundsätzlich alle Infektionswege aus 4.2 möglich.

6.2
Schutz

Die Schutzmöglichkeiten hängen sehr stark von der Qualität der Malicious Hardware ab. In den folgenden Abschnitten werden kurz die gängigen Verfahren erläutert.

6.2.1
Sichtprüfung

Bei einer Sichtprüfung wird nach Geräten oder Bauteilen gesucht, die nicht plausibel erscheinen. Z.B. ist ein Gerät, das zwischen Computer und Tastatur steckt, in den wenigstens Fällen legitim. Oft wird Malicious Hardware in Geräten verbaut, sodass ein Öffnen der Geräte zur Sichtprüfung nötig ist. Hierbei sind legitime Bauteile und Malicious Hardware teilweise nur sehr schwer zu unterscheiden. Ein legitimes Referenzgerät (Golden Sample) kann zum Vergleich genutzt werden. Trotzdem können Sichtprüfungen keinen umfassenden Schutz bieten.

6.2.2
Durchleuchten

Durchleuchten ist eine erweiterte Sichtprüfung mit technischer Unterstützung beispielsweise durch Röntgengeräte. Durchleuchten ist nötig, wenn Geräte nicht geöffnet werden können oder sollen. Auch hier gilt, dass eine Differenzierung von legitimen Bauteilen und Malicious Hardware oft nur schwer möglich ist.

6.2.3
Emissionsprüfung

Malicious Hardware erzeugt meistens Seiteneffekte, die von außen messbar sind. Insbesondere Kommunikationskanäle sind oft erkennbar. Netzwerk- oder Bus-Aktivitäten lassen sich hierbei potentiell von IDS erkennen. Funkkanäle lassen sich ggf. auf anderen Wegen aufspüren. Emissionen können aber auch in anderer Form auftreten wie beispielsweise ungewöhnlichen Wärmesignaturen oder Geräusche.

6.3 Geräteklassen

In der Folge werden diverse Malicious Hardware-Geräteklassen genauer betrachtet.

6.3.1 Keylogger

Beschreibung:
Keylogger sind Geräte, die Tastatureingaben mitschneiden. Es gibt diverse Ausführungen. Die einfachsten Geräte werden zwischen Computer und Tastatur gesteckt. Aufwendigere Geräte sind in die Tastatur eingebaut oder greifen per Funk Tastureingaben von Funktastaturen ab.

Angriffsmöglichkeiten:
Keylogger können dazu benutzt werden, um Zugangsdaten zu stehlen oder per Tastatur eingegebene Nachrichten mitzuschneiden.

Kommunikationskanäle:
In der Regel müssen die Geräte vor Ort ausgelesen werden. Es gibt auch Geräte, die die Eingaben per Funk übertragen. Dazu muss allerdings ein Funkempfänger in Funkreichweite installiert werden.

Mögliche Erkennungsmethoden:
Günstige Geräte können per Sichtprüfung erkannt werden. Aufwändigere Geräte, die z.B. direkt in der Tastatur verbaut werden, sind nur durch Öffnen oder Durchleuchten der Geräte zu erkennen. Aber auch dann kann es schwierig sein, die »böse« von der restlichen legitimen Hardware im Gerät zu unterscheiden.

Vorfälle / PoC:
Es gibt diverse Firmen, die unterschiedlich gut getarnte Keylogger kommerziell vermarkten. Des Weiteren gibt es im Internet diverse Anleitung, wie man teilweise sehr gut getarnte Keylogger selber bauen kann (106).
Auch im NSA ANT Katalog befindet sich ein gut getarnter Keylogger namens Surlyspawn.
Der Einsatz solcher Keylogger ist vielfach dokumentiert. Exemplarisch sei hier ein Vorfall aus dem Jahr 2013 erwähnt, bei dem Kriminelle Hardware Keylogger, der Eingaben per Funk überträgt, in einer Bank installiert haben (2).

6.3.2
Display Cloner

Beschreibung:
Display Cloner beschreibt Geräte, die in der Lage sind das Bild eines Monitors zu speichern oder direkt an einen Angreifer zu übertragen.

Angriffsmöglichkeiten:
Der Angreifer sieht den Bildschirminhalt des Opfers und kann so ggf. Zugangsdaten oder vertrauliche Dokumente sehen.

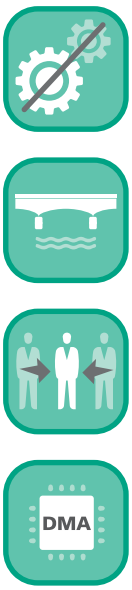
Kommunikationskanäle:
Display Cloner müssen entweder vor Ort ausgelesen werden oder übertragen das Bild per Funk.

Mögliche Erkennungsmethoden:
Erkennungsmethoden sind stark abhängig von der Tarnung des Gerätes. Eventuell lassen sie sich beim Durchleuchten oder, sofern vorhanden, anhand des Funksignals erkennen.

Vorfälle / PoC:
Der Display Cloner Ragemaster aus dem NSA ANT Katalog ist ein kleines Gerät, das in einem Monitorkabel versteckt wird. Es überträgt den Display-Inhalt per Funk.
Im Jahr 2013 nutzten Kriminelle einen Display-Cloner mit Funkkanal bei einem versuchten Cyber-Bankraub (2).

6.3.3
Ethernet / USB Injection und Extraction

Beschreibung:
Für Ethernet / USB Injection und Extraction werden bösartige Geräte in Netzwerk- bzw. USB-Steckern, Buchsen oder Kabeln verbaut. Diese sind in der Folge in der Lage den Datenverkehr mitzuschneiden bzw. auszuleiten oder zu manipulieren. Da diese Geräte in der Regel sehr klein sind, steht nur wenig Rechenleistung und Speicher zur Verfügung. Daher sind diese Geräte in ihren Möglichkeiten beschränkt.



Angriffsmöglichkeiten:
Es können Daten abgefangen und manipuliert werden. Auch ein Kill-Switch wäre möglich, der die Verbindung unter festgelegten Bedingungen beendet. Mit einer über Funk angebundenen Gegenstelle lässt sich auch ein Brückenkopf in Netze aufbauen, die nicht mit anderen Netzen verbunden sind. Auch gezielte Angriffe per USB, wie in Abschnitt 5.4.5 beschrieben, sind möglich.

Kommunikationskanäle:
Das Netzwerk bzw. Bus selbst und ggf. Funk sind mögliche Kommunikationskanäle.

Mögliche Erkennungsmethoden:
Ein Durchleuchten der Geräte kann zur Entdeckung führen.

Vorfälle / PoC:
Der NSA ANT Katalog enthält diverse Geräte zu diesem Zweck. Firewalk ist ein Gerät, das in Netzwerk- oder USB-Steckern verbaut wird und in der Lage ist Daten zu extrahieren oder zu manipulieren. Firewalk wird über einen Funkkanal durch ein Gerät namens Howlermonkey gesteuert. Die Produkte Cottonmouth I-III sind auf USB spezialisiert und haben einen ähnlichen Funktionsumfang wie Firewalk. Zusätzlich gibt der ANT Katalog an, dass über diese Geräte gezielt Schadsoftware auf den angeschlossenen Computern installiert werden kann.

6.3.4
USB-Geräte

IN USE

Es gibt Computer im USB-Stick-Format, die äußerlich nicht von USB-Sticks zu unterscheiden sind. Beispielhaft seien hier USB Rubber Ducky (107) und USB Armory (108) erwähnt. Die Möglichkeiten dieser Geräte sind äquivalent zu ihren Firmware-Trojaner Pendants (siehe Abschnitt 5.4.5).
Des Weiteren gibt es einen kommerziell vermarkteten USB-Killer (109), der nach Anschluss an einen Computer, eine Überspannung am USB-Port erzeugt und damit die Hardware des Computers beschädigt. Ob dadurch allerdings auch die Festplatten inklusive der gespeicherten Daten zerstört werden, ist fragwürdig.

Angriffsmöglichkeiten:
Neben der Beschädigung der Hardware des Hosts, sind alle Angriffe wie beim Firmware-Trojaner Pendant möglich (siehe Abschnitt 5.4.5).

Kommunikationskanäle:
Der Bus selbst und ggf. Funk sind mögliche Kommunikationskanäle.

Mögliche Erkennungsmethoden:
Ein Durchleuchten der Geräte kann zur Entdeckung führen.

Vorfälle / PoC:
2016 wurde demonstriert, dass ein USB-Armory, der sich als Ethernet-Adapter ausgibt, genutzt werden kann, um Windows Benutzernamen und Passwörter zu klauen (110). Dabei wird ausgenutzt, dass Windows sich automatisch versucht an einer Domäne anzumelden, sobald ein Netzwerk-Gerät aktiviert wird. Der Angriff funktioniert auch, wenn der Bildschirm gesperrt ist.

6.4 Fazit

Die Detektionsmöglichkeiten von Malicious Hardware sind stark von den Möglichkeiten des Angreifers abhängig. In manchen Fällen lassen sie sich leicht durch Sichtprüfung erkennen. In anderen Fällen kann man sie kaum finden, da man sie nicht von den »normalen« Bestandteilen der Hardware unterscheiden kann. Die Geräte können nicht Remote installiert werden und erfüllen in der Regel nur einen festgelegten Zweck. Zudem muss man zur Kommunikation mit den Geräten entweder vor Ort oder zumindest in der Nähe sein. Hinzu kommt, dass diese Geräte teilweise sehr aufwendig und teuer in der Produktion sind. So kosten beispielsweise 50 Einheiten von Cottonmouth I mehr als 1 Mio US-Dollar.
Wegen der vergleichsweise hohen Kosten und der eingeschränkten Flexibilität dieser Geräte sind sie für die meisten Angreifer weitaus weniger lukrativ als die günstigen und flexiblen Firmware-Trojaner. Es ist davon auszugehen, dass die Einsätze von Malicious Hardware in den nächsten Jahren zurückgehen werden.

7
Integrated Circuit Trojaner

IC-Trojaner bestehen aus einer festgelegten Schaltung und sind daher in ihrem Funktionsumfang sehr starr und nicht nachträglich veränderbar. Meistens ist nur eine »böse« Funktion implementiert, die in der Regel erst aktiviert wird, wenn der sogenannte Trigger eintritt. Vor dem Trigger funktioniert der Chip wie nicht kompromittierte Gegenstücke.

Das weitere Kapitel ist wie folgt gegliedert. Zunächst werden die Infektionswege und möglichen Schutzmechanismen erläutert. Daraufhin werden mögliche Trigger diskutiert und anschließend die verschiedenen Arten (Funktionen) von IC-Trojanern vorgestellt. Das Kapitel schließt mit einem Fazit.

7.1
Infektion

Die Infektion eines ICs ist nur während der Design oder Produktionsphase möglich. Der Austausch legitimer durch manipulierte ICs ist allerdings auch während des Transports oder vor Ort denkbar.

7.2
Schutz

Es gibt diverse Ansätze, um Infektionen von ICs zu erkennen. Viele dieser Ansätze basieren auf dem Vergleich mit einem Golden Sample, das als nicht infiziert angesehen wird. Die Existenz eines nicht infizierten Exemplars kann in vielen Fällen allerdings nicht vorausgesetzt werden. In der Folge werden die wichtigsten Ansätze beschrieben.

7.2.1
Funktionstests (Logic Testing)

Ursprünglich wurde bei Funktionstests kontrolliert, ob bei validen Eingangssignalen das der Spezifikation entsprechende Ausgangssignal erzeugt wird. IC-Trojaner werden aber oft nur bei selten vorkommenden oder auch bei in der Spezifikation nicht vorgesehenen Eingangssignalen aktiv. Daher gibt es diverse Ansätze ein Fuzzing der Eingangssignale durchzuführen und die Ausgangssignale mit einem Golden Sample zu vergleichen. Funktionstests können keine absolute Sicherheit bieten, da nicht jedes erdenkliche Eingangssignal bzw. jede Folge von Eingangssignalen getestet werden kann.

7.2.2
Strukturvergleich (Destructive Reverse Engineering)

Beim Strukturvergleich wird der Chip geöffnet und mit Hilfe von Elektronenmikroskopen oder ähnlichen Geräten mit einem Golden Sample verglichen. Bei diesem Ansatz gibt es mehrere Probleme. Zum einen werden die Strukturen immer kleiner und die Schaltungen immer komplexer, sodass das Auffinden von Unterschieden zum Golden Sample beliebig schwer wird. Zum anderen ist der Strukturvergleich destruktiv, sodass ein Test nur stichprobenartig durchgeführt werden kann. Dieses Verfahren kann dementsprechend keine absolute Sicherheit geben.

7.2.3
Side Channel Analysis

Bei diesem Ansatz werden ICs mit Golden Samples verglichen. Es werden diverse Signal-Kombinationen an den Chip angelegt, um anschließend zu kontrollieren, ob die Seiteneffekte identisch sind. Seiteneffekte können hierbei verschiedener Art sein. Gängig sind beispielsweise Stromverbrauch oder Delays. Viele dieser Ansätze funktionieren allerdings nur, wenn die Trojaner komplex sind und viele Gatter benötigen. Benötigen die Trojaner nur wenige Gatter, so sind die Seiteneffekte in den meisten Fällen kaum zu erkennen.

7.3 Trigger

Es gibt IC-Trojaner, die permanent aktiv sind und keine speziellen Trigger brauchen. Für alle anderen kommen die folgenden Trigger in Frage.

7.3.1 Sensorische Aktivierung

Sensoren werden genutzt, um unter bestimmten Voraussetzungen, wie z.B. das Erreichen einer bestimmten Temperatur oder einer Position (GPS), das Ereignis auszulösen.

7.3.2 Software-/Daten-Aktivierung

Durch Einfluss einer Software oder eines speziellen Datenpaketes werden die Eingänge auf eine selten vorkommende Art belegt, sodass das Ereignis ausgelöst wird. In diesem Zusammenhang ist es insbesondere möglich, dass ein Netzwerk-Paket, das in Hardware verarbeitet wird, zu einer Auslösung führt. Auf diese Weise lassen sich IC-Trojaner auch aus der Ferne auslösen.

7.3.3 Counter-Aktivierung

Wenn ein Counter einen bestimmten Wert erreicht, wird der IC-Trojaner aktiviert. Auf diese Weise lassen sich Trigger implementieren, die nach einer gewissen Zeit auslösen.

7.4 IC-Trojaner Arten (Funktionen)

IC-Trojaner lassen sich in drei generische Funktionsarten unterteilen, die in den folgenden Abschnitten beschrieben werden. Die Abschnitte sind jeweils unterteilt in eine kurze Beschreibung der Funktionsweise und realen Vorfällen bzw. PoCs.

7.4.1
Kill Switch

Beschreibung:
Ein Kill Switch ist ein Angriff auf die Verfügbarkeit, bei dem der Chip permanent oder temporär unbrauchbar gemacht wird.

Vorfälle / PoC:
2007 griffen israelische Luftstreitkräfte eine Nuklearanlage in Syrien an, wobei im Vorfeld das syrische Radar unbrauchbar gemacht wurde. Unbestätigten Quellen zufolge handelte es sich um einen Kill Switch, der in Mikrochips der Radaranlagen verbaut war und von den Israelis getriggert wurde (111).
Laut eines Mitarbeiters des US Verteidigungsministeriums verbaut ein europäischer Chip-Hersteller Kill Switches in seinen Mikrocontrollern, die aus der Ferne ausgelöst werden können (111). 2008 wurden bei einem von der New York University (NYU) organisierten Wettbewerb zwei PoCs demonstriert, die Crypto-Chips zerstören (112).

7.4.2
Ändern der Funktionalität

Beschreibung:
Das Ändern der Funktionalität wird genutzt, um erzeugte Ausgangsdaten / -signale zu manipulieren. Die Haupteinsatzzwecke sind das Schwächen oder Umgehen von kryptografischen Verfahren und das Umgehen von Sicherheitsfunktionen, was zu einer Rechteausweitung führt. Beide Einsatzgebiete können sowohl die Integrität als auch die Geheimhaltung von Daten gefährden.
Exemplarisch seien hier drei Szenarien beschrieben:

1. Es werden stets vom Angreifer vorgegebene kryptografische Schlüssel »generiert«. Hierbei wird vermutlich ein ganzer Pool an Schlüsseln vordefiniert, damit der Schlüssel nicht immer gleich ist.
2. Die Zufallszahlengeneratoren werden manipuliert, sodass sie entweder eine feste Abfolge von Zahlen generieren oder nicht gleichverteilte Zufallszahlen erzeugt werden. Somit wird eine Verschlüsselung basierend auf dem Zufallszahlengenerator erheblich geschwächt.
3. Code, der im Ring 3 eines Prozessors läuft, kann auf Speicherbereiche zugreifen, die eigentlich nur von Code im Ring 0 genutzt werden kann. Dies wird im Zusammenhang mit IC-Trojanern oft als Backdoor bezeichnet.

Vorfälle / PoC:
2008 gab es eine von der NYU organisierten Wettbewerb, der sich u.A. mit Hardware-Trojanern in Crypto-Devices befasste. In diesem Zusammenhang wurde ein PoC gezeigt, der bestimmte Wörter in Texten durch andere ersetzt (112).
2008 wurden auf der Usenix ein PoC gezeigt, der den Zugriff auf zugriffsbeschränkten Speicher durch nicht autorisierte Anwendungen erlaubt (113).
Auf der Usenix 2008 wurde ein PoC veröffentlicht, der einen »Shadow Mode« in einem Prozessor implementiert. In diesem »Shadow Mode« kann Code abseits des OS ausgeführt werden (113).

7.4.3
Daten Exfiltration (Side Channels)

Beschreibung:
Side Channels sind ein Angriff auf die Geheimhaltung. Sie werden genutzt, um vertrauliche Information, wie z.B. einen kryptografischen Schlüssel, zu exfiltrieren. Der Side Channel muss nicht zwingend ein ausgeleiteter Daten-Port sein, sondern kann auch als Wärme-, Stromverbrauchs- oder Zeitsignaturen implementiert werden. Side Channels kamen in der Vergangenheit oft durch Unachtsamkeit oder Unwissenheit der Chip-Entwickler in Produkte. Es ist aber durchaus denkbar, dass Side Channels gezielt in ICs eingebaut werden.

Vorfälle / PoC:
Bereits seit Mitte der 90er Jahre gibt es diverse Veröffentlichungen zu entdeckten Side Channels in Crypto Hardware (114), die allerdings vermutlich nicht absichtlich eingebaut wurden. 2008 wurde ein PoC veröffentlicht, der über den Stromverbrauch Informationen über AES-Schlüssel liefert (115).
Ebenfalls 2008 wurden im Rahmen eines von der NYU ausgerichteten Wettbewerbs fünf PoCs veröffentlicht, die kryptografische Schlüssel über diverse Kanäle ausleiten (112).
2013 wurde ein PoC präsentiert, der AES-Schlüssel über Funk ausleitet (116).

7.5 Fazit

IC-Trojaner setzen sowohl ein großes technisches Wissen aus diversen Kategorien als auch sehr teure Hardware voraus. Außerdem haben diese Trojaner stets sehr spezielle Anwendungsfälle und taugen kaum für komplexe Angriffe. Andererseits sind sie nur sehr schwer auffindbar und in der Praxis oft kaum von ungewollten »Bugs« zu unterscheiden.
Insgesamt gibt es nur wenige potentielle Angreifer, die technisch und finanziell in der Lage sind IC-Trojaner zu erstellen und einzuschleusen. Jedoch werden auch diese potentiellen Angreifer IC-Trojaner aufgrund des meist geringen Kosten-/Nutzenfaktors nur in Ausnahmefällen einsetzen.

8
Zusammenfassung

Hardware-Trojaner sind Realität und werden bereits seit mehreren Jahren von Geheimdiensten und Kriminellen eingesetzt. Besonders lukrativ für diese beiden Gruppen sind sie, da sie in der Regel nur schwer aufzuspüren und obendrein wirksame Schutzmechanismen in vielen Fällen nicht verfügbar sind.
Der gebräuchliche Begriff Hardware-Trojaner beschreibt dabei eine Gruppe von drei Trojaner-Arten: Firmware-Trojaner, Malicious Hardware und IC-Trojaner.
Malicous Hardware lässt sich nicht Remote verbreiten und die Versteckmöglichkeiten hängen sehr stark von den finanziellen Mitteln des Angreifers ab. Ausgefeilte Geräte, wie sie von Geheimdiensten eingesetzt werden sind, extrem teuer. Günstige Geräte lassen sich allerdings von jedermann legal erwerben, sind aber meist sehr auffällig. Obendrein ist Malicious Hardware im Funktionsumfang relativ unflexibel.
IC-Trojaner sind in der Entwicklung und Produktion extrem teuer und vom Funktionsumfang meist auf wenige Funktionen beschränkt. Andererseits sind sie mit heutigen Mittel kaum aufspürbar und von unabsichtlichen Bugs schwer zu unterscheiden. Alles in allem sind IC-Trojaner im Moment nur für Geheimdienste erschwinglich und werden vermutlich auch von diesen nur in Ausnahmefällen eingesetzt.
Insgesamt scheinen Firmware-Trojaner die größte Bedrohung darzustellen. Diese sind sehr flexibel sowohl was die Infektionsmöglichkeiten, als auch den Funktionsumfang angeht. Dabei sind sie günstig und relativ leicht zu implementieren. Zusätzlich sind sie oft mit heutigen Mitteln nur schwer aufzuspüren. Zudem sind insbesondere die Embedded-Device-Firmware-Trojaner bereits heute weit verbreitet und werden intensiv genutzt.

9 Abkürzungen

ACL	Access Control List
BIOS	Basic Input Output System
C3	Chaos Communication Congress
CCS	Conference on Computer and Communications Security
DAB	Digital Audio Broadcast
DDS	Data Distribution Service
DDoS	Distributed Denial-of-Service
DHCP	Dynamic Host Configuration Protocol
DIMVA	Detection of Intrusion and Malware, and Vulnerability Assessment (Conference)
DMA	Direct Memory Access
DoS	Denial-of-Service
DVB	Digital Video Broadcasting
ECU	Electronic Control Unit
HITB	Hack in the Box (Conference)
HMI	Human Machine Interface
IC	Integrated Circuit
IDS	Intrusion Detection System
IOMMU	Input / Output Memory Management Unit
IoT	Internet of Things
IT	Informationstechnik
ME	Management Engine
MitM	Man in the Middle
NDSS	Network & Distributed System Security Symposium
NFC	Near Field Communication
NSA	National Security Agency
NYU	New York University
OS	Betriebssystem (engl.: Operating System)
PCI	Peripheral Component Interconnect
PCIe	PCI Express
PLC	Programmable Logic Controller
PoC	Proof of Concept
PoS	Point of Sale (Bezahlterminals im Einzelhandel)
RAID	Research in Attacks, Intrusion and Defenses (Conference)
RAT	Remote Access Tool
ROM	Read Only Memory
SMU	System Management Unit
TPM	Trusted Platform Module
UEFI	Unified Extensible Firmware Interface
USB	Universal Serial Bus

10 Literaturverzeichnis

1. **Greenberg, Andy.** Hackers Remotely Kill a Jeep on the Highway. *Wired.* [Online] 21. Juli 2015. [Zitat vom: 21. Juli 2015.] http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/?mbid=social_twitter.
2. **Knocke, Felix.** Versuchter Cyber-Bankraub: Kriminelle installieren Hardware-Trojaner in Bank. *Spiegel Online.* [Online] 16. September 2013. [Zitat vom: 26. Juni 2015.] http://www.spiegel.de/netzwelt/web/cyber-bankraub-kriminelle-installieren-hardware-trojaner-in-bank-a-922409.html.
3. **Krebs, Brian.** KrebsOnSecurity Hit With Record DDoS. *Krebs on Security.* [Online] 21.. September 2016. [Zitat vom: 9.. November 2016.] https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/.
4. **Bhunia, Swarup, et al., et al.** Hardware Trojan Attacks: Threat Analysis and Countermeasures. *Proceedings of the IEEE, Volume: 102.* 15. Juli 2014, S. 1229-1247.
5. **Schirmacher, Dennis.** Lenovos Service Engine: BIOS-Rootkit direkt vom Hersteller. *Heise Security.* [Online] 13. August 2015. [Zitat vom: 14. August 2015.] http://www.heise.de/newsticker/meldung/Lenovos-Service-Engine-BIOS-Rootkit-direkt-vom-Hersteller-2778547.html.
6. **Schmidt, Jürgen.** Mysteriöse Router-Backdoor: Viele tausend Router in Deutschland haben eine Hintertür - jetzt testen! *Heise Security.* [Online] 10. Januar 2014. [Zitat vom: 26. Juni 2015.] http://www.heise.de/security/meldung/Mysterioese-Router-Backdoor-Viele-tausend-Router-in-Deutschland-haben-eine-Hintertuer-jetzt-testen-2080913.html. http://www.heise.de/security/meldung/Mysterioese-Backdoor-in-diversen-Router-Modellen-2074394.html.
7. **Eikenberg, Ronald.** E-Plus verschickt Base-Smartphones mit Virus. *heise Security.* [Online] 23. Oktober 2013. [Zitat vom: 26. Juni 2015.] http://www.heise.de/security/meldung/E-Plus-verschickt-Base-Smartphones-mit-Virus-1984119.html.
8. **Holland, Martin.** NSA manipuliert per Post versandte US-Netzwerktechnik. *Heise Online.* [Online] 13. Mai 2014. [Zitat vom: 26. Juni 2015.] http://www.heise.de/newsticker/meldung/NSA-manipuliert-per-Post-versandte-US-Netzwerktechnik-2187858.html.
9. **Martyn, Darren und Eikenberg, Ronald.** Aufstand der Router - Hinter den Kulissen eines Router-Botnetz. *c't 21/13.* 21. September 2013, S. 46f.
10. **Security Research Labs.** Turning USB peripherals into BadUSB. *SrLabs.* [Online] 2014. [Zitat vom: 30. Juni 2015.] https://srlabs.de/badusb/.
11. **Snowden, Edward.** *Bruce Schneier and Edward Snowden @ Harvard Data Privacy Symposium.* [Befragte Person] Bruce Schneier. 23. Januar 2015.
12. **Fraunhofer FKIE.** Computer können unerkannt über Schall kommunizieren. *FKIE Presseinformationen.* [Online] 28. November 2013. [Zitat vom: 30. Juni 2015.] https://www.fkie.fraunhofer.de/de/presse/pressemitteilungen-2013/versteckte-audiouebertragung.html.
13. **Himmelein, Gerald.** Supertrojaner BadBIOS: Unwahrscheinlich, aber möglich. *heise Security.* [Online] 11. November 2013. [Zitat vom: 30. Juni 2015.] http://www.heise.de/security/meldung/Supertrojaner-BadBIOS-Unwahrscheinlich-aber-moeglich-2043114.html.
14. **Jaquin, Pedro, Colunga, Luis und Gómez, Roberto.** RouterPwn. [Online] [Zitat vom: 26.. September 2016.] http://www.routerpwn.com/.
15. **Scherschel, Fabian A.** Automatisierte Medikamenten-Verteiler mit über 1400 Sicherheitslücken. *Heise Security.* [Online] 31.. März 2016. [Zitat vom: 4.. Oktober 2016.] http://www.heise.de/newsticker/meldung/Automatisierte-Medikamenten-Verteiler-mit-ueber-1400-Sicherheitsluecken-3159439.html.

16. **Klan, Florian.** Fritzbox-Router: AVM veröffentlicht FritzOS 6.20. *Heise Netze.* [Online] 12. August 2014. [Zitat vom: 9. Juli 2015.] http://www.heise.de/netze/meldung/Fritzbox-Router-AVM-veroeffentlicht-FritzOS-6-20-2290849.html.
17. Stranger Danger! What Is the Risk From 3rd Party Libraries. *Blackhat USA 2015.* [Online] 29.. Dezember 2015. [Zitat vom: 26.. September 2016.] https://youtu.be/Qi_kyj8xnH0.
18. **Cisco Systems Inc.** Vulnerability in GNU glibc Affecting Cisco Products: February 2016. *Cisco.* [Online] 18.. Februar 2016. [Zitat vom: 26.. September 2016.] http://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20160218-glibc.
19. **Cerrado Consultants Limited.** RouterPasswords.com. [Online] 2014. [Zitat vom: 28. 09 2015.] http://www.routerpasswords.com/.
20. **Department of Homeland Security.** Sixnet BT Series Hard-coded Credentials Vulnerability. *ICS-CERT.* [Online] 26.. Mai 2016. [Zitat vom: 26.. September 2016.] https://ics-cert.us-cert.gov/advisories/ICSA-16-147-02.
21. **Stewin, Patrick.** *Detecting Peripheral-based Attacks on the Host Memory.* Schweiz : Springer International Publishing Switzerland, 2015.
22. **Red Ballon Security.** Technologie. *Red Ballon Security.* [Online] 2014. [Zitat vom: 20. Juli 2015.] http://frak.redballoonsecurity.com/technology.html.
23. **Duflot, Loïc, et al., et al.** Can You Still Trust Your Network Card. *French Network and Information Security Agency.* [Online] März 2010. [Zitat vom: 31. Juli 2015.] http://www.ssi.gouv.fr/uploads/IMG/pdf/csw-trustnetworkcard.pdf.
24. **Müller, Tilo, Taubmann, Benjamin und Freiling, Felix C.** TreVisor - OS-Independent Software-Based Full Disk Encryption. *Proceedings of the 10th International Conference on Applied Cryptography and Network Security (ACNS 2012).* 26. Juni 2015, S. 66-83.
25. **Lone Sang, Fernand, et al., et al.** Exploiting an I/OMMU vulnerability. *Proceedings of the 5th International Conference on Malicious and Unwanted Software (MALWARE 2010).* 19. Oktober 2010, S. 7-14.
26. **Wojtczuk, Rafal und Rutkowska, Joanna.** Following the White Rabbit: Software Attacks against Intel VT-d Technology. *Invisible Things Lab.* [Online] April 2011. [Zitat vom: 31. Juli 2015.] http://www.invisiblethingslab.com/resources/2011/Software%20Attacks%20on%20Intel%20VT-d.pdf.
27. *VIPER: Verifying the Integrity of PERipherals' Firmware.* **Li, Yanlin, McCune, Jonathan M. und Perrig, Adrian.** Chicago, USA : ACM, 2011. Proceedings of the 18th ACM Conference on Computer and Communications Security (CCS 2011). S. 3-16.
28. **Nguyen, Quan.** Issues in Software-based Attestation. *CyberSecurity for the Next Generation - International Student Conference.* New York, USA : http://www.kaspersky.com/images/Quan%20Nguyen.pdf, 15. November 2012.
29. **Goodin, Dan.** Bizarre attack infects Linksys routers with self-replicating malware. *ars technica.* [Online] 13. Februar 2014. [Zitat vom: 30. Juni 2015.] http://arstechnica.com/security/2014/02/bizarre-attack-infects-linksys-routers-with-self-replicating-malware/.
30. **Krebs, Brian.** Lizard Stresser Runs on Hacked Home Routers. *Krebs on Security.* [Online] 9. Januar 2015. [Zitat vom: 30. Juni 2015.] https://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/.
31. **Bilodeu, Olivier und Dupuy, Thomas.** Dissecting Linux/Moose. *Eset.* [Online] Mai 2015. [Zitat vom: 30. Juni 2015.] http://www.welivesecurity.com/wp-content/uploads/2015/05/Dissecting-LinuxMoose.pdf.
32. **unixfreaxjp.** MMD-0056-2016 - Linux/Mirai, how an old ELF malcode is recycled.. . *Malware Must Die!* [Online] 31. August 2016. [Zitat vom: 26.. September 2016.] http://blog.malwaremustdie.org/2016/08/mmd-0056-2016-linuxmirai-just.html.

33. **Ballano, Mario.** Is there an Internet-of-Things vigilante out there? *Symantec Official Blog.* [Online] Oktober 1, 2015. [Cited: Oktober 1, 2015.] http://www.symantec.com/connect/blogs/there-internet-things-vigilante-out-there.
34. **Schirmacher, Dennis.** Rekord-DDoS-Attacke mit 1,1 Terabit pro Sekunde gesichtet. *Heise Security.* [Online] 29. September 2016. [Zitat vom: 2. Mai 2017.] https://www.heise.de/security/meldung/Rekord-DDoS-Attacke-mit-1-1-Terabit-pro-Sekunde-gesichtet-3336494.html.
35. **Wirtgen, Jörg.** DDoS-Tool Mirai versklavt Gateways von Sierra Wireless fürs IoT-Botnet. *Heise Security.* [Online] 15. Oktober 2016. [Zitat vom: 2. Mai 2017.] https://www.heise.de/security/meldung/DDoS-Tool-Mirai-versklavt-Gateways-von-Sierra-Wireless-fuers-IoT-Botnet-3351085.html.
36. **Kafeine.** An Exploit Kit dedicated to CSRF Pharming. *Malware don't need Coffee.* [Online] 22. Mai 2015. [Zitat vom: 30. Juni 2015.] http://malware.dontneedcoffee.com/2015/05/an-exploit-kit-dedicated-to-csrf.html.
37. **Eikenberg, Roland.** Cisco warnt vor Attacken mittels manipulierter Firmware. *Heise Security.* [Online] 13. August 2015. [Zitat vom: 14. August 2015.] http://www.heise.de/newsticker/meldung/Cisco-warnt-vor-Attacken-mittels-manipulierter-Firmware-2778535.html.
38. **Kim, Pierre.** Multiple vulnerabilities found in Quanta LTE routers (backdoor, backdoor accounts, RCE, weak WPS ...). *A slice of Kimchi - IT Security Blog.* [Online] 4.. April 2016. [Zitat vom: 26.. September 2016.] https://pierrekim.github.io/blog/2016-04-04-quanta-lte-routers-vulnerabilities.html.
39. —. Multiple vulnerabilities found in the Dlink DWR-932B (backdoor, backdoor accounts, weak WPS, RCE ...). *A slice of Kimchi - IT Security Blog.* [Online] 28.. September 2016. [Zitat vom: 9.. November 2016.] https://pierrekim.github.io/blog/2016-09-28-dlink-dwr-932b-lte-routers-vulnerabilities.html.
40. **Leverett, Eireann.** Switches Get Stitches - Industrial System Ownership. *The 31st Chaos Communication Congress (31C3).* Hamburg, Deutschland : Chaos Computer Club e.V., 28. Dezember 2014.
41. **Ermert, Monika.** Schnüffelcode in Juniper-Netzgeräten: Weitere Erkentnisse und Spekulationen. *Heise Security.* [Online] 21.. Dezember 2015. [Zitat vom: 26.. September 2016.] http://www.heise.de/security/meldung/Schnueffelcode-in-Juniper-Netzgeraeten-Weitere-Erkenntnisse-und-Spekulationen-3051260.html.
42. **Cui, Ang und Costello, Michael.** Hacking Cisco Phones. *The 29st Chaos Communication Congress (29C3).* Hamburg, Deutschland : Chaos Computerclub e.V., 1. Januar 2013.
43. **Jodeit, Moritz.** Hacking Video Conferencing Systems. *Blackhat Europe 2013.* Amsterdam, Niederlande : s.n., 15. März 2013.
44. **Kleinz, Torsten und Scherschel, Fabian.** Der Feind hört mit: IP-Telefone von Snom aus dem Netz angreifbar. *heise Security.* [Online] 13. Januar 2015. [Zitat vom: 30. Juni 2015.] http://www.heise.de/security/meldung/Der-Feind-hoert-mit-IP-Telefone-von-Snom-aus-dem-Netz-angreifbar-2517201.html.
45. **Central Intelligence Agency.** sontaran. *Vault 7: CIA Hacking Tools Revealed.* [Online] 7. März 2017. [Zitat vom: 2. Mai 2017.] https://wikileaks.org/ciav7p1/cms/page_524426.html.
46. **Costin, Andrei.** Hacking MFPs. *The 28th Chaos Communication Congress (28C3).* Berlin, Deutschland : Chaos Computerclub e.V., 28. Dezember 2011.
47. **Cui, Ang, Costello, Michael und Stolfo, Salvatore.** When Firmware Modifcations Attack: A Case Study of Embedded Exploitation. *20th Annual Network & Distributed System Security Symposium (NDSS).* Sand Diego, Californien, USA : Internet Society, 25. Februar 2013.
48. **Greif, Björn.** Samsung warnt: Smart-TVs hören auch Privatgespräche mit. *ZDNet.* [Online] 9.. Februar 2015. [Zitat vom: 26.. September 2016.] http://www.zdnet.de/88218506/samsung-warnt-smart-tvs-hoeren-auch-privatgespraeche-mit/.

49. **Resno.** Exploitee.rs. [Online] [Zitat vom: 26.. September 2016.] https://www.exploitee.rs.
50. **Central Intelligence Agency.** Vault 7: CIA Hacking Tools Revealed. *Weeping Angel (Extending) Engineering Notes.* [Online] 7. März 2017. [Zitat vom: 3. Mai 2017.] https://wikileaks.org/ciav7p1/cms/page_12353643.html.
51. **Polizei Gelsenkirchen.** POL-GE: Ergänzende Pressemitteilung zur OTS-Meldung vom 28.01.2015, 11:15 Uhr: Einladung zur Pressekonferenz wegen eines bundesweiten Einsatzes aufgrund von banden- und gewerbsmäßigen Computerbetruges. *Presseportal.* [Online] 29. Januar 2015. [Zitat vom: 9. Juli 2015.] http://www.presseportal.de/blaulicht/pm/51056/2938105.
52. **Heffner, Craig.** Hacking the D-Link DSP-W215 Smart Plug. */DEV/TTYS0 - Embedded Device Hacking.* [Online] 15. Mai 2014. [Zitat vom: 9. Juli 2015.] http://www.devttys0.com/2014/05/hacking-the-d-link-dsp-w215-smart-plug/.
53. **Ronen, Eyal und Shamir, Adi.** Extended Functionality Attacks on IoT Devices: The Case of Smart Lights. *2016 IEEE European Symposium on Security and Privacy.* 2016.
54. **Tierney, Andrew.** Thermostat Ransomware: a lesson in IoT security. *Pen Test Partners.* [Online] 8.. August 2016. [Zitat vom: 26.. September 2016.] https://www.pentestpartners.com/blog/thermostat-ransomware-a-lesson-in-iot-security/.
55. **Rotem, Kerner.** Remote Code Execution in CCTV-DVR affecting over 70 different vendors . *Kerner on Security.* [Online] 22. März 2016. [Zitat vom: 26.. September 2016.] http://www.kerneronsec.com/2016/02/remote-code-execution-in-cctv-dvrs-of.html.
56. **Holland, Martin.** BND verheimlichte angeblich NSA-Hintertür in Überwachungskameras. *Heise online.* [Online] 27.. September 2016. [Zitat vom: 28.. September 2016.] http://www.heise.de/newsticker/meldung/BND-verheimlichte-angeblich-NSA-Hintertuer-in-Ueberwachungskameras-3333992.html.
57. **O'Flynn, Colin, et al., et al.** IoT Goes Nuclear: Creating a ZigBee Chain Reaction. *Cryptology ePrint Archive, Report 2016/1047.* [Online] 7. November 2016. [Zitat vom: 03. Mai 2017.] http://eprint.iacr.org/2016/1047.
58. **Scherschel, Fabian.** Root-Shell im Krankenhaus: Hospira-Infusionspumpe mit Telnet-Lücke. *Heise Security.* [Online] 5. Mai 2015. [Zitat vom: 10. Juli 2015.] http://www.heise.de/security/meldung/Root-Shell-im-Krankenhaus-Hospira-Infusionspumpe-mit-Telnet-Luecke-2633529.html.
59. **Bergert, Denise und Kannenberg, Axel.** Weitere Sicherheitslücke in Hospira-Infusionspumpen. *Heise Security.* [Online] 9. Juni 2015. [Zitat vom: 10. Juli 2015.] http://www.heise.de/newsticker/meldung/Weitere-Sicherheitsluecke-in-Hospira-Infusionspumpen-2682272.html.
60. **Koscher, Karl, et al., et al.** Experimental Security Analysis of a Modern Automobile. *2010 IEEE Symposium on Security and Privacy.* 16. Mai 2010, S. 447-462.
61. **Domke, Felix.** Script Your Car! *The 30th Chaos Communication Congress (30C3).* Hamburg, Deutschland : Chaos Computerclub e.V., 29. Dezember 2013.
62. **Valasek, Chris und Miller, Charlie.** *Adventures in Automotive Networks and Control Units (Whitepaper).* Seattle : IOActive, 2013.
63. **Smith, Craig.** *Car Hackers Handbook.* San Francisco, USA : No Starch Press, Inc., 2016. ISBN: 978-1-59327-703-1.
64. **Valasek, Chris und Miller, Charlie.** *A Survey of Remote Automotive Attack Surfaces (Whitepaper).* Seattle : IOActive, 2014.
65. **Vallance, Chris.** Car hack uses digital-radio broadcasts to seize control. *BBC News.* [Online] 22. Juli 2015. [Zitat vom: 27. Juli 2015.] http://www.bbc.com/news/technology-33622298.
66. **Wilkens, Andreas.** Tesla Model S lässt sich von fern kapern. *Heise Online.* [Online] 20.. September 2016. [Zitat vom: 4.. Oktober 2016.] https://www.heise.de/newsticker/meldung/Tesla-Model-S-laesst-sich-von-fern-kapern-3327510.html.

67. **tw, sb.** Elektronik Bank Robberies. *30th Chaos Communication Congress (30C3).* Hamburg, Deutschland : Chaos Computer Club e.V., 27. Dezember 2013.
68. **Schirrmacher, Dennis.** Kriminelle knacken Geldautomaten in Taiwan und sollen zwei Millionen Euro erbeutet haben. *Heise Security.* [Online] 13.. Juli 2016. [Zitat vom: 29.. September 2016.] http://www.heise.de/newsticker/meldung/Kriminelle-knacken-Geldautomaten-in-Taiwan-und-sollen-zwei-Millionen-Euro-erbeutet-haben-3265584.html.
69. **Department of Homeland Security.** Backoff Point-of-Sale Malware. *US-CERT.* [Online] 31.. Juli 2014. [Zitat vom: 26.. September 2016.] https://www.us-cert.gov/ncas/alerts/TA14-212A.
70. **Eikenberg, Ronald.** Malware zapft Kreditkartendaten von Oracle-Kassensystemen ab. *Heise online.* [Online] 08. Juni 2015. [Zitat vom: 20. Juli 2015.] http://www.heise.de/newsticker/meldung/Malware-zapft-Kreditkartendaten-von-Oracle-Kassensystemen-ab-2680638.html.
71. **Scherschel, Fabian.** Meeresgott bestiehlt Kassensysteme. *Heise Security.* [Online] 24. März 2015. [Zitat vom: 20. Juli 2015.] http://www.heise.de/security/meldung/l-f-Meeresgott-bestiehlt-Kassensysteme-2583596.html.
72. —. Das Stuxnet-Duo: Bösartige Geschwister. *Heise Security.* [Online] 26. November 2013. [Zitat vom: 20. Juli 2015.] http://www.heise.de/security/meldung/Das-Stuxnet-Duo-Boesartige-Geschwister-2053847.html.
73. **Bundesamt für Sicherheit in der Informationstechnik.** *Die Lage der IT-Sicherheit in Deutschland 2014.* Bonn : Bundesamt für Sicherheit in der Informationstechnik, 2014.
74. **Gorman, Siobhan, Dreazen, Yochi J. und Cole, August.** Insurgents Hack U.S. Drones. *The Wall Street Journal.* [Online] 17. Dezember 2009. [Zitat vom: 30. Juli 2015.] http://www.wsj.com/articles/SB126102247889095011.
75. **Greenberg, Andy.** Hackers Can Disable a Sniper Rifle - Or Change its Target. *Wired.* [Online] 29. Juli 2015. [Zitat vom: 30. Juli 2015.] http://www.wired.com/2015/07/hackers-can-disable-sniper-rifleor-change-target/.
76. **Intel Corporation.** TianoCore. [Online] [Zitat vom: 26.. September 2016.] www.tianocore.org.
77. **Ge, Levian.** BIOS Threat is Showing up Again! *Symantec Official Blog.* [Online] 09. September 2011. [Zitat vom: 21. Juli 2015.] http://www.symantec.com/connect/blogs/bios-threat-showing-again.
78. **Kaczmarek, Sébastien.** UEFI and Dreamboot. *Quarkslab Innovative Security.* [Online] April 2013. [Zitat vom: 21. Juli 2015.] http://www.quarkslab.com/dl/13-04-hitb-uefi-dreamboot.pdf.
79. **Kallenberg, Corey und Kovah, Xeno.** How Many Million BIOSes Would you Like to Infect? *CanSecWest 2015.* Vancouver, Canada : http://legbacore.com/Research_files/HowManyMillionBIOSWouldYouLikeToInfect_Full.pdf, 20. März 2015.
80. **Oleksiuk, Dmytro.** Building reliable SMM backdoor for UEFI based platforms. *My aimful life - Another Blog by Dmytro Oleksiuk aka Cr4sh.* [Online] 5. Juli 2015. [Zitat vom: 21. Juli 2015.] http://blog.cr4.sh/2015/07/building-reliable-smm-backdoor-for-uefi.html.
81. **Schmidt, Jürgen.** Hacking Team verwendet UEFI-Rootkit. *Heise Security.* [Online] 7. Juli 2015. [Zitat vom: 21. Juli 2015.] http://www.heise.de/security/meldung/Hacking-Team-verwendet-UEFI-Rootkit-2750312.html.
82. **Ries, Uli.** BIOS/UEFI mit Ransomware infiziert. *Heise Security.* [Online] 20. Februar 2017. [Zitat vom: 3. Mai 2017.] https://www.heise.de/newsticker/meldung/BIOS-UEFI-mit-Ransomware-infiziert-3630662.html.
83. **Tereshkin, Alexander und Wojtczuk , Rafal.** Introducing Ring -3 Rootkits. *Black Hat USA 2009.* Las Vegas, USA : http://www.blackhat.com/presentations/bh-usa-09/TERESHKIN/BHUSA09-Tereshkin-Ring3Rootkit-SLIDES.pdf, 29. Juli 2009.
84. *Understanding DMA Malware.* **Stewin, Patrick und Bystrov, Iurii.** Heraklion, Griechenland : Springer-Verlag Berlin Heidelberg, 2012. 9th International Conference

on Detection of Intrusion and Malware, and Vulnerabilty Assessment (DIMVA 2012). S. 21-41.
85. **Marek, Rudolf.** AMD x86 SMU Firmware Analysis. *31st Chaos Communication Congress (31C3).* Hamburg, Deutschland : Chaos Computer Club e.V., 27. Dezember 2014.
86. **Heasman, John.** Implementing and Detecting a PCI Rootkit. *Black Hat DC 2007.* Sheraton Crystal City, Virginia, USA : https://www.blackhat.com/presentations/bh-dc-07/Heasman/Paper/bh-dc-07-Heasman-WP.pdf, 28. Februar 2007.
87. **Triulzi, Arrigo.** Project Maux Mk.II. *PacSec 2008.* [Online] 2008. November 2008. [Zitat vom: 29. Juli 2015.] http://www.alchemistowl.org/arrigo/Papers/Arrigo-Triulzi-PACSEC08-Project-Maux-II.pdf.
88. **Aumitre, Damien und Devine, Christophe.** Subverting Windows 7 x64 Kernel with DMA attacks. *Hack in the Box Security Conference Amsterdam .* [Online] 2. Juli 2010. [Zitat vom: 29. Juli 2015.] http://conference.hitb.org/hitbsecconf2010ams/materials/D2T2%20-%20Devine%20&%20Aumaitre%20-%20Subverting%20Windows%207%20x64%20Kernel%20with%20DMA%20Attacks.pdf.
89. **Duflot, Loic, Perez, Yves-Alexis und Morin, Benjamin.** What If You Can't Trust Your Network Card? *Recent Advances in Intrusion Detection (RAID 2011).* Menlo Park : Springer Berlin Heidelberg, 2011, S. 378-397.
90. **Ladakis, Evangelos, et al., et al.** You Can Type, but You Can't Hide: A Stealthy GPU-based Keylogger. *2013 European Workshop on System Security.* Prag, Tshechische Repulik : http://www.cs.columbia.edu/~mikepo/papers/gpukeylogger.eurosec13.pdf, 14. April 2013.
91. **Scherschel, Fabian.** l+f: Der Keylogger in der GPU. *Heise Security.* [Online] 11. Mai 2015. [Zitat vom: 22. Juli 2015.] http://www.heise.de/security/meldung/l-f-Der-Keylogger-in-der-GPU-2641154.html.
92. **Domburg, Jeroen.** Hard Disk Hacking. *SpritesMods.com.* [Online] August 2013. [Zitat vom: 22. Juli 2015.] http://spritesmods.com/?art=hddhack.
93. **bunnie und Xobs.** The Exploration and Exploitation of an SD Memory Card. *30th Chaos Communication Congress (30C3).* Hamburg, Deutschland : Chaos Computer Club e.V., Dezember 2013.
94. **Windeck, Christof.** Externe Festplatten mit Verschlüsselung knackbar. *Heise Online.* [Online] 7.. August 2016. [Zitat vom: 27.. September 2016.] http://www.heise.de/newsticker/meldung/Externe-Festplatten-mit-Verschluesselung-knackbar-3289530.html.
95. **Guri, Mordechai, Monitz, Matan und Elovici, Yuval.** *USBee: Air-Gap Covert-Channel via .* Israel : Ben-Gurion University of the Negev , 2016.
96. **Maynor, David.** DMA: Skeleton Key of Computing && Selected Soap Box. *CanSec West.* [Online] Mai 2005. [Zitat vom: 29. Juli 2015.] http://cansecwest.com/core05/DMA.ppt.
97. **Schmidt, Jürgen.** BadUSB: Wenn USB-Geräte böse werden. *Heise Security.* [Online] 31. Juli 2014. [Zitat vom: 22. Juli 2015.] http://www.heise.de/security/meldung/BadUSB-Wenn-USB-Geraete-boese-werden-2281098.html.
98. **Eikenberg, Ronald.** BadUSB-Tools kursieren im Netz, Angriffs-Stick im Eigenbau. *Heise Security.* [Online] 3. Oktober 2014. [Zitat vom: 22. Juli 2015.] http://www.heise.de/security/meldung/BadUSB-Tools-kursieren-im-Netz-Angriffs-Stick-im-Eigenbau-2411135.html.
99. **Hudson, Trammell.** Thunderstrike. *Trammell Hudson's Porjects.* [Online] 05. Februar 2015. [Zitat vom: 30. Juni 2015.] https://trmm.net/Thunderstrike.
100. **Zetter, Kim.** Researchers Create First Firmware Worm that Attacks Macs. *WIRED.* [Online] 3. August 2015. [Zitat vom: 4. August 2015.] http://www.wired.com/2015/08/researchers-create-first-firmware-worm-attacks-macs/.

101. **carmaa.** Inception. [Online] 17. April 2015. [Zitat vom: 29. September 2015.] https://github.com/carmaa/inception.
102. **Frisk, Ulf.** macOS FileVault2 Password Retrieval. *Security | DMA | Hacking .* [Online] 15. Dezember 2016. [Zitat vom: 3. Mai 2017.] http://blog.frizk.net/2016/12/filevault-password-retrieval.html.
103. **Becher, Michael, Dornseif, Maximillian und Klein, Christian N.** 0wn3d by an iPod: Firewire/1394 Issues. *10th annual CanSecWest conference.* Vancouver, Kanada : s.n., April 2005.
104. **Boileau, Adam.** Hit by a Bus: Pysical Access Attacks with Firewire. *Ruxcon 2006.* [Online] 30. September 2006. [Zitat vom: 29. Juli 2015.] http://www.security-assessment.com/files/presentations/ab_firewire_rux2k6-final.pdf.
105. **Piegdon, David R. und Pimendis, Lexi.** Targeting Physically Addressable Memory. *4th International Conference on Detection of Intrusions and Mailware and Vulnerability Assessment (DIMVA 2007).* Luzern, Schweiz : Springer-Verlag Berlin Heidelberg, Juli 2007.
106. **Kamkar, Samy.** Keysweeper. [Online] 12. Januar 2015. [Zitat vom: 24. Juli 2015.] http://samy.pl/keysweeper/.
107. **Hak5 LLC.** USB Rubber Ducky Wiki. [Online] [Zitat vom: 28. 09 2015.] http://usbrubberducky.com/.
108. **Inverse Path S.r.l.** USB Armory. *Inverse Path.* [Online] 2015. [Zitat vom: 9. September 2015.] http://inversepath.com/usbarmory.html.
109. **USBKill.com.** USB Killer. *USB Kill.* [Online] [Zitat vom: 23.. September 2016.] https://www.usbkill.com/usb-killer/8-usb-killer.html.
110. **Fuller, Mubix.** Snagging creds from locked machines. *Room362.* [Online] 6. September 2016. [Zitat vom: 21. September 2016.] https://room362.com/post/2016/snagging-creds-from-locked-machines/.
111. **Adee, Sally.** The Hunt for the Kill Switch. *IEEE Spectrum.* 1. Mai 2008, S. http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch.
112. *Experiences in Hardware Trojan Design and Implementation.* **Jin, Yier, Kupp, Nathan und Makris, Yiorgos.** New York : IEEE, 2009. 2009 IEEE International Workshop on Hardware Oriented Security and Trust (HOST 2009). S. 50-57.
113. *Designing and Implementing Malicious Hardware.* **King, Samuel T., et al., et al.** Berkeley, CA, USA : USENIX Association, 2008. Proceedings of the 1st Usnix Workshop on Large-Scale Exploits and Emergent Threats. S. 51-58.
114. **Kocher, Paul C.** Timing Attacks on Implementations of Diffie-Hellman, RSA, DDS, and Other Systems. *Advances in Cryptology — CRYPTO '96.* s.l. : Springer Verlag Berlin Heidelberg, 1996, S. 104 - 113.
115. **Lang, Li, Burleson, Wayne und Paar, Christof.** MOLES: Malicious off-chip leakage enabled by side-channels. *IEEE/ACM International Conference on Computer-Aided Design - Digest of Technical Papers, 2009 (ICCAD 2009).* San Jose, CA, USA : IEEE, 2009, S. 117-122.
116. *Hardware Trojans in Wireless Cryptographic Integrated Circuits.* **Jin, Yier und Makris, Yiorgos.** San Jose, CA, USA : IEEE, 2013. 2013 IEEE/ACM International Conference on Coputer-Aided Design (ICCAD 2013). S. 399-404.
117. **Samuel, Henry.** Chip and pin scam 'has netted millions from British shoppers'. *The Telegraph.* [Online] 10. October 2008. [Zitat vom: 20. Juli 2015.] http://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-netted-millions-from-British-shoppers.html.