



Security Benchmark and Forensics Framework

Masterthesis

Zur Erlangung des akademischen Grades
Master of Science

vorgelegt
im Winter-/Sommersemester 2020/2021

von

Andreas Maurer
Schiblerstrasse 15
CH-8164 Bachs-ZH

1. Prüfer: Prof. Dr. Martin Rieger, Hochschule Albstadt-Sigmaringen, D-72458 Albstadt
2. Prüfer: Prof. Dr. Adrian Perrig, ETH Zürich, CH-8092 Zürich

©Andreas Maurer, Schiblerstrasse 15, CH-8164 Bachs-ZH

Diese Masterarbeit „SCION Security Benchmark and Forensics Framework“ entstand im Rahmen des Studiengangs MSc Digitale Forensik (JG2017) im Winter-/Sommersemester 2020/2021. Die in dem Dokument enthaltenen Erkenntnisse sind nach bestem Wissen entwickelt und dargestellt. Eine Haftung für die Korrektheit und Verwendbarkeit der Resultate kann jedoch weder vom Autoren noch von den Herausgebern übernommen werden. Alle Rechte verbleiben beim Autor.

Zusammenfassung

Die Internet Architektur SCION wurde auf der grünen Wiese „Clean-Slate-Design“ radikal neu entwickelt. Das primäre Ziel ist, die grundlegende Sicherheit auf ein verbessertes Niveau zu bringen und die allgemeinen Schwächen des Border Gateway Protocol (BGP) auszumerzen. Die Entwicklung ist noch nicht vollumfänglich abgeschlossen und daher wird laufend weiterentwickelt und optimiert. Die stetig steigenden Bedrohungen durch Cyber Attacken aus dem Internet, machen ein Security Operations Center (SOC) und eine neue Architektur wie SCION unabdingbar. Im Providerumfeld und in der Finanzbranche finden bereits die ersten Feldversuche resp. ersten Pilotintegrationen statt. Auch wir, von der Swiss Stock Exchange (SIX), welche den Informations- und Geldfluss zwischen Banken, Händlern, Investoren und Dienstleistern weltweit sicherstellen, sind an einer effizienteren, sichereren und stabileren Internet Architektur bzw. Plattform interessiert. Das Hauptziel ist, ein sicheres und widerstandfähiges Kommunikationsnetzwerk für den Finanzmarktplatz Schweiz aufzubauen.

Mit dieser Masterarbeit soll ein fehlender Baustein erarbeitet werden, der den sichereren Aufbau, die sichere Integration und Inbetriebnahme von SCION bei der Kundschaft ermöglicht. Darunter verstehen wir ein Werkzeug „SCION Security Benchmarks and Forensics Framework“, das die SCION Installation auf ihre Sicherheit durch anerkannte Methoden gründlich überprüft. Im Fokus steht das weitverbreitete und beim Kunden vorortinstallierte SCION IP Gateway (SIG). Es stellt die Verbindung zwischen zwei unterschiedlichen Systemen her und ermöglicht die Kommunikation von Legacy-IP-Anwendungen über SCION. Auf der Appliance laufen die im Fokus stehenden Control Services (CS) und der Border Router (BR). Im praktischen Teilbereich werden die theoretisch behandelten Themenschwerpunkte und Fragestellungen in einem Satz von Sicherheitstests im Open Source Security Auditing Tool namens „Lynis“ integriert. Der SCION Security Benchmark kann lokal oder remote vollautomatisiert und effizient durch einen SCION Administrator durchgeführt werden. Die modular aufgebauten, leicht verständlichen und erweiterbaren Controls, ermöglichen so künftige Optimierungen und Erweiterungen. Ein übersichtlicher Report zeigt eine Gesamtwertung und die Testresultate mit entsprechenden Kommentaren und Empfehlungen.

Auch ein spezieller Fokus gilt der digitalen Forensik und deren Eruierung von forensischen SCION Spuren. Es fehlen noch jegliche Kenntnisse, die z. B. durch die Bereitstellung des gehärteten Betriebssystems oder durch die Installationen der SCION Services und Utilities verursacht wurden. Das Vorwissen aus einer solchen Spurenanalyse gehört zu den essenziell wichtigen Grundbausteinen in forensischen Untersuchungen nach möglichen Sicherheitsvorfällen. Ein SIG-Grundlagenwissen ist unverzichtbar und daher eine Voraussetzung, die hier durch eine Anwendungsanalyse erarbeitet wird. Mit anerkannten und forensischen Methoden werden danach die charakteristischen und persistenten Spuren gewonnen und beschrieben. Es entsteht sozusagen eine forensische SCION Wissensdatenbank.

Durch den Einsatz des Frameworks kann eine sauberere und sicherere Integration im Entwicklungszyklus und vor der Inbetriebnahme beim Kunden gewährleistet werden. SIX als Finanzdienstleister untersteht verschiedenen Regularien der Eidgenössischen Finanzmarktaufsicht (FINMA) und muss für ihre geschäftlichen Tätigkeiten vielzählige Vorgaben seitens Payment Card Industry (PCI) und Society for Worldwide Interbank Financial Telecommunication (SWIFT) erfüllen. Eine regelmässige Sicherheitsprüfung ist beispielsweise in einem halbjährlichen Review vor internen oder externen Audits ein Muss.

Abstract

The SCION Internet architecture has been radically redeveloped in a greenfield „clean-slate“ design. The primary goal is to bring the basic security to an improved level and to eradicate the general weaknesses of BGP. The development is not fully complete yet and, therefore, it is under continuous research, development and optimization. The constantly increasing threats from cyber attacks out of the Internet, make a SOC and a new architecture such as SCION indispensable. The first field tests and pilot integrations are already taking place in the provider environment and in the financial sector. We at SIX, who ensure the flow of information and money between banks, traders, investors and service providers worldwide, are also interested in a more efficient, secure and stable internet architecture or platform. The main goal is to build a secure and resilient communication network for the Swiss financial marketplace.

With this master thesis we want to develop a missing building block that enables a more secure setup, integration and commissioning of SCION at the customer site. By this we mean a tool „SCION Security Benchmarks and Forensics Framework“ that thoroughly checks the SCION installation for its security using recognized methods. The focus is the SIG, which is widely used and installed at the customer’s site. It establishes the connection between two different systems and enables legacy IP applications to communicate via SCION. The appliance runs the CS and the BR. They are the main focus here. The practical part integrates and maps all developed security-related tests, which are included in a set of security tests in the open source security auditing tool called „Lynis“. The SCION Security Benchmark can be performed locally or remotely in a fully automated and efficient way by a SCION administrator. The modular, easy to understand and extendable controls allow future optimizations and extensions. A clear report shows an overall ranking and the test results with corresponding comments and recommendations.

There is also a special focus on digital forensics and its elicitation of forensic SCION traces. There is still a lack of knowledge caused e.g. by the deployment of the hardened operating system or by the installations of the SCION services and utilities. Prior knowledge from such trace analysis is one of the essential basic building blocks in forensic investigations after possible security incidents. A SIG basic knowledge is indispensable and, therefore, a prerequisite, which is developed here by an application analysis. With recognized and forensic methods, the characteristic and persistent traces are then obtained and described. A forensic SCION knowledge database is created, so to speak.

By using the framework, a cleaner and safer integration can be ensured in the development cycle and before going live at the customer’s site. SIX as a financial services provider is subject to various FINMA regulations and has to comply with numerous PCI and SWIFT requirements for its business activities. Regular security check is a must, for example, in a semi-annual review, prior to internal or external audits.

Danksagung

Im letzten Jahr, als ich auf der Suche nach einer interessanten und spannenden Masterarbeit war, überkam mich als passionierter Network Security Engineer eines Tages ein Blitzgedanke: „Warum kein Thema mit SCION?“. Nach einigen Rückfragen vernahm ich von Arbeitskollegen und aus firmeninternen Projekten nur Gutes und teilweise sogar mit richtiger Begeisterung und prägnanter Überzeugung. Ein herzliches Dankeschön geht daher an meine damaligen Vorgesetzten Dr. Thomas Rhomberg Head IT Security & SOC Services und Johannes Hadodo Head Network Security Services, welche es mir ermöglichten, die Masterthesis in der Firma zu schreiben, das vollständige Vertrauen schenkten und den Mehrwert für die Firma SIX sahen. Anfänglich fiel es mir sehr schwer, die Zeit während der Arbeitszeit zu reservieren, da ich noch stark im täglichen Betrieb und in diversen Projekten tätig war. Die Pandemie COVID-19 half mir diesbezüglich nicht und bescherte unserer Firma einen beträchtlichen Mehraufwand. Als ich mich dann aus dem täglichen Geschehen etwas herausnehmen konnte, widmete ich mich zuerst der Einarbeitung in SCION. Als die Thesis begann, war SCION für mich noch Neuland. Ein grosser Dank geht deshalb auch an meine Teamarbeitskollegen, welche während der langen Ausarbeitungszeit auf meine Projektmitarbeit verzichten oder auf eine Antwort länger warten mussten.

Mit meinem Vorgesetzten Johannes Hadodo besuchte ich schliesslich das Zurich Information Security and Privacy Center (ZISC). Wir trafen auch an der Eidgenössischen Technische Hochschule (ETH) Zürich, nur auf Begeisterte und mit Herzblut verbundene Security Professionals. Nach einer Unterredung mit meinem Zweitprüfer Prof. Dr. Adrian Perrig konnte ich ihn von meinem Projektvorhaben überzeugen. Für seine wertvolle Unterstützung und sein entgegengebrachtes Vertrauen, in einen aussenstehenden Studenten, möchte ich mich herzlich bedanken.

Auch ein besonderes Dankeschön geht an meinen Betreuer Samuel Hitz und seiner Entwickler Kollegen von der Anapaya Systems AG. Sie unterstützen mich mit viel Verständnis und Ausdauer in allen technischen Belangen und gaben mir wertvolle Tipps bei der Ausarbeitung und Programmierung. Aber besonders gefreut hat mich ganzheitlich der kollegiale, verständnisvolle, faire und unkomplizierte Umgang unter allen Projektbeteiligten.

Nicht zu vergessen, bedanke ich mich bei meinem Erstprüfer Prof. Dr. Martin Rieger für seine wertvolle Unterstützung und Betreuung.

Zu guter Letzt geht ein ausgesprochenes Dankeschön an meine Frau und meine Kinder. Allesamt unterstützten mich und brachten während meiner gesamten Studienzeit viel Verständnis und Mitgefühl auf. Sie standen mir stets zur Seite und ermutigten mich weiterzumachen, wenn meine Motivation im Keller war oder ich vor einem scheinbar unlösbaren Problem sass.

Eidesstattliche Erklärung

Hiermit versichere ich Andreas Maurer, an Eides statt, dass ich die vorliegende Arbeit „SCION Security Benchmark and Forensics Framework“ selbstständig und ohne Verwendung anderer als der angegebenen Hilfsmittel angefertigt habe. Alle Stellen, die wörtlich oder sinngemäss aus veröffentlichten und nicht veröffentlichten Schriften entnommen sind, sind als solche kenntlich gemacht. Die Arbeit hat in gleicher oder ähnlicher Form noch in keiner anderen Prüfungsbehörde vorgelegen. Alle eingereichten Versionen der Arbeit sind identisch.

Ort, Datum

Unterschrift

Inhalt

Zusammenfassung	i
Abstrakt	iii
Danksagung	v
Eidesstattliche Erklärung	vii
1. Einleitung	1
1.1. SCION Services	2
1.2. Problemstellung	8
1.3. Aufbau der Arbeit	11
2. Forschungsstand	17
2.1. SCION und andere konkurrierende Ansätze	18
2.2. SCION Faktoren	20
2.3. Grundfragen und aktuelle Entwicklungen	29
2.4. Warum SCION?	31
3. Security Audit Tool Evaluation	33
4. SCION Laborumgebungen	37
4.1. SCION Trainingsumgebung	37
4.2. SCION Testumgebung	38
4.2.1. Hardware	38
4.2.2. Virtuelle Maschinen	38
4.2.3. Images	39
4.2.4. Konfigurationen	40
4.2.5. Software	41
5. Anapaya - Appliance OS Security	45
5.1. Einleitung OS Baseline Security	45
5.2. Empfehlungen zur Systemhärtung	46
5.2.1. File System [FILE]	47
5.2.2. Software Updates [SWUP]	48
5.2.3. Superuser Rights [SUDO]	48
5.2.4. File System Integrity [FINT]	49
5.2.5. Secure Boot [BOOT]	49
5.2.6. Process Hardening [HDME]	50
5.2.7. Mandatory Access Control [AMAC]	50

5.2.8. Command Line Warning Banners [CLWB]	51
5.2.9. Disable/Enable OS Services [DSVC]	51
5.2.10. Disable Network Services [DNWS]	52
5.2.11. Disable Network Protocols [DNWP]	53
5.2.12. Mandatory Firewall Configuration [MFWC]	53
5.2.13. Enable Audit Logging [ENLA]	54
5.2.14. Enable Logging Service [ELOG]	55
5.2.15. Enable Monitoring Service [EMON]	55
5.2.16. System Jobs and Automation Tasks [SJAT]	56
5.2.17. Configuration Secure Shell [CSSH]	56
5.2.18. Configuration Pluggable Authentication Module [CPAM]	57
5.2.19. Configuration User Accounts and Environment [CUAE]	57
5.2.20. System Maintenance and File Permissions [SMFP]	58
5.3. Erkenntnisse	59
6. Docker Security	63
6.1. SCION Networking Stack	64
6.2. Container Bundels	66
6.2.1. SCION Host	69
6.2.2. Control Services	70
6.2.3. Border Router	71
6.2.4. SCION IP Gateway	73
6.2.5. Common Configuration	74
6.2.6. AS-spezifische Service Konfigurationsoptionen	75
6.3. Einleitung Container Baseline Security	75
6.4. Empfehlungen zur Containerhärtung	76
6.4.1. File System [FILE]	76
6.4.2. Enable Docker Auditing [ENDA]	77
6.4.3. Secure Docker Daemon [SDOD]	77
6.4.4. Protect Docker Daemon Configuration [PDOD]	82
6.4.5. Secure Container Runtime Configuration [SCRC]	83
6.4.6. Docker Container Security Operations [DCSO]	87
6.4.7. Disable Cluster Operation Threats [DCOT]	87
6.5. Erkenntnisse	88
7. Forensische Analyse	91
7.1. Implementierung	91
7.1.1. Untersuchungsumgebung	92
7.1.2. Angewendete Methode	95
7.1.3. Berücksichtigte Spurenbilder	99
7.1.4. Angewendete Werkzeuge mit ihren Eigenheiten	100
7.2. Spurenauswertung	111
7.2.1. Charakterische Spuren des SCION Hardening - OS Konfiguration	115
7.2.2. Charakterische Spuren der SCION Services - SCION Konfiguration	120
7.2.3. Charakterische Spuren des SCION Auditing - Lynis Audit Tool	126
7.2.4. Allgemeine (Super)Timeline Analyse	128

7.3. Erkenntnisse	131
8. Fazit	133
9. Ausblick	135
Abkürzungsverzeichnis	137
Literatur	143
Abbildungsverzeichnis	147
Tabellenverzeichnis	149
Listings	151
A. Nutzungsvereinbarung	153
B. Elektronische Fassung	155

EINLEITUNG

Die Geschichte des Internets begann nicht vor allzu langer Zeit. Wie den meisten Technikinteressierten bekannt, begann alles vor ca. 60 Jahren in den 1960er Jahren. Aufgrund von Forschungsförderungen im militärischen und akademischen Bereich, gab es in relativ kurzer Zeit grosse Fortschritte und das internationale Wachstum und die Ausbreitung des Internets nahm rasant Fahrt auf. Eine neue, öffentlich und anfänglich ungeschützte Kommunikationsplattform mit unbeschränkten Möglichkeiten schien geboren zu sein und wucherte fast selbstorganisatorisch dahin. Die Gesellschaft erkannte also sehr früh das Potenzial im Internet, aber unterschätzte verständlicherweise das zukünftige Ausbreitungsausmass mit den Seiteneffekten und daraus resultierenden Problemstellungen.

Durch die stetige Digitalisierung wurden die Wirtschaft und die Gesellschaft stark beeinflusst und verändert. Dadurch steigen und verändern sich die Angriffsvektoren und die Anforderung für entsprechende Gegenmassnahmen. Im Zusammenhang mit der Onlinekommunikation sind insbesondere die permanente Verfügbarkeit, die Digitalisierung, die weite Verbreitung, die Vielzahl an Anwendungen und die praktisch nicht löschbaren Informationen (right to be forgotten) auf Grund ihrer Zerstreuung zu nennen. Die technologischen Neuerungen[37] und Möglichkeiten führen unweigerlich zu stetigen Herausforderungen. Wegen der drohenden IPv4-Adressknappheit wurde die Version 6 des Internet Protokolls schon vor über 20 Jahren standardisiert und verabschiedet. Das sehr stark verankerte Internet Protocol (IP) und die ergänzenden Routing-Protokolle wie z. B. das BGP bergen allgemeine Schwächen[18] und führen zu gravierenden Sicherheitslücken auf der Netzwerkschicht im Internet. Das kommt daher, weil das Protokoll unter anderen Voraussetzungen, Anforderungen und Annahmen entwickelt wurde und den heutigen Ansprüchen schlichtweg nicht mehr gerecht wird.

Schon vorzeitig wurde erfolglos versucht, die bekannten Probleme[19][52] mit zusätzlichen Protokollen oder Erweiterungen zu umgehen, beziehungsweise zu korrigieren. Es wird bereits über einer Dekade an verlässlicheren und sicheren Internet Architekturen geforscht. SCION gilt als solche Architektur und hat das primäre Ziel die grundlegende Sicherheit auf ein verbessertes Niveau zu bringen und die allgemeinen Schwächen des BGP auszumerzen. Ein grosser Vorteil von SCION ist, dass es auf der grünen Wiese unter viel besseren Voraussetzungen, mit dem Wissen der Schwächen seines Vorgängers, von Grund auf neu entworfen werden konnte. Wie angesprochen, werden nicht nur einzelne Teile wie etwa die Übertragungsprotokolle weiterentwickelt, sondern die grundlegende Funktionsweise des Internets verändert. Der absolut passende Name „SCION“ verkörpert resp. benennt die Hauptziele treffend, nämlich Scalability, Control, and Isolation On Next-generation Networks. Die stetig steigenden Anforderungen an die Vertraulichkeit, Verfügbarkeit und Sicherheit, hauptsächlich verursacht durch Cyber Attacken aus dem Internet, machen in Unternehmen nicht nur ein SOC sondern auch eine neue Internet Architektur wie SCION unabdingbar.

1.1. SCION Services

Ein Grundverständnis über die SCION Internet Architektur erscheint notwendig, um den nachfolgenden Erläuterungen folgen zu können und die Themenschwerpunkte zu verstehen. Dieses Kapitel bietet sich, für eine kurze SCION Einführung, mit einem Überblick über die wichtigsten und relevanten SCION Services, beziehungsweise die im Fokus stehenden SCION Infrastrukturkomponenten an. Die nachfolgenden Erläuterungen basieren auf den SCION Kursunterlagen[28][29], dem SCION Buch[52], aus den Gesprächen und Diskussionen mit den Anapaya Entwicklern und den SIX internen SSFN Konzepten[30][3][58][57][33][34] und Projekterfahrungen.

Bekannt ist SCION vor allem durch seine vier Hauptmerkmale. Im SCION Netzwerk entscheidet der Absender wohin und wie die Datenpakete sicher, zuverlässig und über mehrere Pfade zum Zielsystem gelangen. Die Sicherheit und Vertraulichkeit entsteht durch die spezifizierte Isolation Domain (ISD). Ein ISD ist ein Vertrauensbereich, der in der Trusted Root Configuration (TRC) hierarchisch definiert wird und zwischen den Netzwerkteilnehmern gilt. Es gibt zwei Routingebenen, die intra-ISD für ISD interne und inter-ISD für externe Routinginformationen. Durch die Authentifizierung der Netzwerkteilnehmer und dank Überprüfung der Netzwerkinformationen ist ein Route Hijacking nicht mehr möglich. Sollte einmal ein Datenpaket einen anderen Weg nehmen, als der von der Source vorbestimmt wurde, so wird die Inkonsistenz durch die gegebene Transparenz umgehend festgestellt und verhindert. Die nachfolgend beschriebenen Services können grundsätzlich auf einem dedizierten System (z. B. VM) oder zusammen auf einem SCION Router betrieben werden. Für einen sicheren und solideren Betrieb, empfiehlt sich vor allem, aus Performancegründen im Providerumfeld eine physische Trennung der SCION Control Services vom Router. Innerhalb derselben ISD, beispielsweise auf den Border Routern bei Kunden, wird aufgrund der sicheren und logischen Serviceseparierung (Control und Data Plane) und unter normalen Performanceanforderungen keine physische Trennung empfohlen. Die ersten drei Server sind sogenannte Control Services und laufen bei der Schweizerischen Nationalbank (SNB), anders als wie bei der SIX, gemeinsam mit dem Border Router auf derselben Hardware Plattform. Dies hatte konzeptionelle Gründe, da SIX im SSFN ISD mehrere Aufgaben mit Schlüsselfunktionen wahrnimmt. Der nachfolgende Abschnitt verschafft darüber Klarheit. Für einen reibungslosen Betrieb sind noch weitere Komponenten, welche das Monitoring und Troubleshooting unterstützen notwendig und sehr empfohlen. Diese Komponenten sind nicht Teil der vorliegenden Arbeit und werden bewusst ausser Betracht gelassen. Bereits jetzt möchte für ein besseres Verständnis und zur realen Veranschaulichung der nachfolgenden SCION Service Funktionsbeschreibungen auf die Abbildung 1.3 verwiesen werden.

Bei der logischen Gruppierung von Autonomous Systems (ASs) zu einer ISD nimmt jedes AS gewisse Aufgaben und Verantwortungen wahr. Das Vertrauensverhältnis wird verteilt über mehrere ASes aufgebaut. Der wohl wichtigste Bereich, sozusagen das Herzstück von SCION, auf dem die ganze SCION Vertrauensstruktur und Sicherheit aufgebaut ist, wird im signierten TRC pro ISD definiert. Das TRC ist eine signierte Sammlung von X.509 v3 Zertifikaten und Richtlinien. Der formale Inhalt der TRC (Voting-, Issuing-, Core- und Authoritative-Members) wurde nach der Bestimmung der SSFN Governance[22] von der SSFN Association (SNB, SIX und zukünftige Finanzunternehmen) festgelegt. ASes mit mindestens einer Schlüsselrolle werden auch primäre ASes genannt und werden zusammen mit dem öffentlichen Schlüssel (Public Keys) und den Richtlinien (Policies) im TRC spezifiziert. Für das bessere Verständnis und vor allem, weil es einen sehr wichtigen Teil von SCION ist, werden die Schlüsselrollen kurz erklärt und ihre Zusammenhänge anhand der nachfolgenden Abbildung 1.1 veranschaulicht.

Voting Members sind grundsätzlich nicht am laufenden ISD-Betrieb beteiligt. Ihre Hauptaufgabe ist es das Erstellen und Aktualisieren der TRC. Es wird zwischen zwei TRC-Update-Schlüsseln unterschieden. Die Regular-TRC-Updates werden automatisch unter Verwendung von Online-Keys angestossen und sind für

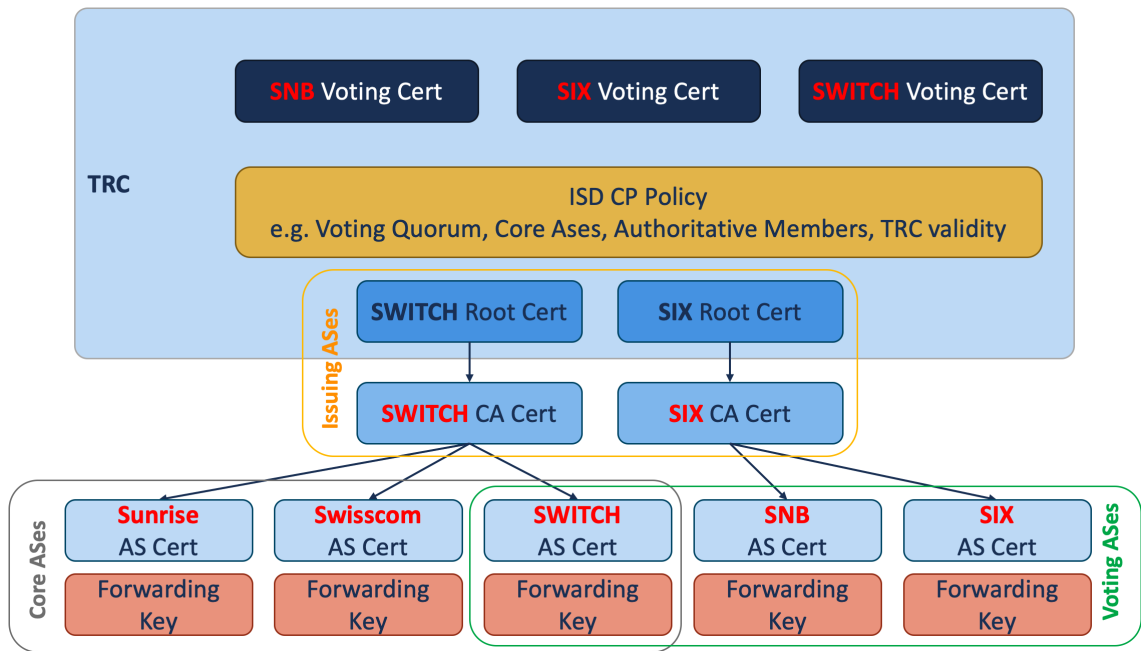


Abbildung 1.1.: SSFN Certificate Hierarchy / Trusted Root Configuration (nach [29])

unsensible Informationen wie Verlängerung der Gültigkeitsdauer oder Änderungen von Beschreibungen zuständig. Sensitive-TRC-Updates können nur mit Offline-Keys manuell ausgelöst werden. Wie es der Name andeutet, sind sie für sensible TRC-Updates zuständig. Über diese eher selten vorkommenden Updates können die Voting Members, das Voting Quorum oder die Root Certificates angepasst werden. Sensitive Voting Keys sind sicher zu verwahren.

Issuing Members (Certificate Authorities) stellen den ISD-Netzwerken die AS Zertifikate aus. Die AS Zertifikate werden für die Authentifizierungen der Netzwerkteilnehmer und für die Verifizierungen der Routing-Pfad- und Netzwerk-Informationen verwendet. Kommt ein neues ISD-Mitglied hinzu, muss er für das erste AS Zertifikat einen Zulassungsprozess durchlaufen. Aufgrund der sehr kurzen Lifetime geschieht danach eine Erneuerung der AS Zertifikate vollautomatisiert. Der Reissuing-Request wird immer mit dem noch gültigen AS Zertifikat authentisiert. Ohne die AS Zertifikate, findet keine Kommunikation im Netzwerk statt. Können über einen längeren Zeitraum, keine AS Zertifikate mehr ausgestellt werden, kann es unweigerlich zu Netzwerkausfällen führen. Die Issuing Members wie die SWITCH und SIX müssen daher einen hochverfügbaren Zertifikatsdienst bereitstellen. Das ist auch einer der Gründe, weshalb die Control Services bei der SIX auf dem Border Router betrieben werden.

Core Members oder Netzwerk Infrastructure Providers stellen die Netzwerkverbindung zu den Kunden und zwischen anderen Providern her. Innerhalb einer ISD definieren die Core ASes den ISD Core. Grundsätzlich sprechen wir hier über die Rolle eines klassischen ISPs mit den bekannten betrieblichen und gesetzlichen Aspekten. In unserem Fall stellen beispielsweise die ISPs Sunrise, Swisscom und SWITCH für sich und die Kunden eine hochverfügbare und hochperformante SCION Infrastruktur, mit den notwendigen Core Services und gewünschten Konnektivitäten von verschiedenster Datenübertragungsmethoden, zur Verfügung. Alle Pfadsegmente innerhalb einer ISD (intra-ISD-Routing) und ISD-übergreifend (inter-ISD-Routing) starten von den Core Members aus.

Authoritative Members müssen über die neusten Versionen aller Zertifikate und dem TRC verfügen. Aus Gründen der Erreichbarkeit und des Bootstrapping-Verfahrens muss ein autoritatives Mitglied auch ein Core Member sein und die zusätzliche Aufgabe übernehmen, um alle Anfragen nach Vertrauensmaterialien mit der neusten Version zu beantworten. Nur synchronisierte und autoritative ASes können Anfragen beantwor-

ten. So wird sichergestellt, dass alle massgebenden ASes über alle und neusten Zertifikate und TRCs verfügen und bei ihnen registriert sind. Aus Redundanzgründen sind mindestens zwei Mitglieder empfohlen. Alle ausgewählten ISPs sind im Normalfall gleich wichtig und geniessen das gleiche Vertrauensverhältnis, daher ist es meist sinnvoll, so wie in unserem Fall, alle ISPs zu autoritativen Mitgliedern zu definieren.

Wie angesprochen bestimmt und kontrolliert das Voting Quorum von ASes, welche Netzwerke dem ISD angehören. Jede TRC Version muss auch vom Quorum mit entsprechender Stimmberechtigung (Voting Power) unterzeichnet werden, damit die Aktualisierungen authentifiziert, validiert und umgesetzt werden können. In der Konzeptphase wurde entschieden, dass der Provider SWITCH und die SIX die wichtige Aufgabe eines Certificate Issuers wahrnehmen sollen. Wie in der Abbildung 1.1 ersichtlich, sind in der SSFN ISD zwei Certificate Authorities (CAs) vorhanden und werden einerseits vom Provider SWITCH und andererseits von der SIX betrieben. SWITCH bewirtschaftet für alle berechtigten Provider, und SIX für die berechtigten SSFN Finanzunternehmen, die AS Zertifikate. Jeder Netzwerkteilnehmer besitzt also ein eigenes AS Zertifikat. Die PKI in SCION stellt keine Certificate Revocation List (CRL) bereit, und daher müssen die Zertifikate eine kurze Lebensdauer aufweisen. Die SSFN Assosiation wählte die folgende Gültigkeitsdauer für die Root Zertifikate 1 Jahr, CA Zertifikate 1 Woche, und AS Zertifikate 3 Tage. Muss ein Zertifikat für ungültig erklärt werden, gibt es zwei Lösungsvarianten: Einerseits durch das Auslaufenlassen des Zertifikates oder durch den Austausch des Root Zertifikates im TRC. Bei einer Kompromittierung erlaubt der TRC-Verbreitungsmechanismus einen schnellen Widerruf und eine schnelle Erneuerung des Vertrauensstammes. Die Grösse des Quorums ist massgebend und sollte also immer grösser als eins sein, ansonsten ist das Vertrauenskonstrukt gefährdet. Darüber hinaus sind die privaten Schlüssel, mindestens von den Root und Voting Zertifikaten, sicher und vor Verlust, am besten in redundanten Hardware Security Modules (HSMs) geschützt und abgespeichert aufzubewahren.

Nach einem kurzen Ausflug in die essenziell wichtige SCION Vertrauensstruktur wieder zurück zu den zu untersuchenden Core Services. Die Control Plane ist vereinfacht gesagt grundsätzlich für das Routing zuständig. Sie erstellt und verwaltet die Pfadsegmente (Path Segments), die zu Weiterleitungspfaden (Forwarding Paths) kombiniert werden können. Alle drei Funktionen (Beacon-, Path- und Certificate-Server) sind in einem Control Service implementiert. Für das zustandslose und effiziente Packet Forwarding sind die Internal und Border Router zuständig. Internal Routers leiten lediglich die Pakete innerhalb eines AS weiter, und die Border Router verbinden unterschiedliche ASes zur Weiterleitung der Pakete miteinander. Durch regelmässige Keep-Alive-Messages¹ werden Link- oder Schnittstellen-Ausfälle zu benachbarten ASes durch den Beacon Server registriert. Bei einem solchen Fehler reagiert der Beacon Server umgehend, indem er das Path Segment zurückzieht und falls vorhanden ein Neues registriert. Über die Ungültigkeit eines Pfades informiert ein Router den Sender mittels dem SCION Control Message Protocol (SCMP). Die Data Plane (DP) ist nicht nur für die reine Datenpaketweiterleitung zuständig, sondern kombiniert auch die Path Segmente zu Forwarding Paths und stellt die Integrität der Hop Fields (HFs) sicher. Der AntiSpoofing-Mechanismus, durch Überprüfung des eingehenden Interfaces, findet zusätzlich bei jedem eingehenden Datenpaket statt. Durch die HF-Integrität werden Fälschungen oder Veränderungen der HFs verhindert. Das Überprüfen von Signaturen benötigt Zeit und würde die Effizienz der Data Plane behindern. Der Message Authentication Code (MAC) wird über die einzelnen Paketweiterleitungsinformationen im HF generiert und für die schnelle Paketweiterleitung benutzt. Für die Berechnung des MACs besitzt jedes AS seinen eigenen geheimen, symmetrischen Schlüssel (AS Forwarding Key). Das Local Secret kennen die Beacon Server und Border Router nur im jeweiligen AS und wird nicht unter den ASes weiterverbreitet. So wird die Paketweiterleitung massiv beschleunigt und die Korrektheit des Pfades sichergestellt. Ein weiterer Vorteil ist, dass jedes AS unabhängig und einfach von den benachbarten ASes seine Schlüssel

¹Die Keep-Alives werden in zukünftigen Releases mit Hilfe des bewährten Protokolls Bidirectional Forwarding Detection (BFD) zwischen benachbarten Border Router sichergestellt.

und kryptographischen Methoden aktualisieren kann. Anders als beim BGP-Routingprotokoll benötigt die Paketweiterleitung keinen Routing Lookup mehr, da der Forwarding Path, vor der Versendung des ersten Datenpaketes, verifiziert und bekannt ist.

Für die Paketweiterleitung werden immer Routinginformationen (Path Information) benötigt. Ausgehend vom ISD Core ist der Beaconing-Prozess für die periodische Erzeugung, Vermehrung, Weiterleitung und Empfang der Path-Segment Construction Beacons (PCBs) verantwortlich. Durch diese PCBs werden die Path Segments eruiert und enthalten Topologie- und Authentifizierungsinformationen, sowie Metadaten zur Unterstützung beim Pfadmanagement und der Pfadauswahl. SCION unterscheidet zwischen zwei Beaconing-Prozessen: Das intra-ISD-Beaconing erzeugt die Path Segments innerhalb der ISD, ausgehend von den Core ASes zu den non-Core ASes. Das inter-ISD-Beaconing erzeugt die Path Segments innerhalb des ISD Cores, zwischen den Core ASes und ISD übergreifend zwischen fremden ISDs.

Wichtig in diesem Zusammenhang ist zu wissen, dass es drei Typen von Path Segments gibt, und sie für die Datenkommunikation bidirektional verwendet werden können:

- * Ein Path Segment zwischen Core ASes ist ein Core-Segment.
- * Ein Path Segment von einem Core AS zu einem non-Core AS ist ein Down-Segment.
- * Ein Path Segment von einem non-Core AS zu einem Core AS ist ein Up-Segment.

Auf der Reise durch das Netzwerk sammeln die Beacons kryptografisch geschützt, schrittweise alle notwendigen Inter- und Intra-ISD-Routing-Pfadinformationen. Erhält ein eingehender Border Router eines Downstream-AS ein PCB-Paket mit einer SCION Service Address (SVC)², so leitet er es zu einem seiner **Beacon Server** weiter. Bei jedem eingehenden AS fügt der Beacon Server vor der Weiterleitung gewisse Informationen, wie z. B. das sogenannten HF, gestapelt zum PCB hinzu, signiert es mit seinem AS Schlüssel und leitet es zu seinem benachbarten AS weiter. Dieses Konzept wird als Packet-Carried Forwarding State (PCFS) bezeichnet. Welche Informationen auf AS-Ebene (AS Entry) hinzugefügt werden, sehen sie in der nachfolgenden Auflistung:

- + Metadata
 - ISD-AS Identifiers
 - TRCVersion
 - CertVersion
 - IFSsize
 - Maximum Transmission Unit (MTU)
- + Hop Field (Packet Forwarding Information)
 - Flags
 - Expiration Time
 - Link Identifiers (Ingress and Egress Interfaces)
 - Message Authentication Code (MAC)

²Die Serviceadresse (SVC) wird verwendet, um den gewünschten SCION-Dienst/Applikation anzusprechen. Intra-AS Control Plane Messages z. B. für das Beaconing, die Path Registration oder den Certificate Request etc. finden über das Transportprotokoll TCP/IP statt. Inter-AS Control Plane Messages verwenden das experimentelle Netzwerkprotokoll SCION/QUIC. Für detailliertere Informationen möchte auf das SCION-Buch verwiesen werden.

- + RevocationToken
- + Extensions (Optional)
- + AS Signature (AS Certificate)

Trifft nun ein PCB-Paket beim Beacon Server ein, wird umgehend die PCB-Paketstruktur und die Signatur überprüft. Zum Beispiel fordert er bei einer Nichtübereinstimmung der TRC- oder Zertifikat-Version umgehend ein Update beim Upstream-Beacon Server an. Erst bei einer Übereinstimmung leitet er die TRCs und Zertifikate zu seinem Certificate Server weiter und trägt die Pfadinformationen in die lokale Datenbank (Cache) ein. Die lokale Datenbank wird auch Beacon Store genannt. Aus dem Beacon Store werden schliesslich die zwischengespeicherten PCBs modifiziert, signiert und zu Path Segments aufbereitet. Nach der Aufbereitung werden die Up-Segments im Lokalen und die Down-Segments im Core **Path Server**, durch senden an den Path Registration Service, registriert. Wird bei der Pfadregistrierung festgestellt, dass die Path Segments mit einer anderen neueren TRC-Version authentifiziert wurden, fragen die Path Server den Beacon Server nach der aktuellen TRC-Version ab. Erst nach Erhalt der neuen TRC-Version können die neuen Path Segments verifiziert und registriert werden. Der Beacon Server wählt anhand der lokalen AS-Policy und Datenbank die besten PCBs und setzt seine Pfadsuche periodisch zu seinen Downstream-ASes fort. Die vom Beacon Server bereitgestellten Pfadinformationen (Zuordnung von AS-IDs zu Gruppen angehöriger Path Segments) sind im Path Server Cache hierarchisch organisiert und verwaltet. Die Beacon-Server in einem AS wählen die Down-Segments aus, über die die Downstream-ASes erreicht werden sollen. Diese Pfadsegmente enthalten Informationen von einem Core AS zu einem non-Core AS und werden dem Core Path Server zurückgemeldet und registriert. Wird ein Pfad von einem Beacon Server für ungültig erklärt, erfolgt umgehend eine Rückmeldung (Path Revocation with a new set of Up- or Down-Segments) zu den Path Servern (Local and Core) und zu allen im AS befindlichen Border Router. In diesem Zusammenhang unterstützt das RevocationToken, innerhalb des PCBs, für einen authentifizierten Widerruf einer Schnittstelle im Path Segment. Alle anderen Komponenten, so wie der Path Server und der Border Router, verwenden für die Path Revocation das SCMP³. Im Revocation Prozess übernimmt der **Border Router**, je nach Situation zur Signalisierung, gewisse Aufgaben. Er generiert falls notwendig oder leitet SCMP Revocation Packets zu den Source- oder Destination-Hosts und/oder zum lokalen Path- und Beacon-Server weiter. Die Path Server nehmen die Revocation Messages entgegen, überprüfen sie und bei Übereinstimmung entfernt er seine korrespondierenden Path Segments aus dem Cache. Der Beacon Server erhält die SCMP Pakete zur Verhinderung von der Verbreitung fehlgeschlagener Links. Zur Kommunikation benötigen die Endhosts untereinander einen kompletten End-to-End-Path, der zum Weiterleiten der Pakete zum Zielsystem erforderlich ist. Die erforderlichen Pfadsegmente werden von den Endsystemen mittels Path-Lookup beim lokalen Path Server abgerufen und dem Ziel entsprechend kombiniert. Die Endsysteme können grundsätzlich selbst entscheiden, über welche Wege die Datenverbindung aufgebaut wird. Sollte ein lokaler Path Server das benötigte Path Segment nicht im Cache haben, so sendet er einen Request zum lokalen Core Path Server. Ist das Path Segment auch nicht in diesem Cache vorzufinden, dann kontaktiert dieser die Remote Core Path Server. Schliesslich erhält der Source Host vom Path Server die Path Segments zurück. Befinden sich die Kommunikationspartner z. B. in unterschiedlichen ISDs, können unter diesen Umständen alle drei Typen Up-, Down- und Core-Segments als Antwort zurückgegeben werden. Die gelernten Path Segments legt der lokale Path Server im Cache zur Wiederverwendung ab. Das Zielsystem antwortet, indem es den End-to-End-Path aus dem Paket-Header invertiert oder seinen eigenen Pfad sucht und verwendet. Grundsätzlich sind die Pfadinformationen bidirektional, aber das bedeutet nicht, dass das Zielsystem auch wieder

³SCMP kann mit dem ICMP-Protokoll verglichen werden. In SCION wird es hauptsächlich für die Netzwerkd Diagnose (analog zu Ping und Traceroute) und die Problemsignalisierung in der Paketverbreitung auf Netzwerkebene verwendet.

auf demselben Rückweg antworten muss. Anders als bei IP, enthalten die über das Netzwerk gesendeten Datenpakete, bereits die Routinginformationen auf AS-Ebene. So können sie direkt über die gewünschte AS-Sequenz vom Border Router weitergeleitet werden. Durch die AS-Tabellen wird eine effizientere, zustandslose Weiterleitung erreicht. Das PCFS-Konzept ermöglicht mit der Nutzung des OPT-Protokolls⁴ (Origin and Path Trace) und seinen Mechanismen, nicht nur die Source Authentifizierung, sondern auch die Path Validation. Damit können Sender, Empfänger und Router den Pfad, den das Datenpaket durchlaufen hatte, kryptographisch überprüfen. Nur unter Anwendung des DRKey-Mechanismus können Router ihren Schlüssel effizient ableiten, im Path Validation Field (PVF) aktualisieren und die Pfadüberprüfung umsetzen. Es ermöglicht den Endhosts, die Pfadkonformität gemäss ihrer Pfadauswahl zu erzwingen, und darüber hinaus wird ein schneller und zustandsloser Betrieb auf Routern erreicht. Bisher wurde der **Certificate Server** in seiner entscheidenden Rolle etwas vernachlässigt. Er zwischenspeichert die vom ISD Core abgerufenen Trust Root Configurations (TRC), speichert die eigenen AS-Zertifikate als Kopie und verwaltet die kryptografischen Schlüssel und Zertifikate für die Intra- und Inter-AS-Kommunikation. Vereinfacht gesagt, verwaltet und aktualisiert der lokale Certificate Server (Trust Store) die für den lokalen AS-Betrieb notwendigen Schlüsselmaterialien und stellt diese den Control Services bereit. Die AS Zertifikatserneuerung läuft automatisch im Hintergrund ab, aber ein Rückzug von AS Zertifikaten ist eine heikle Sache und kann einen direkten Einfluss auf die Produktion haben. Die Beacon Server rufen den Zertifikatsserver ab, um die Authentizität der PCBs zu überprüfen und zu gewährleisten. Wie angesprochen ist in der initialen Aufnahme eines AS einen manuellen Prozess vorgesehen, und es gibt in SCION keine AS Certificate Revocation List. Wir können im Netzwerk, in allen möglichen Fällen, keine unauthentifizierte Path Segments tolerieren. Aus diesem Grund muss eine kurze Lebensdauer von 3 Tagen bei solchen Zertifikaten toleriert werden. Wie bestimmt bemerkt, war bisher nur die Rede über das intra-ISD-Beaconing. Das inter-ISD-Beaconing läuft nur mit wenigen Unterschieden sehr ähnlich ab. Im ISD Core wird keine hierarchische Struktur, sondern meist eine Fully Meshed AS Topologie aufgebaut. Durch die ISD-Core-Topologie-Flutung mit PCBs können identische PCBs mehrfach am selben Ort auftreten. Daher benötigt es in diesem Core-Segment-Evaluation-Prozess, seitens Core Beacon Server, eine Loop Prevention auf AS- und ISD-Ebene. Die Core PCBs sind nur im ISD Cores aufzufinden und die vom Core Beacon Server aufbereiteten Core Segmente werden nur in den Core Path Servern registriert. Innerhalb der jeweiligen ASes wird, durch die Bildung eines Clusters über mehreren Core Services, für Redundanz gesorgt. Von minimal drei Nodes⁵ verkörpert einer die Master-Funktion, und die anderen gelten als Followers. Der Master-Node ist für die Replikation der Datenbank und die Koordination verschiedenster Aufgaben, wie das Beaconing und die Path Registration, unter den Mitgliedern zuständig. Nur innerhalb des ISD-Cores findet unter den Core ASes eine Synchronisation von Pfadinformationen und Schlüsselmaterialien statt. Eine Synchronisation unter non-Core-ASes gibt es demnach nicht, und alle fehlenden Informationen müssen über den ISD-Core bezogen werden. Mit der vorangegangenen kurzen Einführung wurden die wichtigsten SCION Services mit ihren Funktionen verdeutlicht. Die Grundlagen für einen vereinfachten Einstieg und das bessere Verständnis in die nachfolgenden Themenschwerpunkte und Kapiteln ist somit gegeben. Nebst dem SCION-Buch möchte für detailliertere Informationen zusätzlich auf die öffentlich erhältliche und umfangreiche Literatur auf GitHub^{6,7} oder Anapaya.net⁸ verwiesen werden.

⁴Das OPT wurde in der Forschung einst theoretisch beschrieben und wird voraussichtlich durch das EPIC-Protokoll[35] ersetzt. Es befindet sich im Forschungsstadium, daher existiert in SCION noch keine Path Validation.

⁵Ein High Availability Control Service Cluster kann in ungeraden Schritten hoch skaliert werden. Für einen HA-CS-Cluster benötigt es jedoch mindestens drei Members.

⁶<https://github.com/scionproto/scion>

⁷<https://github.com/netsec-ethz/scion-apps>

⁸<https://scion.docs.anapaya.net>

1.2. Problemstellung

Angesichts der Geschwindigkeit der technologischen Neuerungen ist der Wandel nicht zu stoppen und es benötigt dringend Handlungsbedarf. Die technologischen Innovationen sind so spannend wie nie zuvor! Die Gesellschaft wurde vom Internet stark abhängig und ist auf eine robuste, stets verfügbare, verlässliche und vertrauenswürdige Infrastruktur angewiesen. SCION als mögliche revolutionäre Secure Internet Architecture schreibt und lebt das Prinzip „Security by Design“ vor[62]. Daher wird bereits bei der Softwareentwicklung auf einen sehr hohen Sicherheitsstandard gelegt. Seit Beginn wird in der Forschung und Entwicklung des SCION Quellcodes mit bekannten und ausgewiesenen Techniken und Methoden auf Schwachstellen geprüft. Es entstanden diesbezüglich auch einige Arbeiten von Studenten an der ETH Zürich. Genau bei diesem Punkt setzt die vorliegende Masterarbeit an und rundet das genannte Prinzip ab.

Bevor in den Hauptteil der vorliegenden Arbeit eingetaucht wird, werden im nachfolgenden Kapitel 2 „Forschungsstand“, kurz aus Vollständigkeitszwecken, der Werdegang und der aktuelle Fortschritt von SCION umrissen. Darauf folgt eine kommentierte Auflistung der wichtigsten konkurrierende resp. andere mögliche Lösungsvorschläge, aus der internationalen und anerkannten Wissenschaft. Das heisst, es wird versucht die Themenschwerpunkte von zukünftigen Technologien oder Netzwerkarchitekturen herzuleiten, um aufzuzeigen wo der jeweilige Fokus der zu lösenden Problemstellungen liegt. Bei der Betrachtung wird besonders Wert auf die Sicherheit und den Datenschutz auf der Ebene Netzwerkschicht gelegt. Das Ziel ist keine Studie von möglichen Umgehungslösungen, Optimierungen, Technologien oder zukünftigen Internet Architekturen zu betreiben. Das würde den Rahmen der Masterarbeit sprengen und vor allem das Hauptziel der Masterarbeit verfehlen. Die Recherche wird sich daher auf die IEEE Datenbank[2][14], die bereits getätigten Nachforschungen von Adrian Perrig zu Future Internet Projects[51] und der frei verfügbaren Wissensdatenbank dem Internet beschränkt. Als einleitende Abrundung wird zu guter Letzt aus Sicht des Autors erklärt, weshalb zukünftig in SCION weiter investiert werden soll, und es die zu bevorzugende, sowie vermeintlich beste zukünftige Internet Architektur sein wird.

Wie sicher oder widerstandsfähig ist ein IT-System ohne umfassende Sicherheitstests gegen Cyberangriffe? Die Antwort ergibt sich vermutlich von selbst und betrifft selbstverständlich auch die auf dem System laufenden SCION Services, trotz den sehr hohen Sicherheitseigenschaften per Design. Die SCION Services sind auf etlichen Hardware Plattformen und virtuellen Umgebungen voll funktionsfähig. In der Industrie werden sie auf anerkannten Linux-Distribution wie Ubuntu und RedHat betrieben. Mit dem Fokus auf zwei nahezu unterschiedlichen Themengebieten „Cyber Security“ und „Computer Forensics“ verfolgt die vorliegende Thesis ein ganzheitliches SCION Security Framework. Beide Themengebiete konzentrieren sich auf den Schutz digitaler Assets und Informationen. In der Tat ist es hilfreich, sich Cybersicherheit und Computerforensik, als zwei wesentliche Seiten derselben Medaille vorzustellen. Die Arbeit, die sie leisten, ist sehr ähnlich, unterscheidet sich jedoch in einigen wesentlichen Punkten: Bei der Cybersicherheit geht es um Prävention und bei der Computerforensik um Reaktion. Das ist genau der Grund, weshalb wir hier beide Bereiche behandeln und die sicherheitsrelevanten und forensischen Aspekten sowie Fragestellungen theoretisch grundlegend aufarbeiten. Andererseits findet in einem praktischen Teil eine vollautomatische und menügesteuerte Überprüfung der unerlässlichen Sicherheitschecks statt. Die Abbildung 1.2 veranschaulicht bildlich die Themeninhalte. Als Kern stehen die zu schützenden SCION Services hervor. Umkreist werden sie einerseits von drei präventiven Cyber Security Massnahmen und andererseits von der gesamtheitlichen Computer Forensics zur Identifizierung und Reaktion auf Cybersicherheitsverletzungen nach bereits stattgefunden Angriffen. Die beiden Themengebiete „Cyber Security“ und „Computer Forensics“ sind bekanntlich weitaus komplexer und umfangreicher als geschildert und abgebildet. Es wird und kann daher kein umfassendes und abschliessendes Cyber Security and Forensics Framework entstehen. SCION wird bereits in der Industrie eingesetzt und bezüglich Cyber Security sind vor allem die aufgezeigten drei Schwerpunkte

gefordert. Computer Forensics ist für SCION noch ein Fremdwort und in der Industrie momentan noch „Nice to Have“ resp. besteht noch kein dringender Bedarf. Deshalb finden vorerst grundlegende, forensische Betrachtungen statt. Weiterführende Arbeiten in zukünftigen Forschungsarbeiten sind gewünscht, sollen berücksichtigt und gefördert werden.

Gestartet wird mit dem in der Abbildung 1.2, der grün gekennzeichneten Bereich, bei der fundamentalen und wichtigen Basis der System- und Betriebssystemsicherheit. Standardmässig „Out of the Box“ sind Linux Server Betriebssysteme nicht optimal gehärtet. Die Angriffsfläche und die Verwundbarkeit der SCION Services muss auf das Minimale reduziert werden. Das Härten des Host-Betriebssystems, z. B. durch Reduzieren der Anzahl verfügbarer Dienste, also auf das Nötigste minimiert, in dem nur die Container-Laufzeit, Host-Sicherheitskontrollen und Überwachungsanwendungen laufen, ist entscheidend für den Sicherheitserfolg. Nur so können mittels den notwendigen Leitlinienempfehlungen die Kontrollen und Konfigurationsgrundlagen abgeleitet werden. Die daraus resultierenden best-practices Benchmarks garantieren ein optimal gehärtetes Betriebssystem zum Schutz der SCION Services und der kompletten Infrastruktur als Basis. Es entsteht quasi ein **Secured SCION Host OS Image**.

Auf dem gehärteten Betriebssystem werden danach die benötigten SCION Services installiert und betrieben. Im nächsten Schritt, das ist in der Abbildung 1.2 der blaue Bereich, werden die sicheren Installationen, Konfigurationen und Funktionen der SCION Services validiert. Die Services laufen grundsätzlich immer virtualisiert in einem vom Betriebssystem mehr oder weniger abgeschotteten und geschützten Docker Container. Mit Docker kann SCION relativ schnell auf eine sichere, vereinfachte und standardisierte Art und Weise in unterschiedlichen Infrastrukturen bereitgestellt werden. Die Technologie bringt viele Vorteilen und auf der Gegenseite sind trotzdem gewisse Sicherheitsmassnahmen erforderlich. Insbesondere die fehlende Isolation zwischen Host und Container bereitet Kopfschmerzen. Container teilen sich die Ressourcen mit dem Host und haben somit direkten Zugriff auf den Host-Linux-Kernel. Hier gilt es anzusetzen, um zusätzliche Schutzmauern, ähnlich wie auf einem komplett virtualisierten System, zu errichten.



Abbildung 1.2.: Thesisinhaltsübersicht - SCION Security and Forensics Framework

Ein potenzieller Angreifer wird gezwungen mehrere Hürden zu überwinden. Mit der Härtung des Host-Systems vergleichbar, wird an dieser Stelle in Bezug auf die Dockerisierung der SCION Services in Sicherheitsbelangen notwendigen und angemessenen Richtlinien festgelegt und auf eine sichere Implementation geprüft. Nur so kann eine mögliche Kompromittierung des SCION Services oder im Umkehrschluss des Host-Systems im weiteren Sinne, verhindert werden. Ein weiteres wichtiges Sicherheitsmerkmal entsteht

und der Aufstieg auf ein höheres Sicherheitsniveau, zur sogenannten **Secured SCION Platform**, wird erreicht. Nur am Rande erwähnt, in der SIX werden solche Hardening Guidelines in einem Secure Configuration Baseline (SCB) Dokument festgehalten und jährlich rezertifiziert. Bevor SCION produktiv geschaltet wird, muss auch dafür ein entsprechendes SCB Dokument mindestens im Draft-Status vorhanden und von der Security Architecture, sowie Corporate Security abgenommen sein.

Nachdem die zwei essenziell wichtigen und elementaren Bausteine bezüglich Plattform Vulnerability Assessment eine sichere Grundlage für die SCION Service sicherstellen, werden im letzten Themenbereich von „Cyber Security“ die eigentlichen SCION Services auf mögliche Schwachstellen getestet. Das betrifft in der Abbildung 1.2 der orange Themenbereich. Die auszuarbeitenden Tests werden nach den üblichen Techniken und Ansätzen, wie man sie vom Black und White Box Testing her kennt, durchgeführt. Zu diesem Themengebiet entstanden bereits an der ETH Zürich einige Bachelorarbeiten und bei Anapaya Systems AG fanden einige Überlegungen statt. Daher werden im Vorfeld zuerst eine Begutachtung und Auswertung der bestehenden Arbeiten und Überlegungen stattfinden. Zusätzlich mit der Unterstützung und dem Insiderwissen der SCION Entwickler werden die bestehenden Testsysteme weiter ausgearbeitet, und dadurch die Prüfsicherheit verbessert. Ausgehend von den zusätzlichen formalen oder informalen Spezifikationen werden neue Testfälle erarbeitet, die sicherstellen, dass der geforderte SCION Funktionsumfang eingehalten wird. Das zu testende SCION System wird dabei als Ganzes betrachtet, nur sein Aussenverhalten wird bei den Black Box Tests (Behavior Testing) zur Bewertung der Testergebnisse herangezogen. Das SCION System wird also mit unterschiedlichen Traffic Pattern (Fuzzing Traffic) auf unterschiedlichen Layern konfrontiert und auf korrektes Verhalten ausgewertet. In Kombination mit den White Box Tests (Logical Testing) kann die Korrektheit des SCION Systems selbst mit einer höheren Überdeckung garantiert werden. Diesbezüglich konnte an der Universität und während der Entwicklung schon relativ viel Forschung betrieben werden. Hinsichtlich der bereits getätigten Forschung, dem einflussenden Insiderwissen und den zur Verfügung stehenden Mitteln der Cyber-Kriminellen, steht das Black Box Testing klar im Vordergrund. Das Penetration Testing macht die Schwächen transparent oder untermauert die Widerstandsfähigkeit der SCION Services. Die nächste Sicherheitsstufe **Secured SCION Services** wird erreicht. Der direkte Bezug zur Industrie wurde dargelegt und zeigte die fehlende Notwendigkeit auf. Primär in grossen und namhaften Unternehmen wie bei der SIX sind auch Penetrationstests nicht wegzudenken und oft vor Inbetriebnahme gefordert. In der damaligen SSFN PoC Phase fanden bei Anapaya Systems AG und SIX, durch externe und unabhängige Partner, einige derartige Sicherheitstests statt. Auffallend sind hinsichtlich der Bedeutsamkeit auch die bereits getätigten grossen Anstrengungen. Darum ist dieser Themenbereich in dieser Arbeit optional anzusehen und in einer weiterführenden Arbeit weiterzuverfolgen.

Nach der Ausarbeitung und Festlegung der erwähnten Leitlinienempfehlungen (SCION Security Benchmarks) entsteht, bildlich gesprochen, ein Werkzeugkasten in Form einer Auditing-Anwendung, die über ein Menü oder ähnliches je nach Auswahl automatisiert die gewünschten Sicherheitsüberprüfungen durchführt und bewertet. Mit diesem Tool kann künftig eine sicherere SCION Service Integration, immer nach einem Entwicklungszyklus oder vor der SCION Service Inbetriebnahme beim Kunden oder Internet Service Provider (ISP), gewährleistet werden. Alle Finanzdienstleister wie SIX unterstehen verschiedenen Regularien der Finanzmarktaufsichtsbehörde FINMA. Wir müssen für unsere geschäftlichen Tätigkeiten zusätzlich vielzählige Vorgaben seitens PCI-DSS[50] und SWIFT[59] erfüllen, darum wird eine wiederkehrende Ausführung in halbjährlichen Zyklen gefordert. Kommt eine Vorgabe nicht von externer Natur, so wird sie meist aus der internen IT Governance gefordert. Diskussionslos untersteht die Toolsuite fortan unter lebenslanger Wartung. Nach jeder Änderung an dem Betriebssystem, den Dienstprogrammen, dem SCION Quellcode und/oder beim Bekanntwerden von relevanten Sicherheitslücken (Vulnerabilities), muss das Framework entsprechend justiert oder erweitert werden.

Abschliessend beschäftigen wir uns mit einem Zweig aus der forensischen Wissenschaft. Sie umfasst die

Wiederherstellung und Untersuchung von digitalen Daten auf deren Spuren. Häufig findet eine Analyse der Computersysteme im Zusammenhang mit Cyberkriminalität statt. Die forensischen Analysen finden nach anerkannten, wissenschaftlichen Prinzipien statt. In einer ganzheitlichen Betrachtungsweise, wie im violetten Ring in der Abbildung 1.2 hervorgehoben, nähern wir uns den von SCION verursachten Spuren im Dateisystem. Das Hauptziel von **SCION Forensics** ist eine gründliche Aufarbeitung der Spurenbilder, beginnend beim nativen Linux Image (Ubuntu oder Red Hat). Einerseits sind die Spurenbilder, die der Entwickler bei der Systemaufbereitung verursacht hat, sehr von Interesse und andererseits die verursachten Spuren der SCION Services. An diesem Punkt gilt es sich exakt abzugrenzen und den Umfang zu definieren. Es ist wichtig festzuhalten, welche Spuren in welchem Systemzustand, eruiert wurden. Jede Aktion verursacht viele Änderungen im Dateisystem. Ausgeführte Aktionen in einer anderen Reihenfolge können das Spurenbild komplett ändern. Im Nachgang ist es praktisch nicht mehr möglich festzustellen und eine sichere Aussage zu treffen, welche Artefakte nun von welcher Aktion verursacht wurden. Damit ein sinnvoller und begründeter Aktionsumfang hergeleitet und bestimmt werden kann, benötigen wir entsprechendes Fachwissen aus der Industrie. Dafür wird ein SCION Entwickler und einen System Integrator beigezogen, da nur sie die von ihnen getätigten Interaktionen aufzeigen können. In diesem Abschnitt beschränken wir uns vorerst auf die grundlegenden Installationen und Konfigurationen, bis ein SCION Service in Betrieb genommen werden kann. Wie angesprochen, gehört ein solides SCION Fachwissen und eine forensische Wissensdatenbank für eine Spurenanalyse zu den essenziell wichtigen Vorkenntnissen nach einem möglichen Sicherheitsvorfall. Es hilft, vereinfacht und beschleunigt eine Untersuchung beträchtlich. Mit dem Einsatz von diesem Framework kann eine sauberere und sicherere Integration im Entwicklungszyklus und vor der Inbetriebnahme beim Kunden vor Ort gewährleistet werden.

Für die forensischen Analysen kommen aufgrund der Glaubwürdigkeit und vereinfachten Wiederholbarkeit mehrere gesonderte Anwendungen zum Einsatz. Die verwendeten Open Source Tools sind wissenschaftlich anerkannt und die selbst entwickelten Anwendungen erprobt. Die erfassten Daten können nur so für die Herleitungen und Hypothesen verlässlich und effizient aufbereitet werden. Des weiteren lassen sie sich bei den Kunden relativ zügig und unkompliziert nach einem möglichen Sicherheitsvorfall wiederverwenden. Nach jedem SCION Release Cycle untersteht die forensische Wissensdatenbank faktisch einer wiederkehrenden Justierung.

1.3. Aufbau der Arbeit

Als Schweizer Finanzinstitut legen wir einen sehr hohen Stellenwert an die Informations- und Datensicherheit. Wir schützen unsere vertraulichen Kundendaten stets mit höchster Priorität, aktuellen und anerkannten Methoden, angemessenen Mitteln, sowie innovativer und ausgereifter Technik. Aus diesem Grund führt SIX vor dem Einsatz neuester Technologien eine Marktanalyse, siehe dafür auch Kapitel 2 „Forschungsstand“, mit dazugehöriger Bewertung durch. Die Bewertung wurde im Vorfeld seitens Network Security Architecture und dem SSFN Projektteam gemacht, und ist nicht Inhalt der vorliegenden Arbeit. Bei der Bewertung werden, wenn immer möglich, die zukünftigen Anforderungen aller SIX Divisionen mit angemessenen Kompromissen miteinbezogen. Je nachdem, wie das Kosten- und Nutzen-Verhältnis ausfällt, findet nur eine informelle Beurteilung oder ein Proof of Concept (PoC) statt. Übersteht einer von den maximal drei Produkten oder Technologien die Bewertung oder den PoC, wird wie in unserem aktuellen Fall von SCION in die Pilot-Phase übergegangen und unter realen Bedingungen getestet. In der relativ langen Pilot-Phase kann und darf es zu laufenden Korrekturen und Erweiterungen kommen. Schliesslich geben die Geschäftsbereiche und Sicherheitsorganisation den Takt an und geben die Infrastruktur bei genügender Marktreife für die Produktion frei.

Zum Schutz der Infrastruktur setzt SIX auf Richtlinien aus der Industrie, die von einer globalen Community mit Cybersicherheitsexperten kommen. Wir halten uns, wenn immer möglich, an die weltweit anerkannten CIS Empfehlungen⁹. Darauf aufbauend kommt eine Reihe von obligatorischen und beratender PCI-DSS und SWIFT Sicherheitskontrollen und bewährte Methoden für die ganze SIX Infrastruktur dazu. Auch die SWIFT Controls bauen auf drei internationalen Security Frameworks auf und können je nach Vorgabe dem Industriestandard NIST, ISO/IEC 27002 und PCI-DSS zugeordnet werden. Es kann immer wieder zu Ausnahmesituationen kommen oder Hersteller geben, für die es keine CIS Benchmarks gibt, oder wir die Anforderungen nicht direkt oder optimal umsetzen können. Üblicherweise greifen wir in solchen Fällen, falls vorhanden, zu best-practice Vorgaben seitens Hersteller oder ziehen Empfehlungen von unseren externen Cybersicherheitsberater bei. Die Auditoren begrüßen und schätzen diese Methode sehr, denn jegliche Abweichungen werden detailliert begründet dokumentiert.

Vor allem in Anlehnung an die erwähnten und öffentlich erhältlichen Richtlinien und unseren SIX spezifischen SCBs werden im Kapitel 5 „Anapaya - Appliance OS Security“ auf SCION ausgerichtete Benchmarks erarbeitet. Nur auf SCION angepasste spezifische Kontrollen verkleinern die Angriffsfläche und schützen so das Betriebssystem, die Software und das Netzwerk effizient vor allfälligen Schwächen gegen Cyber-Angriffe. Die Umsetzung der Sicherheitsempfehlungen auf dem untersten Level bereiten vor allem den Host-Computer vor, um eine solide und sichere Ausführung von den containerisierten SCION Workloads zu ermöglichen.

Bekanntlich machen die Docker Container die virtuellen Maschinen (VM) nicht obsolet, da VMs eine höhere Isolationssicherheit besitzen. Mit erhöhtem Schutzbedarf folgen im Kapitel 6 „Docker Security“ die weiterführenden Sicherheitsempfehlungen und -kontrollen mit direktem Bezug auf die einzelnen SCION Services. Zusätzlich zu den Docker Security Leitlinien gehören, nach der Definierung der Ausgangslage, also mit welchen Installationskombinationen bezüglich SCION auf dem System zu rechnen sind, weiterführende und angepasste Sicherheitsmassnahmen. Ausschliesslich mit den SCION spezifischen Eigenschaften ist es möglich weitere Sicherheitskontrollen zu spezifizieren. Die Transparenzschaffung über eine Art von Kommunikations- und Schnittstellenmatrix sowie den Dateisystemabhängigkeiten macht erst eine Aufzeichnung aller Interaktionen und Beziehungen zwischen dem Host OS und den SCION Services möglich. Nicht nur die Prozess- und Dateisystem-Berechtigungen sind sicherheitsrelevante Metriken. Auch eine auf das nötige begrenzte SCION Konfiguration ist sowohl für die einwandfreie Funktion, als auch für eine erhöhte Sicherheit relevant.

Wie angesprochen werden in der Praxis unter Kapitel „App Security“ im Sinne von einem Penetrationstest, die Widerstandsfähigkeit und Sicherheit vom SCION System durch simulierte Angriffe bewertet. Je nach Bedarf gibt es grundsätzlich zwei Blickwinkel von Penetrationstests. Der interne Test zeigt Risiken aus Sicht eines internen Mitarbeiters und der externen eines Hackers. Unter Berücksichtigung bestimmter und ausgerichteten Methoden, mit bewusstem Sichtfeld eines potentiellen externen Hackers, werden die bestehenden Testsysteme weiter ausgearbeitet. Bei der Identifizierung von möglichen Bedrohungen oder Schwachstellen, können sie dann gegebenenfalls weiter analysiert und durch Quellcodeanpassungen gezielt eliminiert werden. Ein Penetrationstest kann grosse Risiken bergen und schwerwiegende Folgen für das Netzwerk haben. Wenn er schlecht oder unachtsam ausgeführt wird, kann der Versuch die Sicherheitslücken aufzufinden zur Überlastung oder Systemabstürzen führen. Im schlimmsten Fall, kann auch gerade das Auffinden einer Lücke zu einem Absturz führen. Aus diesem Grund finden die Tests in einer geschützten Laborumgebung statt. Damit die Testdurchführung relativ unkompliziert, mit grösstmöglicher Wirkung und Aussagekraft von statten geht, werden die im Voraus ausgearbeiteten Black Box Testfälle durch das Insider-Knowhow der SCION Entwickler optimiert und in Begleitung eines SIX Mitarbeiters durchgeführt. Hinsichtlich der frühen Phase des Einsatzes von SCION und dem Aufbau der sogenannten SCION-Inseln

⁹<https://www.cisecurity.org/cybersecurity-best-practices>

erhöhten Gefahr und des daraus resultierenden Risikos stehen die beiden Komponenten der Arbeit im Vordergrund. Im abschliessenden Themenbereich „Forensische Analyse“ geht es um Fragestellungen im Fall einer möglichen Kompromittierung resp. der Schaffung von forensischen Grundlagen und den Aufbau einer Art von forensischer Wissensdatenbank bezüglich SCION. Bei einem Vorfall muss sich der Forensiker, unter streng methodisch vorgenommenen Datenanalysen, fast unzähligen komplexen Fragen stellen und klären. Besonders wichtig ist auch hier die solide Basis, nämlich das gehärtete System als Startpunkt. Bei der Betrachtung von Spureninformationen ist die Frage, in Bezug auf ihre Integrität und Authentizität eines digitalen Objektes (z. B. eine Datei), ausgesprochen relevant. Die Integrität und Authentizität der Spurenbilder wird nicht nur durch die korrekte Arbeitsmethodik des Forensikers sichergestellt, sondern auch durch den zuständigen System Integrator und Software Entwickler, die für eine saubere und ordnungsgemässe Programmierung, Installation und Konfiguration des Systems zuständig sind. Wir müssen uns initial auf ein nicht kompromittiertes Basisbetriebssystem und einer unveränderlichen Ausgangslage verlassen können. Die vorangehenden Themenschwerpunkte unterstützen und festigen die Grundannahme so, dass darauf forensisch aufgebaut werden kann und die digitalen Spurenbilder korrekt ermittelt werden können. Die Konfiguration der Testumgebung und den ausgeführten Aktionen unterliegen strengen Vorgaben, die in den nachfolgenden Kapiteln spezifiziert und detailliert beschrieben werden.

Grundsätzlich stehen die folgenden forensischen Fragestellungen im Vordergrund:

- + Welche persistenten Spuren hinterlässt der Systemadministrator während seinen Arbeiten bis zum gehärteten und kundenspezifischen Anapaya Base SIX Image (SCION Hardening)?
 ⇒ **Secured SCION Host OS Image**
 - * Alle Spuren, verursacht durch die manuellen und/oder automatisierten grundlegenden Programminstallationen (z. B. SCION Dienstprogramme, Konfigurationen etc.)
 - * Alle Spuren, verursacht durch die manuellen und/oder automatisierten Härtungsmassnahmen (z. B. De-Installationen, Konfigurationen etc.)
- + Welche persistenten Spuren hinterlässt der Systemadministrator während seinen Arbeiten bis zum abgeschlossenen Anapaya SCION SIX Image (SCION Services)?
 ⇒ **Secured SCION Platform**
 - * Alle Spuren, verursacht durch die manuellen und/oder automatisierten Installationsroutinen für die Inbetriebnahme der SCION Control Services (Path-, Certificate- und Beacon Server)
 - * Alle Spuren, verursacht durch die manuellen und/oder automatisierten Installationsroutinen für die Inbetriebnahme des Border Routers resp. SCION IP Gateways
- + Welche persistenten Spuren hinterlässt der Systemadministrator durch den automatisierten SCION Security Benchmark des SCION IP Gateways?
 ⇒ **Audited SCION Services**
 - * Alle Spuren, verursacht durch das Security Benchmark Tool
- + Welche Artefakte verbleiben nach einer ordnungsgemässen SCION Service Deinstallation?
 - * Alle verbliebenen Spuren nach einer manuellen und/oder automatisierten Deinstallation der SCION Control Services (Path-, Certificate- und Beacon Server)
 - * Alle verbliebenen Spuren nach einer manuellen und/oder automatisierten Deinstallation des Border Routers resp. SCION IP Gateways

Auffallend ist auch hier, der sinnvolle und abrundende direkte Bezug zu den Vorthemen. In der IT-Forensik ist es essentiell wichtig zu wissen, welche Spuren gewollt oder funktionell verursacht sind. Im Vordergrund der Analysen stehen die persistenten Spuren auf dem Datenträger. Bei der Post-mortem-Analyse (Offline-Analyse) sind die in einem bestimmten Zeitraum nachträglich übriggebliebenen Artefakte, also nach der Ausführung der vordefinierten manuellen Benutzerinteraktionen oder Programmaktionen, von Interesse. Das Hauptaugenmerk liegt wie nach einem Vorfall auf der Gewinnung und Untersuchung von veränderten, gelöschten, umbenannten sowie anderweitig versteckten und verschlüsselten Dateien. Zu Gunsten der Vereinfachung und der automatisierten Analysen kommen die zu untersuchenden Systeme in virtueller Form zum Einsatz. Immer nach der Aktionsausführung wird das System nachträglich auf Spuren untersucht. Um die Nebengeräusche bestmöglich herauszufiltern, findet die Spurengewinnung mindestens in drei Durchläufen statt. Daraus kristallisiert eine Liste mit charakteristischen Artefakten. Sie werden herleitend erklärt und grob beschrieben. Jede Änderung am Computersystem, wie z. B. verursacht durch Softwareaktualisierungen, kann das gewonnene Bild beeinflussen, und es ist daher nur als Momentaufnahme zu verstehen. Eine stetige Aktualisierung ist daher auch hier anzustreben und unumgänglich. Im Kapitel 7 „Forensische Analyse“ finden sie vor der Aufschlüsselung der Spuren eine weiterführende und detaillierte Beschreibung der angewandten Methodik. Sie vermitteln die ganzheitliche und abschliessende Sicht, wie und mit welchen Mitteln die persistenten Spuren ermittelt wurden. Die hergeleiteten Analyseergebnisse, der bewusst verursachten typischen Spurenbilder, wirken in künftigen Untersuchungen von realen Cybervorfällen unterstützend und senken den Aufwand deutlich.

An dieser Stelle möchte erwähnt werden, dass das im praktischen Teil erarbeitete Benchmark-Tool keinen Vulnerability-Scan im engeren Sinn durchführt. Es überprüft auf Schwachstellen in der Systemintegration (Hardening) und reduziert so die allgemeine Angriffsfläche und Verwundbarkeit. Das klassische intelligente Schwachstellenmanagement (Vulnerability Management) liegt in der Verantwortung vom SIX Swiss FinSOC. Sie führen mit einer dedizierten Lösung die automatisierten und in laufend wiederholenden Zyklen die Scans durch. Das in Shellsript oder Python programmierte Benchmark-Tool wird schliesslich von einer geschützten Admin- oder Forensik-Workstation gestartet. Es kann lokal oder remote auf dem zu untersuchenden SCION-System ausgeführt werden. Sobald der Benutzer die gewünschte Funktion gewählt hat, verbindet sich die Anwendung via SSH und authentifiziert den Administrator am prüfenden SCION System. Anschliessend finden die sicherheitsrelevanten Überprüfungen (read-only) gemäss den definierten Kontrollen statt. Bei einem Sicherheitsverstoß wird eine Warnmeldung mit einem begründeten Kommentar ausgegeben. Aus Sicherheitsgründen muss der Admin die daraus resultierten Systemanpassungen bewusst und manuell durchführen. Daraus resultiert ein anschliessender Regressionstest zur Verifikation. Gleich wie die theoretisch erarbeiteten Leitlinien und Kontrollen, untersteht das Auditing-Tool einer laufenden Aktualisierung.

Die forensischen Analysen werden mit separaten und fachspezifischen Tools durchgeführt. Einige der Tools sind wissenschaftlich anerkannt und frei erhältlich und andere wurden einst im Studiengang entwickelt. Eine Integration in das Audit-Tool ist nicht zweckmässig, da die Untersuchungen aus mehreren und aufwändigen Schritten an unterschiedlichen Datensätzen erfolgen. Ausserdem sind die Aufgaben und Funktionen zu unterschiedlich. Alle Analysen finden offline an einem zuvor gezogenen Abbild statt und daher wird keine direkte Verbindung auf das zu untersuchende System benötigt. Einerseits könnte eine Remote Verbindung die Resultate verfälschen und andererseits die Analysen erschweren. Das ist auch der Hauptgrund, weshalb die Services in einer virtuellen Umgebung aufgebaut werden und lediglich der Zugriff auf das Host System benötigt wird.

SIX, als ein Unternehmen mit hohen regulatorischen Sicherheitsstandards, ist es nicht ohne weiteres möglich, eine Anwendung wie SCION ohne geeignete Sicherheitsmassnahmen in der Infrastruktur bereitzustellen. Diese und weitere Kontrollen müssen zukünftig kontinuierlich gegen Sicherheitslücken und anderen

Schwachstellen¹⁰ optimiert werden, um sich den entwickelnden Herausforderungen im Bereich der Cybersicherheit entgegenzuwirken. Oft gibt es für selbstentwickelte Programme oder in ihrer frühen Phase keine externen Quellen oder eine Community wie CVE, für die öffentliche Bekanntgabe von Schwachstellen. In solchen Fällen muss dem Herstellerprozess und Support vertraut werden. Die angebundenen SSFN-Kunden sind besonders auf einen offenen, transparenten und verlässlichen Kommunikationskanal angewiesen. Die noch eher kleine SCION Community besteht zurzeit hauptsächlich nur aus internationalen Universitäten und der Anapaya Systems AG. Etwas blauäugig wäre es, dies bei dem alleine stehen zulassen und daher macht eine jährliche Überprüfung durch einen unabhängigen Penetrationstest von Cyber-Security-Experten unumgänglich. Üblicherweise sind die „Application Manager“ und „Application Operator“ als CERT Scouts in der Pflicht ihre Applikationen auf mögliche Schwachstellen zu prüfen und gegebenenfalls zu beheben. Das Patchmanagement des Betriebssystems eines SIX Standardservers findet üblicherweise über eine zentrale Abteilung statt. Würde es sich bei den SCION Systemen per Definition um Appliances handeln, so liegt die volle Verantwortung über das komplette Patchmanagement (OS und App) wieder bei den erwähnten Applikationsverantwortlichen.

¹⁰<https://cve.mitre.org>

FORSCHUNGSSTAND

Zu Projektbeginn schilderte Adrian Perrig[52] grob die spannenden Anfänge und der aktuelle Forschungsstand von SCION. Um das Komplettbild zu erhalten, folgt vor dem aktuellen Forschungsstand ein kurzer Einblick in die Vergangenheit. Im Sommer 2009 startet Adrian Perrig et al. an der Carnegie Mellon University (CMU) das SCION Projekt und begann mit Überlegungen, wie eine sichere domänenübergreifende Internetarchitektur grundlegend aussehen könnte. Nach anfänglichen Schwierigkeiten mit schier unlösbaren Herausforderungen, verursacht durch immer wieder auftauchende und vermehrende Problemstellungen, gelang dank ihrem Durchhaltevermögen im Sommer 2010 der Durchbruch. Der grundlegende Ansatz erfüllte die meisten Anforderungen, und die neue Architektur vermittelte das Gefühl, alle Probleme künftig lösen zu können. Der Motivationsschub beschleunigte das Projekt und den Arbeitsfortschritt so, dass die Architekturdokumente vom IEEE-Symposium für Sicherheit und Datenschutz 2011 akzeptiert wurden. Schliesslich konnte das Team von eXpressive Internet Architecture (XIA) für das SCION Projekt gewonnen werden. XIA ist ein Projekt aus dem Programm namens Future Internet Architecture (FIA) und wird von der U.S. National Science Foundation (NSF) finanziert. Im Rahmen von XIA wurde dann die Weiterarbeit gesichert und damit die frühe Forschung unterstützt.

Vermutlich aufgrund dieser bewussten und strategisch sinnvollen Projektaufteilung auf zwei Achsen in „Forschung und Entwicklung“ und „Implementierung“ führte zum jetzigen Ausbaustatus in der Industrie. Durch den frühen Aufbau und die ständige Weiterentwicklung des ersten Prototyps in den Jahren 2011-2013 und den von der ETH Zürich ermöglichten Aufbau des globalen Forschungsnetzwerks „SCIONLab“ in den Jahren 2015/16, ermöglichte das schnellstmögliche Testen der Internetarchitektur der nächsten Generation in einem realen Umfeld für jedermann[52]. Alle Interessierten können sich mit dem SCIONLab-Netzwerk verbinden und realistische Experimente durchführen. SCION läuft problemlos auf physischen und virtuellen Standardservern. Mit diesem Vorgehen machten sich die Problemstellungen und geforderten Anforderungen sehr früh sichtbar, und sie konnten entsprechend angegangen und implementiert werden. Dank der breiten Community aus der Wirtschaft, wurden nicht nur technische Funktionen, wie die essenziell wichtige Interoperabilität und Kompatibilität etc. berücksichtigt, sondern auch die allgemeine Wirtschaftlichkeit als solches. Um SCION wird noch immer an der ETH Zürich vom SCION Team mit Studenten und zusammen mit dem Spin-Off Anapaya Systems AG weiter Forschung und Entwicklung betrieben. Unterstützung auch von ausserhalb der Community sind gerne gesehen und willkommen. Laufend kommen weitere Anforderungen aus der Industrie zur Umsetzung hinzu. Wie z. B. Kamila Součková in ihrer Masterthesis[60] schreibt, wird SCION in Bezug auf hohe Bandbreiten zukünftig eine eigene für SCION abgestimmte Hardware benötigen, und es sind sehr wahrscheinlich noch Protokollanpassungen zu erwarten. Durch den reinen Software-basierten Ansatz ohne spezieller Hardware, kann keinen Router-Durchsatz von mehreren 10Gb/s erreicht werden. Mit Unterstützung von spezieller Hardware, könnten Bandbreiten von mehreren 100Gb/s oder sogar im Terabit-Bereich erreicht werden. Vor allem im Provider-Umfeld werden künftig als erstes solche Durchsätze verlangt. Nichtsdestotrotz hat SCION dank seiner Flexibilität und

Stabilität jetzt schon marktreife erreicht. Anfänglich war SCION „verständlicherweise“ von Skepsis geprägt, und es fehlte an der Akzeptanz. Die potenziellen Vorteile wurden mittlerweile von verschiedenen Interessensgruppen erkannt. Vermutlich auch wegen dem hohen Stellenwert des Finanzplatzes Schweiz, konnten bereits diverse Schweizer ISPs erfolgreich mit Native-SCION aufgeschaltet werden. Aktuell findet zusammen mit Anapaya Systems AG die Anbindung verschiedener schweizerischer Finanzunternehmen statt. Das bereits erwähnte Projekt SSFN hatte im Jahr 2020 das Projektziel der erfolgreiche, sichere und verifizierte Feldaufbau vom SCION Finanznetzwerk „ISD SSFN“. In diesem Jahr 2021 sollen demnach die ersten Finanzapplikationen in einer erweiterten Pilot-Phase über das sichere SCION Netzwerk betrieben werden. Schon während der Aufbauphase sind etliche Erweiterungswünsche entstanden, und bestimmt werden noch weitere spannende und zu lösende Herausforderungen auf uns warten. Nach erfolgreicher Betriebsphase scheint einer stetigen Markteindringung, mit einer gesicherten fortlaufenden Forschung und Entwicklung, nichts mehr im Wege zu stehen.

2.1. SCION und andere konkurrierende Ansätze

Das Internet wurde ursprünglich nicht für die jetzigen und anstehenden Anforderungen konzipiert und gebaut. Die Evolution des Internets ist nach herrschender Meinung schon so weit fortgeschritten, dass es mittlerweile zur Lebensgrundlage von Privatpersonen gehört und die Industrie stark davon abhängig ist[47]. Die starken Veränderungen und daraus resultierenden Problemstellungen wurden von Experten schon relativ früh erkannt und das veranlasste die Erforschung von alternativen Internetarchitekturen. Der Mangel an Sicherheit im Internet ist bekanntlich das grösste Problem. Die ganzheitliche Sicherheit kann aber nicht in einem einheitlichen System stattfinden, da der Schutz je nach Anwendungsfall in unterschiedlichen Schichten erfolgen muss. Nicht alle Probleme können und dürfen in der Verantwortung des Netzwerks liegen. Jedoch von einem zukünftigen Internet wird ein vertrauenswürdigen und kooperatives System erwartet. Aus diesem Grund wird in manchen Lösungen eine vertretbare Position der Netzwerkrolle bei der Unterstützung der Endhost-Sicherheit beansprucht und eine konsequente Aufteilung der Verantwortung zwischen dem Netzwerk und dem Endhost vorgeschlagen. Im Jahr 2010 startete die NSF¹ ihr Fünfjahresprogramm namens FIA. Es umfasste ursprünglich vier Forschungsprojekte mit unterschiedlichen Visionen, aber alle verfolgten dasselbe Hauptziel. Die neuen Architekturen sollen die Sicherheit und den Datenschutz aufgrund der heutigen Abhängigkeit von Internetdiensten verbessern. In der sogenannten Next-Phase nach 5 Jahren wurden nur noch drei Architekturen, wie unter anderem auch das bereits erwähnte XIA, weiter finanziert. Nebst den Projekten aus FIA gab es im letzten Jahrzehnt noch einige andere Forschungsprogramme, aus denen weitere interessante Architekturvorschläge kamen. Darunter gab es auch Forschungsprogramme wie 2STiC² mit dem Hauptziel, den Anschluss zu potentiell neuen Architekturen und Technologien nicht zu verpassen. Es zeigte sich, dass einen direkten Vergleich der Ansätze mit teilweise sehr unterschiedlichem Forschungsstand, abweichendem Zielumfang und Dokumentationsgehalt sehr schwierig und praktisch unmöglich zu sein scheint. Ausserdem fanden schon an etlichen Universitäten in der Vergangenheit einige Erhebungen mit überschaubarem und limitiertem Umfang statt. Einen aufgefrischten, erweiterten, fairen und neutralen Vergleich mit einem gerechtfertigten Aufwand scheint zum jetzigen Zeitpunkt nicht gegeben zu sein. Für bereits getätigte Evaluationen und weiterführende Informationen möchte jedoch auf die verwendeten und verwandten Arbeiten[48][14][45][17][52][2][10][36][8][31][67] verwiesen werden. Deshalb wird im nachfolgenden Kapitel auf einen Benchmark von SCION gegen seine Rivalen bewusst verzichtet. Grundsätzlich kann gesagt werden, dass es sich bei den unterschiedlichen Ansätzen immer um

¹<http://www.nets-fia.net>

²<https://www.sidnlabs.nl/en/news-and-blogs/2stic-long-read>

Techniken wie Software Defined Networking (SDN)/Network Functions Virtualization (NFV)³, Overlay Networks oder Information Centric Networking (ICN)⁴ handelt. Die Netzwerkarchitekturen bewegen sich also immer mehr in Richtung einer hardwareunabhängigen und softwaredefinierten Architektur. In mancher Literatur - zwischen den Zeilen gelesen - bestehen zukünftig letztendlich je nach Anforderung oder Bereich mehrere parallellaufende, virtualisierte Internets, ermöglicht und hervorgerufen durch die programmierbaren Netzwerke. Das Offenlegen des Netzwerkes als Plattform schafft mehr Freiraum für Innovationen und muss daher mehr Sicherheit, Stabilität, Transparenz, Effizienz und Skalierbarkeit bieten[44]. Mit einer vollständigen Automatisierung resultiert im Internet eine enorme Eigendynamik mit sehr hohem Potential an Flexibilität. Die Industrie könnte von einem durchgehenden, zukünftigen, kosteneffizienten und kurzen Time-to-Market (TTM) profitieren. Das Internet wird künftig seinen Best-Effort-Charakter ablegen müssen. Die Qualitätsanforderungen rücken auf das Niveau von anderen WAN-Technologien oder Anbindungsarten. Firmennetzwerke verbinden sich bei hohen Ansprüchen mit dem ISP über das Multiprotocol Label Switching (IP/MPLS) oder realisieren Direktverbindungen (Point-to-Point). Solche logische oder physische ISP-Anbindungen sind kostspielig. Die Kehrseiten sind die zusätzlichen Herausforderungen addiert zu den bereits konfrontierten Problemen (z. B. Erweiterbarkeit, Kapazität etc.) auf der Seite des ISPs. Die ISPs sollten einen Dienst bereitstellen, der den Benutzeranforderungen der entscheidenden Rolle des Internets, sowohl im geschäftlichen als auch im privaten Bereich, hinsichtlich Zuverlässigkeit, Ausfallsicherheit und Verfügbarkeit über dieselbe Plattform entspricht[62]. Um die Benutzeranforderungen künftig zu erfüllen, muss ein weiteres ungelöstes Problem nämlich das Netzwerkmanagement adressiert werden. Es fehlen Werkzeuge zur Erkennung, welche Netzwerkelemente von welchen Benutzern/Benutzergruppen (Domänen) verwendet werden, und welche Anwendungen derzeit welche spezifischen Netzwerkkomponenten verwenden. Im heutigen Internet verstehen wir immer noch nicht durchgehend, wie das Netzwerk für einen zuverlässigen Betrieb, eine einfache Verwaltung, ein Debugging und eine gute Skalierung eingerichtet und gesteuert werden kann. Verstärkt drängt sich die Verantwortung der erwähnten Punkte bei zukünftigen Internetarchitekturen auf. Darunter verstehen wir entsprechende Vorkehrungen im Bereich des Netzwerkmonitoring, gegen Hindernisse von vorübergehender Routing-Instabilität bis hin zu Denial-of-Service-Angriffen, hinsichtlich der Verfügbarkeit zu beseitigen. Wir stellen durch die geforderten hohen Anforderungen in verschiedensten Architekturen der nächsten Generation eine stetige Zunahme an Komplexität und Vielschichtigkeit fest. Bei allen Clean-Slate-Ansätzen ist eine Akzeptanz in der Internet Community von enormer Bedeutung, und sinnvollerweise liegt der Fokus auf den wesentlichsten Problemstellungen, welche der Markt am Meisten beschäftigt. Des Weiteren ist es immens wichtig, eine gewisse Kompatibilität oder Interoperabilität mit IP und anderen Bemühungen im Internet der Zukunft zu gewährleisten[53]. Eine Gewährleistung der Interoperabilität zwischen unterschiedlichen Technologien ist vor allem in der Migrationsphase z. B. von BGP auf SCION von hoher Bedeutung. Ausserdem besteht mit einer neuen Architektur vermutlich eine schwindende Chance den Markt zu durchdringen, wenn sie keine ganzheitliche Lösung aller zukünftigen Anforderungen an das Internet mit sich bringt, oder den effizienten Informationsaustausch von unabhängigen, heterogenen Systemen verunmöglicht oder erschwert. Obwohl in der Vergangenheit schon sehr viel Forschung betrieben wurde, erscheint noch kein durchgehender Lösungsansatz in punkto Sicherheit und Hochverfügbarkeit als abgeschlossen zu sein[64]. Der technologische Fortschritt schaffte es bei manchen aufstrebenden Architekturen[51], wie NDN, MobilityFirst, XIA, RINA und SCION, mit dem Status „experimental Systems“ in eine grosse Testumgebung. Das Projekt SSFN zielt darauf ab, SCION von der experimentellen Testevaluierung zu Technologieversuchen „Technology-Trials“ mit realen Benutzern und Anwendungen überzugehen.

³<https://www.cisco.com/c/en/us/solutions/software-defined-networking/sdn-vs-nfv.html>

⁴https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/information-centric-networking-education.pdf

2.2. SCION Faktoren

Bei einer grundlegend neuen Internet Architektur können bestimmte Eigenschaften und Ziele nicht von Beginn an implementiert werden. Die Integration solcher Funktionen, schon zu Beginn, erhöhen die Komplexität enorm und bringen zusätzliche Problemstellungen hervor. Das hatten die Forscher von SCION erkannt und wählten daher einen agilen Entwicklungsansatz. Der Fokus lag vorerst klar beim Ersatz vom heutigen Internet-Routing-Protokoll. BGP, als das heutige Inter-Domain-Routing-Protokoll, verbindet so wie SCION autonome Systeme (ASes) miteinander. Die Stärken von SCION liegen klar bei sogenannten Punkt-zu-Punkt-Kommunikationen. Eine robuste, hochverfügbare und sichere Kommunikationsinfrastruktur benötigt z. B. nicht von Anfang an Multicast oder die effiziente Auslieferung von Daten im Sinne eines Content Delivery Networks (CDN)⁵. Ein CDN kennt den darunter liegenden Netzwerkstatus, und umgekehrt kennt das Underlay die auszuliefernden Informationen nicht. Das CDN wird so seinem Namen nicht in allen Belangen gerecht. Für die noch effizientere Verbreitung von Inhalten könnte in Kombination ein Information-Centric Network (ICN) zusätzlich unterstützen[7]. Wie dieses Beispiel und auch die Vergangenheit zeigte und bestätigte, ist es enorm schwierig eine „perfekte“ oder ganzheitliche Internet Architektur zu entwickeln. Die technologischen Entwicklungen machen keinen Halt, und daher ist es von hoher Bedeutung, dass neue Architekturen spätere Funktionserweiterungen berücksichtigen und ermöglichen. Bei SCION wurden solche Erweiterungen bewusst bedacht oder zumindest nicht ignoriert, damit eine Integration stets ermöglicht oder nicht erschwert wird. Wie angedeutet, können gewisse Funktionalitäten auch ganz einfach in SCION als Underlay Network mit einem Overlay Network erweitert werden[52]. Auch diese Technologien sind auf einen effizienten, darunterliegenden Routing-Mechanismus für die reine Paketweiterleitung angewiesen. Das Underlay ist also mindestens genauso wichtig, wenn es nicht die bedeutendste Funktionalität im Netzwerk darstellt! Das Underlay verkörpert das verlässliche Fundament, auf das vertraut und laufend aufgebaut wird. Gleich wie das heutige Internet, ist auch SCION problemlos in der Lage, die heutigen klassischen und zukünftigen Overlay Technologien zu transportieren. Die bekanntesten klassischen Overlay Netzwerke erkennen wir unter Virtual Private Networks (VPNs), Peer-to-Peer (P2P), non-native Software Defined Networks (SDN) und viele mehr. Auch SCION kann und nutzt sogar das heutige Internet als Underlay Network vor allem in der Ablösungsphase von BGP auf SCION. In dieser Übergangsphase können verständlicherweise nicht alle Vorzüge von SCION ausgeschöpft werden, aber es verdeutlicht wie flexibel und anpassungsfähig SCION grundsätzlich ist.

Veranlasst durch die extremen Änderungen in der Internetnutzung, führte es zu einer starken Abhängigkeit von Internetdiensten. Unweigerlich führt das zu einer zunehmenden Reichweite und Komplexität von Cyber Angriffen, sowie steigender Nachfrage nach entsprechenden Datenschutzmassnahmen. Der Stellenwert von Security und Privacy ist in der Wirtschaft schon lange hoch. Seit einigen Jahren wird dem im privaten Umfeld glücklicherweise auch vermehrt Beachtung geschenkt. Angesichts des Mangels an Sicherheit und Datenschutz im aktuellen Internet, liegt das Hauptaugenmerk von den meisten Future Internet Architekturen bei diesen beiden Themenbereichen. Die Architektur der aktuellen Internetplattform ist IP-basiert und ist auf dem OSI-Layer 3 der Vermittlungsschicht (Network Layer) angesiedelt. Diese Schicht hat die Aufgabe, die Pakete vom Sender zum Empfänger zu bringen. Auf demselben OSI-Layer, mit grundlegender gleicher Aufgabe, arbeitet auch das IPSec-Protokoll. Mit der Security Extension sollte die grundlegende Sicherheit bezüglich Authentifizierung, Datenintegrität und Vertraulichkeit für IP-Datagramme gesteigert werden. Mit weiteren Optimierungen von SCION könnte ein reines SCION-Netzwerk theoretisch künftig IP ablösen. Deshalb nehmen wir IP/IPsec als Referenzpunkt bei der Gegenüberstellung und konzentrieren uns besonders in der gezeigten Tabelle 2.1 auf die Security und Privacy im heutigen und zukünftigen Internet. In den einzelnen Punkten werden die Funktionalitäten, Stärken, Schwächen und Vorteile von SCION

⁵<https://www.ionos.de/digitalguide/hosting/hosting-technik/was-ist-ein-content-delivery-network-cdn>

gegenüber von IP mit seinen Erweiterungen aufgelistet und kurz erklärt. Selbstverständlich dürfen wir hier, auf keinen Fall, das BGP nicht ausser Acht lassen, da SCION vor allem auch das Routing-Protokoll im Internet zwischen den ASes ablöst. Die Auflistung soll einen guten und leicht verständlichen Überblick der Verbesserungen gegenüber seinem Vorreiter BGP/IP auf der Vermittlungsschicht geben. Sie ist nicht als vollständig zu verstehen und darf künftig gerne mit tiefgründigen Informationen und Punkten erweitert werden. Das hier verfolgte und wohl erreichte Hauptziel ist, die Vorzüge von SCION besonders hervorzuheben.

Tabelle 2.1.: Network Security and Privacy (nach [2])

	SCION	IP/IPsec
Trust	SCION pflegt, z.B. innerhalb einer ISD Schweiz, ein hierarchisches und ISD-übergreifendes, zwischen zwei Ländern z. B. der Schweiz und Deutschland, verteiltes Trusted Model.	IP verfolgt ein hierarchisches Trusted Model, und die Hosts schenken ihr Vertrauen immer einer übergeordneten Autorität/Identität.
	Als Trusted Entity gelten in einer SCION-Island alle Netzwerkkomponenten (Control Services, Router und Hosts). Jedes AS in SCION verfügt über ein eigenes, gültiges Zertifikat und die Informationen untereinander sind authentifiziert. Findet die Kommunikation über ein SCION IP Gateway (SIG) statt, so kann z. B. zwischen IP-Endhosts keinen direkten Trust ohne weitere Massnahmen aufgebaut werden.	Als Trusted Entity gelten bei IPsec lediglich die Endhosts oder Netzwerke untereinander. Die Identifizierung wird durch die Security Association (SA) definiert, und die Authentifizierung erfolgt meist über digitale Signaturen oder PSKs.
	In der ISD definiert das TRC den Root of Trust und die Schlüsselmaterialien werden von der jeweiligen Control Plane PKI (Trust Management) verwaltet und ausgestellt.	Die Vertraulichkeit (Trust Management) zwischen den Endsystemen basiert zumeist über eine PKI mit Zertifikaten oder Pre-shared Keys (PSKs).

Tabelle 2.1: weiter auf nächster Seite

Tabelle 2.1: Weiterführung von vorheriger Seite

	SCION	IP/IPsec
Confidentiality	Die SCION Nodes authentifizieren sich nicht untereinander. Der Informationsaustausch zwischen den SCION Komponenten findet standardmässig mittels kryptografisch gesicherter Authentifizierung statt. Alle Informationen wurden durch einen Private Key von dem entsprechenden AS Zertifikat signiert. Den ausgetauschten Informationen wie beispielsweise den PCBs können also vertraut werden. Sie schützt vor bössartigen Netzwerkteilnehmern und Fehlinformationen auf Netzwerkebene.	Bei BGP/IP kann zwischen BGP-Peers eine Authentifizierung aktiviert werden. Die BGP-Nachbarn müssen ein identisches Passwort aufweisen. Mit der Erweiterung von BGPsec kann zusätzlich sichergestellt werden, dass keine bössartige Routinginformationen eingeschleust werden können. Eine RPKI (Resource Public Key Infrastructure) sichert BGP für die globalen IP-Routing-Informationen ab. Im Gegensatz zu SCION gibt es bei RPKI eine zentrale Autorität und birgt so seine Tücken. ^{6,7}
	Die Pfadinformationen innerhalb der PCBs werden per se unverschlüsselt übertragen und sind somit vom Mitlesen Dritter ungeschützt. Die Verschlüsselung kann optional aktiviert werden, aber wird aus Effizienzgründen nicht empfohlen.	Ähnlich wie in SCION werden die BGP Route Advertisements durch BGPsec signiert, um die Routing-Integrität sicherzustellen. Eine Verschlüsselung der Routinginformationen findet in BGP und BGPsec nicht statt.
	Die Datenübertragung findet über ein SCION-Netzwerk grundsätzlich in „Klartext“ statt. Die Header- und Payload Daten sind unverschlüsselt und nicht vor unberechtigtem Zugriff von Dritten geschützt. Durch die bekannten Verschlüsselungsprotokolle auf höherem Layer, wie SSH und TLS/SSL oder durch den Einsatz vom experimentellen System namens High-speed onion routing at the network layer (HORNET[6]), können die Header- oder/und Payload Daten geschützt werden.	Wie SCION setzt IP auf entsprechende Erweiterungen, wie SSL- und IPsec-VPNs oder auf die genannten Verschlüsselungsprotokolle auf höherem Layer, wie SSH und TLS/SSL, um die Header- und/oder Payload Daten abzusichern.

Tabelle 2.1: weiter auf nächster Seite

⁶<https://www.computerweekly.com/de/tipp/Mit-einer-RPKI-Resource-Public-Key-Infrastructure-BGP-absichern>⁷<https://www.scion-architecture.net/newsletter/RPKI.pdf>

Tabelle 2.1: Weiterführung von vorheriger Seite

	SCION	IP/IPsec
Confidentiality	Bevor der Sender die Datenübertragung startet, ruft er die Path Segments beim Path Server ab und definiert den Ent-to-End-Path. Die Routinginformationen müssen daher komplett im SCION Header vorhanden sein. Für einen unberechtigten Dritten ist es relativ leicht herauszufinden über welchen Weg kommuniziert wird.	Wird im Internet von einem Dritten ein ungesichertes Datenpaket mitgelesen, so kann dieser nur die Source- und Destination-Adresse herauslesen. Das Routing zwischen den Endhosts bleibt jedoch ohne zusätzliche Massnahmen wie z.B. BGP Looking Glass ⁸ verborgen.
	Die allgemeine Vertraulichkeit (Routing- und Payload-Daten) erfolgt mittels der Erweiterung HORNET[6] (Encryption and Onion Routing) zwischen Host-Host und Gateway-Gateway.	Durch verschlüsseln mittels IPsec oder SSL (Transport/Tunnel Mode) zwischen Gateway-Gateway, Host-Gateway und Host-Host kann die allgemeine Vertraulichkeit gesteigert werden. Die originalen Protokoll-Header-Daten z.B. Source- and Destination-Adressen bleiben aber nur bedingt geschützt.
Integrity	Die Integrität der Pfadinformationen wird in SCION durch die stetige Authentifizierung der PCBs und TRCs sichergestellt. Dieser Prozess ist Bestandteil von SCION und kann nicht abgeschaltet werden. Eine Path Validation kann von den Endhosts durchgeführt werden. Durch die Überprüfung wird sichergestellt, dass die Datenpakete auch wirklich den vorgeschriebenen Weg genommen haben. Die hochverfügbare Control Plane PKI dient zur Sicherung der SCION-Steuerebene.	Nur mit BGPsec kann die Integrität der BGP Route Advertisements zwischen den BGP-Peers sichergestellt werden. Der End-to-End-Path kann nicht vorbestimmt oder überprüft werden. RPKI stellt die Schlüsselmaterialien für die Signierung der Pfadinformationen bereit.
	Üblicherweise stellt SCION keinen Mechanismus für die Datenintegrität bereit. Mit dem Einsatz der Erweiterung HORNET[6] kann eine durchgehende End-to-End-Integrität erzielt werden.	IP stellt üblicherweise keine durchgehende End-to-End-Integrität bereit. Der Mechanismus IPsec+HMAC im Tunnel Mode kann für die Integrität von jedem Datenpaket gewährleisten.

Tabelle 2.1: weiter auf nächster Seite

⁸<https://www.bgp4.as/looking-glasses/>

Tabelle 2.1: Weiterführung von vorheriger Seite

	SCION	IP/IPsec
	Die Datenpakete kommen in SCION stets von authentifizierten Quellen, aber auf Payload-Ebene ist SCION auf die Erweiterung HORNET[6] angewiesen. HORNET deckt die Integrität vollumfänglich zwischen Host-Host und Gateway-Gateway ab.	Mit der Erweiterung von IPsec+HMAC wird die Integrität zwischen Gateway-Gateway und Host-Gateway sichergestellt.
Availability	Die Trennung der Control und Data Plane trägt zu einer erhöhten Verfügbarkeit bei, da die Weiterleitung nicht rückwirkend durch Operationen (z. B. Routingänderungen) auf der Control Plane beeinflusst werden kann. Der Pfad wählt grundsätzlich der Sender, und er ist solange gültig bis ein Path Segment zurückgezogen wurde.	In BGP/IP sind zwar die Control und Data Plane auch separiert, aber Änderungen an der Control Plane Ebene können einen direkten Einfluss auf die Routinginformationen haben und das Forwarding entsprechend negativ beeinflussen. Durch die grossen Routingtabellen im Internet können Routingänderungen einen relativ langen Unterbruch verursachen.
	Der Sender kann in SCION mehrere Wege für die Datenkommunikation wählen. Die Multipath Communication erhöht die Verfügbarkeit und Bandbreite. Über welche ASes und/oder ISDs die Pakete nehmen, entscheidet und beeinflusst grundsätzlich der Sender.	BGP/IP verfügt auch über Multipath-Funktionalitäten. Auf den Routern können die Routinginformationen, über welche Pfade die Datenpaket gehen, gesteuert und beeinflusst werden. Die Kontrolle über das Routing unterliegt grundsätzlich und grösstenteils der ISP-Netzwerkadministratoren.
	Der Pfad ist Bestandteil des signierten SCION Headers. Die Path Validation, Path Control und Authentication schützt vor gewissen Netzwerkangriffen und verhilft so zu einer erhöhten Verfügbarkeit.	BGPsec stellt die Integrität der Routinginformationen (Route Prefixes) sicher und schützt hauptsächlich vor Prefix Hijacking. BGPsec weist immer noch gewisse Schwächen ⁹ auf, da beispielsweise eine Konsistenzüberprüfungen zwischen der Control und Data Plan fehlt. Ein weiterer Nachteil kommt durch BGPsec hinzu, da die Path Control Funktionalität „AS path pre-pending“ mit BGPsec nicht mehr verfügbar ist und so die allgemeine Verfügbarkeit abschwächt.

Tabelle 2.1: weiter auf nächster Seite

⁹<https://ieeexplore.ieee.org/document/8594708>

Tabelle 2.1: Weiterführung von vorheriger Seite

	SCION	IP/IPsec
Access Control	Die Path Server und Sender können Path Segments auf Richtigkeit überprüfen. PCBs und Path Segments sind bekanntlich mit den AS Zertifikaten authentifiziert. Jedes AS signiert sie mit ihrem eigenen Private Key, welcher basierend auf dem aktuellen TRC validiert wird.	IP selbst hat keine Authentifizierung implementiert und daher kann dafür auf IPsec zurückgegriffen werden. Authentifiziert werden die Hosts und Gateways meist über Zertifikate und PSKs. Auf der Routingebene können nur die BGP-Members ihren direkten Nachbarn mittels Passwortes authentifizieren und zusätzlich mit Hilfe von BGPsec können die Router über die signierten Routing Advertisements authentifiziert werden.
	Jegliche Path Segments müssen aktuell und korrekt vom Path Server zur Verfügung gestellt werden. In unterschiedlichen Fällen benötigt es eine entsprechende Autorisation. Einerseits dürfen nur autorisierte Hosts auf gewisse Path Information zugreifen, und andererseits dürfen nur autorisierte Nodes Änderungen auf den Path Servern resp. an den Path Information vornehmen. Gesteuert über Policies wird die Autorisation sichergestellt, dass Applikationen nur auf die berechtigten Path Information abrufen können und keine Angreifer die Path Information abrufen oder fälschen können.	Eine Autorisation wird auf IP-Ebene auf den Hosts und/oder Gateways mittels Access Lists (ACLs) erzwungen. Die ACLs steuern im Zusammenhang mit IPsec-Tunnels die SAs. Je nachdem, ob einen IPsec Tunnel zwischen Hosts aufgebaut wird oder nicht, findet die Authentifizierung und Autorisation gleichzeitig statt. Auch auf der Routingebene können Routinginformationen über ACLs (Prefix Lists) autorisiert werden. Mit BGPsec autorisiert die Zertifizierungsstelle die BGP-Router.

Tabelle 2.1: weiter auf nächster Seite

Tabelle 2.1: Weiterführung von vorheriger Seite

	SCION	IP/IPsec
Access Control	Die Accountability wird durch die Authentifizierung und Transparenz im Netzwerk erreicht. In SCION sind die Path Segments und Entitäten stets authentifiziert und verifiziert. Des Weiteren wird bei allen eingehenden Paketen die Topologie (AntiS-poofing) geprüft.	Meist ist bei IP die Quelladresse nicht mehr auszumachen. IPsec garantiert die Peer-Entity-Authentifizierung aufgrund der IPsec SAs zwischen den Tunnel-Endpunkten. Somit kann mit IPsec eher das Accountability gewährleistet werden. Auf der Routingebene stellt BGP bekanntlich die Routing-Infrastruktur bereit, so dass schliesslich die Netzwerkteilnehmer untereinander kommunizieren können. BGPsec kann lediglich die Accountability bezüglich BGP-Router und Routing Advertisements gewährleisten.
Attack Prevention	Es wird zwischen drei Kategorien von DDOS unterschieden. Das Internet als Transportsystem kann nur Massnahmen gegen die sogenannten Volume-based Attacks implementieren. Alle anderen Angriffe finden auf einem höheren Layer statt. Dank der Source Authentication und Path Validation bringt SCION die notwendige Transparenz ins Netzwerk, um vielen volumetrischen DDoS Angriffen, verursacht durch Botnets und Malicious Network Entities die Stirn zu bieten. Des Weiteren verhilft die Erweiterung SIBRA für noch einen besseren Schutz vor DDoS. SIBRA ermöglicht eine garantierte Bandbreitenzuweisungen, um die Verfügbarkeit auch Angriff zwischen den Endhosts zu gewährleisten.	Gegen Volume-based Attacks hat IP per se keine Vorkehrungen getroffen. Es gibt viele Gegenmassnahmen, die zur Abwehr und Erkennung von DDoS Angriffen entwickelt wurden. Jedoch ergeben die unzähligen, aufwändigen und kostspieligen Methoden, welche die Internet Provider und Enterprise Kunden einsetzen können, keinen umfassenden DDoS-Schutz und Zufriedenheit.
	Ein erhöhter Schutz gegen Man-in-the-Middle (MITM) ist in SCION gegeben, da aufgrund des ISD-Konzeptes, ohne mehrfacher Kompromittierung in der SCION-PKI-Struktur, keine weiteren Nodes hinzugefügt werden können.	IP selbst hat gegen Man-in-the-Middle (MITM) Attacks keine Vorkehrungen getroffen. Um bösartige BGP-Router dazwischen zu vermeiden, empfiehlt es sich die Authentifizierung von BGP oder BGPsec zu nutzen.

Tabelle 2.1: weiter auf nächster Seite

Tabelle 2.1: Weiterführung von vorheriger Seite

	SCION	IP/IPsec
Attack Prevention	Wird zwischen zwei Aktivkomponenten (Router/Switch) beispielsweise mit Hilfe von Network Tabs oder IP-Routern im Underlay mitgelesen, kann Packet Sniffing nicht ohne Weiteres erkannt und blockiert werden. HORNET[6] und andere Authentifizierungs- und Verschlüsselungstechniken geben einen zusätzlichen und erhöhten Schutz gegen Packet Sniffing.	Auch in IP-Netzwerken kann Packet Sniffing nicht ohne geeignete Massnahmen erkannt und blockiert werden. Gegen Packet Sniffing verschafft lediglich die Verschlüsselung und Authentifizierung z. B. mittels IPsec oder anderen Authentifizierungs- und Verschlüsselungstechniken.
Attack Prevention	Wie bei MITM erwähnt, ist ein AS Spoofing eher sehr schwierig zu erreichen, da ein gültiges AS Zertifikat für die Generierung von gültigen PCBs und HF-Informationen benötigt wird. Address Spoofing wird in SCION erschwert, da der Angreifer für alle Datenpakete einen gültigen SCION Header mit korrekter HF-Sequenz benötigt. Einerseits wegen der Authentifizierung und Interface-Verifizierung und andererseits aufgrund der Paketweiterleitungsart. Alle Datenpakete werden gemäss den Path Information und nicht anhand der Destination Adresse weitergeleitet. Das heisst, der Forward Path sowohl der Reverse Path muss stimmen. Wenn das Zielsystem auf eine Source Authentication ¹⁰ besteht oder ein Path Lookup durchführen muss, kann der Nebeneffekt (Reflection Attack) einer Source Address Spoofing verhindert werden.	Grundsätzlich gibt es in IP keine implementierten AntiSpoofing-Mechanismen. Im heutigen Internet ist IP-Spoofing schwierig zu verhindern. Es empfiehlt sich jedoch eine restriktive Source Filterung auf den Netzwerkkomponenten zu pflegen, um Unstimmigkeiten in der Topologie festzustellen und zu unterbinden.

Tabelle 2.1: weiter auf nächster Seite

¹⁰Das EPIC-Protokoll ersetzt das noch immer theoretisch beschriebene OPT und übernimmt künftig die Source Authentication und Path Validation.

Tabelle 2.1: Weiterführung von vorheriger Seite

	SCION	IP/IPsec
Attack Prevention	Prefix Hijacking ist in SCION nicht mehr möglich. Ein SCION-Pfad kann aufgrund der Trennung von Steuer- und Datenebene und wegen des PCFS nicht umgeleitet werden. Auch die Trennung in ISDs gibt die Garantie, dass interne Routingentscheidungen keinen Einfluss auf andere Netzwerke haben.	Das Internet lässt noch heute bei unsachgemässer Konfiguration von BGP ein Prefix Hijacking zu. Es empfiehlt sich den Einsatz von restriktiven Prefix-Filtern an Border Routern, um eingehenden böswilligen Verkehr zu blockieren. Eine andere Möglichkeit ist die kryptographische Überprüfung von Routen durch den Einsatz der Erweiterung BGPsec. Den Angreifern wird deutlich erschwert, falsche Routen zu verbreiten.
	SCION bietet eine globale Sicherheit ohne globale Vertrauenswurzel, erreicht über die verteilten TRCs. Ein sogenannter globaler Kill Switch über ISDs hinaus ist nicht möglich.	Wie schon kurz angesprochen wird in BGPsec auf eine monopolistische (hierarchische) Vertrauensstruktur gesetzt. Die RPKI Struktur erlaubt übergeordnete Stellen mit ihren Private Keys gewisse Teilbereiche vom Internet zu beeinflussen oder abzuschalten.
Attack Prevention	SCION ist im Umgang mit Compromised Keys sehr umgänglich. Ein Remote ISD kann grundsätzlich die anderen ISDs nicht beeinflussen. Wird trotzdem davon ausgegangen, dass die Private Keys von einem ISD abhanden kamen, ist deshalb nur das entsprechende ISD betroffen. Ausserdem benötigt der Angreifer für die Beeinflussung zusätzlich Zugriff auf ein Remote-ISD-AS. Je nachdem an welcher Stelle die Private Keys abhanden kamen, ist der Einfluss auf das bestehende Forwarding bei der Erneuerung der Zertifikate grösser oder kleiner. Bei abhanden kommen von Core-AS Root Keys (Online/Offline) benötigt es eventuell eine Erneuerung aller Zertifikate innerhalb der ISD und ein TRC-Update. Betrifft es ein non-Core-AS muss nur das AS Zertifikat erneuert werden.	BGPsec setzt auf eine überschaubare Struktur und Anzahl von Vertrauensstellen innerhalb der RPKI. Der sogenannte Trust Anchor bildet die Internet Assigned Numbers Authority (IANA), und darauf folgen die Internet Registries Regional Internet Registry (RIR), National Internet Registry (NIR) und Local Internet Registry (LIR). Die Route Origination Authorization (ROA) erfolgt schliesslich von den lokalen ISPs. Wie ersichtlich wurde, kann eine Kompromittierung in Abhängigkeit der betroffenen Hierarchiestufe, eine grosse Auswirkung und eine Tragweite aufweisen.

Tabelle 2.1: weiter auf nächster Seite

Tabelle 2.1: Weiterführung von vorheriger Seite

	SCION	IP/IPsec
Anonymity	Grundsätzlich unterstützt SCION keine anonyme Kommunikation. Mit der bereits erwähnten Erweiterung HOR-NET[6] kann eine hochperformante anonyme Netzwerkinfrastruktur auf Network Layer Ebene bereitgestellt werden.	Grundsätzlich unterstützt IP/IPsec keine anonyme Kommunikation. Partiiell kann mittels IPsec oder SSL im Tunnel Mode eine minimale Anonymität erreicht werden. Das Tor Projekt als IP Overlay Network ermöglicht durch Verschlüsselung und Onion-Routing eine anonyme Kommunikation im Internet.

Tabelle 2.1: Ende der Tabelle erreicht.

Die Vergangenheit verdeutlichte mit ihren evolutionär entstandenen Techniken und im Zusammenhang mit der vorangegangenen Auflistung wie komplex eine neue Internetarchitektur wäre, wenn sie die Under- und Overlay-Technologien zusammen beherrschen müsste. In der zweiten Halbzeit der Internet-Revolution scheint der Zeitpunkt gekommen zu sein, um das Internet mit neuen Technologien für die Zukunft aufzufrischen und zu optimieren.

2.3. Grundfragen und aktuelle Entwicklungen

Vor allem bei neuen Internetarchitekturen kommt verständlicherweise die Frage auf: Welche Konsequenzen oder Auswirkungen haben die neuen Technologien auf die Grund- und Menschenrechte¹¹? Wie sieht es denn mit der Anonymität¹² und der Netzneutralität¹³ aus? Wie schon mehrfach erwähnt, stand das Internet anfänglich für Jedermann und Jedefrau offen zur Verfügung. Relativ lange gab es keine Rechtsgrundlagen in Bezug auf Internetkriminalität. In der Schweiz sind sämtliche Serviceanbieter von Post-, Telefon- und Internetdiensten gesetzlich verpflichtet, gewisse Daten auf Vorrat für sechs Monate aufzubewahren. Die Vorratsdatenspeicherung¹⁴ verspricht ein einfacheres Strafverfolgungsverfahren bei illegalen Machenschaften in der Telekommunikation. Bei diesen Überwachungsmassnahmen sind ausnahmslos alle betroffen, daher schaffen sie bei den Politikern stets für angeregte Diskussionen. In der Gesellschaft werden sie meist als einen unverhältnismässigen Eingriff in den verfassungsmässig garantierten Schutz der Privatsphäre angesehen.

Um die eigene Privatsphäre zu schützen, ist es erlaubt, entsprechende Vorkehrungen zu treffen. Das heisst, jeder Internetnutzer kann und darf offiziell Verschleierungstechniken einsetzen, um seine Privatsphäre zu bewahren. Bei einer Google Search Abfrage nach „network anonymity“ erscheint an erster Stelle, vermutlich das bekannteste und effektivste anonyme Overlay Netzwerk weltweit, das auch unter Darknet bekannte Tor Project. Die Anonymität im Internet hat bekanntlich seine Vor- und Nachteile. Privatpersonen und Unternehmen gewährleisten so ihren vertraulichen und anonymen Informations- und Kommunikationsfluss, ohne negative Folgen oder Reaktionen gegen sich selbst, erwarten zu müssen. Oftmals können schon persönliche Meinungsäusserungen einen Imageschaden verursachen. Umgekehrt hat Anonymität ein nicht zu unterschätzendes Gefahrenpotential für kriminelle Machenschaften. SCION unterstützt standardmässig die

¹¹<https://www.digitale-gesellschaft.ch/2019/12/04/>

¹²<https://files.ifl.uzh.ch/hilty/t/examples/IEG/>

¹³<https://www.netzneutralitaet.ch/#sources>

¹⁴<https://www.amnesty.ch/de/themen/ueberwachung/ueberwachung-in-der-schweiz/>

Anonymity und Privacy im Netz nur begrenzt. Dank dem PCFS-Verfahren und der Pfadtransparenz kann der Weg vom Sender selbst vorbestimmt werden. Zusätzlich kann der Paket-Header policygesteuert in anderen ASes verschleiert werden. In diesem Zusammenhang wird von Hidden Paths gesprochen. Nicht direkt verbundene ASes können auf dem Pfad den Weg nicht über die Source- und Destination lernen oder ableiten. Die Erweiterung HORNET[6] bringt eine verbesserte anonyme Kommunikation mit hoher Bandbreite, sowie geringer Latenz auf der Netzwerkebene. Grundsätzlich ist HORNET in der Lage die Anonymität lediglich des Senders oder des Senders und Empfängers auf Netzwerkebene zu gewährleisten. Alle anderen Anonymitätsaspekte auf höherem OSI Layer z. B. verursacht durch Browser-Cookies oder Anmeldeinformationen werden daher nicht berücksichtigt. Vor allem in der heutigen Zeit ist die Privatsphäre hoch im Kurs. Überall hinterlassen wir vielzählige Spuren. Sie sind auf den besuchten Webservern oder lokalen Geräten (Computer, Smartphones etc.) vorzufinden. Nicht nur der Staat, sondern auch Google, Facebook & Co. tracken ihre Benutzer. Neue Internet Architekturen sollen möglichst Methoden zum Schutz der Privatsphäre unterstützen. Sie verschleiern und sichern nicht nur die Kommunikation, sondern schützen auch gegen manche Netzwerkangriffe. Jedoch ist es schwierig allen Anforderungen verschiedenster Parteien wie beispielsweise die von den Regierungen resp. den Gesetzgebern gerecht zu werden. Daher ist es wichtig bei der Entwicklung von neuen Technologien ein vertretbares Mittelmaß zwischen anonymer Kommunikation und der Rechenschaftspflicht zu finden.

In der Vergangenheit, war die freie Nutzung des Internets kein Problem, da es technisch unmöglich war in die Datenpakete hineinzuschauen und auszuwerten. Mittlerweile ist es möglich in Echtzeit eine Auswertung zu fahren und entsprechende Eingriffsmassnahmen vorzunehmen. Jeder darf das Internet unter denselben Bedingungen nutzen - das verspricht die Netzneutralität¹⁵ und möchte es so gut wie möglich beibehalten. Der Innovationsmotor hat seine Früchte getragen und entsprechend des Internets im Positiven, sowie im Negativen verändert und geprägt. Das soll auch künftig so bleiben. Alle Serviceanbieter möchten ihre Dienstleistungen mit bester Qualität oder mit dem Motto^{16,17} „You get what you pay for.“ anbieten können. Im Internet galten bisher dieselben Rechte und Spielregeln für alle. Der Konkurrenzkampf ist auf dem best-effort Netzwerk entsprechend gross und die Nachfrage nach einzelnen Bevorzugungen steigt. Manche Suchmaschinen oder Serviceprovidern nehmen schon heute gewisse Eingriffe vor und bevorzugen ihre eigenen Produkte, Dienstleistungen und Werbung. Weltweit wird schon lange über die Netzneutralität debattiert und manche Länder möchten die Netzneutralität gesetzlich verankern. Manche möchten es den Providern offenlassen. In der Schweiz steht noch die Vermeidung eines Zweitklasseninternets im Vordergrund. Meines Erachtens müssten alle Staaten weltweit am selben Strick ziehen, ansonsten macht eine gesetzliche Regulierung nur einen beschränkten Sinn und die stetige, innovative Entwicklung für Kleinunternehmen oder Start-Ups wird beträchtlich ausgebremst. Viele Fragen zur Netzneutralität sind sehr komplex und nicht einfach zu beantworten. Eine gerechtfertigte Regulierung ist sehr kostspielig, aufwändig und langwierig. Schlussendlich müssen alle Fragen unabhängig der darunterliegenden Internetarchitektur beantwortet werden, denn schon im heutigen Internet wird teilweise eine Priorisierung und Filterung gemacht. Da drängt sich die Frage vor, ob eine gesetzliche weltweite Regulierung überhaupt gewollt und durchsetzbar ist. Unabhängig von SCION setzten sich einige Wissenschaftler mit dem Thema „Transparenz anstelle von Neutralität“ ausgiebig auseinander und versuchen zusätzlich die Notwendigkeit der Transparenz im zukünftigen Internet aufzuzeigen. Der empfehlenswerte Artikel „Transparency Instead of Neutrality[49]“ gibt diesbezüglich zusätzliche Informationen und veranschaulicht indirekt die Vorzüge von SCION auf. Bestimmt ist es sinnvoll diese Themen auf internationaler Ebene auszudiskutieren und Regierungsvereinbarungen zu treffen. Der Stand der Technik ist genügend fortgeschritten und einer Service-Diskriminierung

¹⁵<https://www.srf.ch/news/panorama/internet-netzneutralitaet-was-ist-das-eigentlich>

¹⁶<https://www.netzneutralitaet.ch>

¹⁷<https://arstechnica.com/information-technology/2017/05/title-ii-hasnt-hurt-network-investment-according-to-the-isps-themselves/>

steht schon lange nichts mehr im Wege. Allgemein benötigen wir auch bestmögliche Transparenz im Internet durch entsprechende Netzwerk-Management und -Monitoring-Systeme, um eine gewisse Variabilität der eigenen Kommunikationsverbindungen zu erreichen und um Vorkehrungen gegebenenfalls einzuleiten[64]. Auch bei künftigen internationalen Vereinbarungen werden gewisse Massnahmen notwendig sein. Transparenz ist eines der Versprechen von SCION und selbstverständlich bringt SCION etliche Vorzüge bezüglich Steuerung und Beeinflussung der Pfadinformationen mit. Die PCBs und Path Segments werden basierend auf verschiedenen Pfadqualitätsmerkmalen (z. B. Policy, Bandbreite, Latenz, Auslastung und Verfügbarkeit etc.) gesteuert und ausgewählt. Der Sender kann selbst anhand der eigenen Datenschutzbestimmungen darüber entscheiden, über welche ASes die Verbindung aufgebaut wird und der Empfänger hat eine kryptografisch überprüfbare Pfadgarantie (EPIC-Erweiterung[35]). Das versetzt Organisationen in die Lage die Regularien einzuhalten, die es erfordern, dass der Datenverkehr innerhalb der Gerichtsbarkeit eingeschränkt wird. Wie bereits angesprochen möchten die Dienstanbieter auch unter allen Umständen ihren Kunden den versprochenen Service anbieten. Dabei unterstützt die Erweiterung COLIBRI[24] und ermöglicht eine globale und durchgehende Bandbreitengarantie zwischen Endhosts. Mit COLIBRI wird effektiver gegen Bandbreitenengpässe und DDoS Angriffe vorgegangen. Grundsätzlich wird zwischen garantierter und best-effort Datenflüssen unterschieden. Bleibt von der reservierten Bandbreite etwas übrig, kann der best-effort Bereich davon profitieren. Dynamisch werden die Verbindungen gesteuert und überwacht. Je nach Gebrauch können sogenannte Dynamic Inter-domain Leased Lines (DILLs) aufgeschaltet werden. Sollte das Internet zukünftig auf SCION basieren, so erscheinen die MPLS und Punkt-zu-Punkt-Mietleitungen (Leased Lines) nicht mehr benötigt zu werden, da solche Verbindungen künftig über eine einheitliche SCION-Plattform laufen. Das eröffnet ganz neue Möglichkeiten und fördert Innovationen. Vermutlich hat dieses Konzept zusätzliche Fragen bezüglich Netzneutralität aufgeworfen. Die Befürchtungen und Einwände mögen berechtigt sein. Sollte es wirklich soweit kommen, unabhängig von der Future Internet Architecture, so benötigt es eine vernünftige Regulierung des Internets auf internationaler Ebene. Eine Unterdrückung der finanziell schwächeren Unternehmen sollte der Innovationskraft zuliebe, wenn möglich verhindert werden.

2.4. Warum SCION?

Stark vom Markt getriebene Trends motivieren oder zwingen die Forscher zu revolutionären und evolutionären Projekten, welche das Internet optimieren oder neu erfinden. Zur Beschreibung des Internets der Zukunft werden in der Community etliche Buzzwords wie Security, Privacy, Availability, High Performance, Ultra Low Latency, Scalability, Transparency and Control, Compatibility, Interoperability, Expandability und Flexibility um sich geworfen. Die Wunschvorstellungen scheinen schier unendlich zu sein. Wie es die Vergangenheit zeigte, kann eine Clean-Slate Technologie wie SCION nicht zu Beginn alle geforderten Funktionalitäten perfekt unterstützen. Diese Meinung vertreten auch die SCION-Forscher und sie beschränkten sich vorerst auf die Netzwerkschicht mit den wichtigsten Funktionalitäten. Bestimmte Eigenschaften und Ziele wurden bewusst ausgeschlossen, die später als zusätzliche Funktionalität (z. B. Multicast) hinzugefügt werden könnten. Die Stärken von SCION liegen klar bei sogenannten Punkt-zu-Punkt-Kommunikationen und ist als Ersatz vom IP basierten Routingprotokoll BGP gedacht[52]. Seit ich mich mit diesem Thema auseinandersetze, bin ich immer mehr der Ansicht und Überzeugung, dass alle oben genannten Schlagwörter auf SCION relativ gut zutreffen. Eine Erklärung über die Hardfacts erhielten sie in der ausführlichen Einführung aus den vorangegangenen Kapiteln. Mir erscheint ein komplettes Internet-Redesign, begonnen auf den unteren Media Layers, der richtige und zielführendste Weg zu sein. Damit wir die bereits geforderten und kommenden Anforderungen an das Internet der Zukunft bestmöglich erfüllen, müssen wir uns vom

heutigen „Patchwork Design“ mutig lösen. SCION als mögliche zukünftige Internet Architecture benötigt bestimmt noch an manchen Punkten gewisse Optimierungen und Erweiterungen. Das ist verständlich und durchaus erwünscht, da SCION noch immer ein laufendes Forschungsprojekt ist und bisher noch keinen Request for Comments (RFC) verabschiedet wurde. Das sehr grosse Interesse und Ansehen, in der Internet Community mit dem Open Source Ansatz, verhalf zum grossen Entwicklungsfortschritt und sehr positivem Ansehen. Der Ansatz mit der Trennung von Forschung/Entwicklung und Implementierung war bestimmt der richtige Weg. An den Universitäten wird weltweit fleissig weiter Forschung betrieben und das Spin-Off-Unternehmen Anapaya Systems AG integriert, mit ihrem jungen und professionellen Entwicklerteam die Erweiterungen, und setzt die Industrieforderungen aus erster Hand um. Die internationalen Tests im SCIONLab und die bereits erfolgreich getätigten Feldversuche verhalfen zur besseren Stabilität und einem erweiterten Funktionsumfang. Auf die Anforderungen und Wünsche aus der Industrie kann und konnten so schneller und flexibler reagiert, berücksichtigt und integriert werden. Im Projekt SSFN konnte ich ein wenig den Netzwerkaufbau und die Inbetriebnahme mitverfolgen und begleiten. Die Implementierungen und Anbindungen ans SSFN verliefen, mit den normalen Anfangsschwierigkeiten und üblichen Herausforderungen wie man sie aus der IT kennt, sehr unbürokratisch und problemlos ab. Es beeindruckte mich, zu sehen, wie einfach und verständlich die Anapaya Integratoren die funktionierende SSFN-Infrastruktur, mit Messwerten untermauern und visualisieren konnten. Bei der Inbetriebnahme konnte ich einige Versprechen von SCION in der Praxis live miterleben. Dank dem bewusst begrenzten Funktionsumfang, konnte unnötige Komplexität herausgenommen werden und so blieb der modulare SCION Quellcode überschaubar. Über den gefestigten Entwicklungsprozess kann sehr schnell auf entsprechende Anpassungen reagiert werden. Im Entwicklungsprozess wird das Motto „Security by Design“ verfolgt, aber trotzdem werden die SCION Services zusätzlich und wiederkehrend von einem unabhängigen Dritten in einem Penetration Test auf Sicherheitslecks untersucht. Mir ist bisher noch keine neue Internet Architektur zu Ohren gekommen, die von der experimentellen Testevaluierung zu Technologieversuchen „Technology-Trials“ mit realen Benutzern und Anwendungen übergegangen ist. Ausserdem stellt es mich auf, zu sehen, wie gross das Interesse an SCION auf dem Schweizer Finanzplatz ist, um in den Kampf gegen Cyberrisiken vorzugehen. Wenn weiterhin so hart und qualitativ hochstehend an SCION gearbeitet wird, stehen meines Erachtens die Sterne für ein langes Bestehen und einem weiteren erfolgreichen Markteintritt nichts mehr im Wege.

SECURITY AUDIT TOOL EVALUATION

Auf der Suche nach dem potentiell richtigen Security Audit Tool, das den gewünschten Anforderungen am ehesten gerecht wird, wurden viele Anstrengungen unternommen. Es fanden einige Interviews von SIX internen Arbeitskollegen in unterschiedlichen Arbeitsbereichen statt. Wir sprechen hier von Corporate Security, Security Architecture und dem System Engineering. Das System Engineering beschäftigt sich hauptsächlich um die Hardware und das darauf laufende Betriebssystem. Für die Applikationen sind die Applikations Manager oder Platform Owner zuständig. Je nach Jobsparte fielen die Anforderungen und Wünsche an das Security Audit Tool teilweise sehr unterschiedlich aus. Dies machte natürlich die Evaluation nicht einfacher und führten eher zu mehr Herausforderungen. In der Industrie stehen etliche ausgewiesene, zertifizierte und von Gartner bewertete Technical Security Auditing Tools für Unix-Derivate und MS Windows zur Verfügung. Diese Lösungen sind kostenpflichtig und meist aufwändig in der Implementierung. Wir in der SIX unterstehen bekanntlich einigen regulatorischen Anforderungen und müssen etlichen Standards und Verordnungen gerecht werden, da kommen uns solche bewährten Produkte gelegen. Wir setzen vor allem auf die CIS Empfehlungen, weil die Regulatoren und viele andere namhafte Institute auch daraufsetzen, oder ihre Anforderungen davon ableiten und/oder erweitern. Firmenintern benutzen wir vorwiegend weitverbreitete und akzeptierte „Commodity“-Produkte mit Agent-based und Agent-less Lösungsansätzen. Trotz allen Nachteilen möchten wir, um die Security zu erhöhen, wenn immer möglich auf den Systemen einen Agenten einsetzen und darum entschieden wir uns für das Produkt „Tripwire Enterprise“. Obwohl wir sehr viel von der Community CIS halten, sind wir leider noch keine CIS Members. Die Mitgliedschaft hat einige Vorteile und ist kostenpflichtig. CIS selbst würde den Mitgliedern ein modifizierbares und erweiterbares CIS Benchmark Tool (CIS-CAT Pro) zur Verfügung stellen, das unseren Anforderungen hier sehr gut gerecht werden würde. Leider bietet sich, aus verschiedenen Gründen, für die genannten beiden Produkte in diesem Projekt und zu diesem Zeitpunkt, keine Gelegenheit und effiziente Einsatzmöglichkeit. Aus diesem Grund musste auf eine Open Source Lösung ausgewichen und evaluiert werden. Selbstverständlich können die SCION Tests, die in den nachfolgenden Kapiteln ausgearbeitet und definiert wurden, zu einem späteren Zeitpunkt relativ leicht z. B. in Tripwire umgesetzt und implementiert werden. Nachfolgend werden die Tool-Anforderungen, denen in der Evaluation ein besonderes Augenmerk und eine hohe Gewichtung galten, rudimentär aufgelistet. Die Auflistung ist nicht als vollständig und abschliessend zu betrachten. Sie gilt lediglich als Referenz und zeigt die groben Bewertungsschwerpunkte in der Evaluationsphase.

- * Das Projekt muss ein Lizenzmodell wie Open Source (GPL-3.0 License) oder ein ähnlicher EULA haben.
- * Das Projekt ist angesehen, bekannt und verzeichnete schon mehrere Auszeichnungen aus der Industrie.
- * Das Projekt unterstützt und ermöglicht die Prüfung von Empfehlungen und Anforderungen aus der Industrie.

- * Das Projekt unterstützt schon Out-of-the-Box, viele Tests, die von den NIST-, NSA- und CIS-Empfehlungen abgeleitet wurden.
- * Das Projekt besitzt und gewährleistet Massnahmen, die die Portabilität unter den verschiedenen Unix-Derivaten sichern.
- * Das Projekt wird von vielen Contibuters schon über mehrere Jahre weiterentwickelt und verbessert.
- * Das Projekt unterstützt gängige Programmiersprachen, um dem Projekt und unseren Anforderungen beizutragen.
- * Das Projekt wird auf GitHub gepflegt und geniesst ein hohes Ansehen „GitHub Star“ unter den Nutzern.
- * Das Projekt verzeichnet auf GitHub einen regen und relativ aktuellen Issue-Tracker „GitHub Issues“.
- * Das Projekt weist einen aktuellen Software Release und einfache Installation ohne Abhängigkeiten fremder Applikationen auf.
- * Das Projekt unterstützt eine Überprüfung von Remote-Systemen ohne Agent oder zusätzlicher und lokaler Applikationen.
- * Das Projekt bietet eine umfangreiche, vollständige, einfache und verständliche Dokumentation.
- * Das Projekt sollte überschaubar, relativ einfach und verständlich konzipiert sein, damit die Evaluation und Einarbeitungszeit so gering wie möglich gehalten werden kann.
- * Das Projekt gibt dank dem vorangegangenen Punkt die nötige Visibilität und gewährleistet so die Sicherheit, um mögliche Sicherheits- und Datenschutzverletzung, verursacht durch das Tool, zu erkennen und zu verhindern.

Die Tool-Evaluation fand grösstenteils, vor allem aufgrund von zeitlichen Aspekten, auf theoretischer Basis statt. Die Feedbacks aus den internen Interviews und der umfangreichen Literaturrecherche flossen in die Bewertungen ein. Auf eine tiefe und schriftlich nachvollziehbare Auswertungsmatrix wurde bewusst verzichtet und der Toolentscheid entstand auf reinen Eindrücken und Abwägungen aus Sicht des Autors. Die relevanten Punkte aus der Tool-Recherche wurden jedoch in dem Zwischenstatusmeeting 2 (siehe Beilage der elektronischen Fassung) präsentiert und besprochen. Schlussendlich wurde nur ein Security Auditing Tool, das in Anbetracht des Autors in die engere Auswahl kam, zusätzlich vertieft mit praktischen Aspekten und Analysen angeschaut. Nach der Code-Analyse stand schliesslich der finale Entscheid für „Lynis“ fest. Lynis entstand im Jahr 2007 und wird von einer grossen Community weiterentwickelt. Es wird vor allem als Security Auditing Tool für Systeme basierend auf UNIX eingesetzt und nutzt vollumfänglich aus Portabilitätsgründen die Bourne Shell „/bin/sh/“. Das Tool und die Tests sind übersichtlich und verständlich mit Shell-Skripts umgesetzt, daher muss es nicht installiert werden und nutzt lediglich die bereits vorhandenen Bordmittel. Der wichtigste Aspekt, in der Evaluation, ist bestimmt der letzte Punkt in der Auflistung. Anhand dem durchgeführten Code-Review konnten keine Security and Privacy Breaches festgestellt werden. Eine kostenpflichtige Version „Lynis Enterprise“ erweitert den Testumfang¹ mit zusätzlichen und hilfreichen Plugins und bereichert bezüglich Compliance das Reporting. Die bereits vorhandenen und kostenlos nutzbaren Tests kommen aus der Community und decken unseren Bedarf bei weitem nicht ab. Welche Tests die erweiternden Plugins beinhalten, konnte nicht in Erfahrung gebracht werden und daher müssen die Tests

¹<https://cisofy.com/compare/lynis-and-lynis-enterprise/>

in den nachfolgenden Kapiteln komplett neu überdenkt und ausgearbeitet werden.

Abschliessend möchten noch einige wichtige Optimierungspunkte und Ergebnisse auf den Tisch gebracht werden. Für einen künftigen und erfolgreichen, produktiven Einsatz erscheinen mir nachfolgende Punkte für wissenswert und sollten gegebenenfalls umgesetzt werden. Nach der theoretischen Ausarbeitung der umfangreichen Security Controls musste der Lynis Code für unseren Nutzen entsprechend angepasst und erweitert werden. Lynis selbst wird über ein Hauptskript mit dem Namen „lynis“ gesteuert und ist von vielen weiteren Hilfsdateien wie beispielsweise „default.prf“, „tests.db“ oder „languages/en“ und Hilfsprogrammen wie „binaries“, „consts“, „functions“, „osdetection“, „parameters“, „profiles“ oder „report“ etc. abhängig. Die genannten Beispiele sind nicht abschliessend zu verstehen und sollen lediglich einen Einblick über die Komplexität und Abhängigkeiten gewähren. Auch die angewandten Testmethoden und Parameterabfragen finden teilweise in unterschiedlicher Art und Weise statt. Vermutlich wegen der grossen Lynis Community ist es schwierig ein sauberes und einheitliches Konzept im Code zu bewahren. Bei Code-Erweiterungen sind also oft direkte Abhängigkeiten zu vorangegangenen Testresultaten gegeben, dass eine komplette Separierung resp. Trennung vom originalen Lynis-Code faktisch verunmöglicht. Es würden unweigerlich Redundanzen, mehrfach Überprüfungen und Performanceeinbussen beim Testdurchlauf entstehen. Was zudem deutlich wird, ist die Fehleranfälligkeit durch die Flexibilität und Mächtigkeit von Lynis selbst. Bevor Lynis als Auditing Tool für SCION im produktiven Umfeld zum Einsatz kommen soll, muss sich ernsthaft überlegt werden, auch gewisse Beiträge wie die Bugfixes und OS Hardening Tests mit der Lynis Community zu teilen. Denn jegliche gemachten Anpassungen und Erweiterungen an den genannten Beispieldateien und bestehenden Testskripten sind von allgemeinem Interesse und können nicht ohne erheblichen Aufwand unabhängig zum originalen Lynis Code herausgelöst werden. Mit diesem Vorgehen würden wir dem offenen Entwicklungsmodell gerecht werden und uns so viele zusätzliche Herausforderungen ersparen. Alle anderen SCION spezifischen Security Controls konnten in einer eigenständigen Testdatei abgebildet werden und müssten nicht zwangsläufig veröffentlicht werden. Mit diesem Vorschlag wären die grössten Probleme und Mehraufwände bei Lynis-Updates gelöst.

Als Teil dieser Thesis wurde eine einfache Gebrauchsanleitung „README_SCION“ erstellt. Sie soll die Installation, den Umgang und die Arbeit mit Lynis und vor allem den Einstieg in das Thema vereinfachen. Eine Ausarbeitung eines offiziellen und detaillierteren Betriebshandbuch wird daher empfohlen. Zusätzlich zur Unterstützung und einfacheren Handhabung wurde ein Hilfsprogramm namens „j2lynis.sh“ entwickelt. Es ist sehr einfach gehalten und wird vorwiegend zur Ausführung von lokalen und remote SCION Audits verwendet. Menügesteuert werden die einzelnen Audits ausgewählt und angestossen. Abschliessend an einen Remote-Audit folgt umgehend eine System-Bereinigung, damit das geprüfte SCION-System sauber und aufgeräumt bleibt. Lynis bietet Out-of-the-Box keine Funktion für Remote-Audits. Jedoch gibt es über eine Helper-Datei eine valable Empfehlung ab. Bei einer Sichtung der zusätzlich ausgearbeiteten Skripten sind die teilweise ausführlichen Kommentare auffallend. Sie dienen lediglich der Nachvollziehbarkeit der Arbeit und als Verweise zu den konkret ablaufenden Lynis-Tests. Das Lynis-Konzept schreibt grundsätzlich die Verwendung von kundenspezifischen Test-IDs vor. Diese Vorgabe konnte aus Gründen der Einfachheit und Effizienz nicht immer eingehalten werden. Da diese Informationen im produktiven Einsatz nicht mehr von Interessen sind, wird eine Bereinigung empfohlen. Der Aufwand ist sehr gering und überschaubar, daher ist eine Bereinigung schnell und unkompliziert umsetzbar.

SCION LABORUMGEBUNGEN

Die Forschung und Entwicklung rund um SCION verläuft turbulent und sehr erfolgreich. Ganz nach dem DevOps-Ansatz werden die Erweiterungen und Optimierungen in den Pilot-Umgebungen kundenseitig implementiert und getestet. Auch während der Ausarbeitungszeit der Thesis verzeichneten wir einerseits in der Funktionsart und andererseits im Funktionsumfang einige Veränderungen. Daher ist es notwendig die untersuchten SCION-Images auch mit dem jeweiligen Forschungsstand zusätzlich zu deklarieren. Es dürfen keine Ungereimtheiten im Verlaufe des Projektes aufkommen, ansonsten könnten die Analyseergebnisse fehlinterpretiert oder missverstanden werden. Dieses Kapitel dient daher einer groben Beschreibung und Darstellung der Trainings- und Testumgebung, einer Veranschaulichung des Funktionsumfangs und der gewählten SCION-Konfiguration. Eine detaillierte Erläuterung der ausgeführten SCION-Applikationen sowie der Darstellung, welche Untersuchungsmethoden in welchem Fall angewendet wurden, erfolgt jeweils in den dafür vorgesehenen Kapiteln.

4.1. SCION Trainingsumgebung

Die vertiefte, praktische Einarbeitung in die SCION Systeme und Services fand vorallem in den beiden Wochen zwischen dem 7. – 20.09.2020 mittels der von Anapaya Systems AG entwickelten SCION Trainingsumgebung statt. Die in der Cloud aufgebaute Trainingsumgebung wird hauptsächlich zur fundierten Ausbildung von Partnern und ISP-Administratoren verwendet und entspricht oft nicht dem aktuellsten Softwarestand (siehe dafür auch Unterabschnitt 4.2.5 „Software“). In der Thesis unter dem Themenbereich „Docker Security“ setzen wir uns ausgiebig mit den SIG-Services und deren Funktionalitäten einer einzelnen SCION-Appliance auseinander. Ein grundlegendes SIG-Verständnis ist nicht wegzudenken und wird für diese Arbeit vorausgesetzt, um die ausgearbeiteten SCION-Security-Controls und forensischen Analysen nachvollziehen und verstehen zu können. Aufgrund der erwähnten Schnelllebigkeit von SCION entstand die Ausarbeitung der einleitenden Themen unter Kapitel 1 „Einleitung“ und Kapitel 6 „Docker Security“ mit Hilfe von nicht mehr aktuellem Software- und Literaturstand. Das führt nicht vor grundsätzliche Probleme, da die untersuchten Konfigurationen und elementaren SCION-Funktionen immer noch dieselben sind. Die Unterschiede zu aktuelleren Releases liegen vor allem im Design und den erweiterten Funktionalitäten, die für die vorliegende abgegrenzte Arbeit nicht zu Schwierigkeiten oder Mängel führt.

4.2. SCION Testumgebung

In den nachfolgenden Unterkapiteln werden die wichtigsten Bausteine für die vorliegende Arbeit kurz aufgeführt, spezifiziert und erläutert. Die Transparenzschaffung verschafft die nötige Klarheit und ein besseres Verständnis für das weitere Vorgehen und andererseits verhilft es, für eine vereinfachtere und nachträgliche Nachvollziehbarkeit der Analyseergebnisse.

4.2.1. Hardware

Als effektive und pragmatische Arbeitsumgebung genügt ein leistungsfähiges Notebook, mit relativ grosser Festplattenkapazität als Host, mit einer geeigneten Virtualisierungssoftware für die benötigten SCION-Gastsysteme aus. Für die Untersuchungen und automatisierten Spurenanalysen genügt der aufgeführte Rechner gemäss den Spezifikationen Tabelle 4.1 aus.

Funktion	Hardware	Spezifikationen	Betriebssystem
VBox Host	Apple MacBook Pro	Prozessor: Intel Core i7 Speicher: DDR3 16GB Disk: APPLE SSD SM0512G Netzwerk: Apple 57762-A0 1Gbs	macOS Big Sur v11.2.3

Tabelle 4.1.: Hardware Spezifikation

4.2.2. Virtuelle Maschinen

Alle Untersuchungen wurden einfachheitshalber und zur besseren Nachvollziehbarkeit in einer virtuellen Umgebung durchgeführt. Auf dem Host lief die Virtualisierungssoftware VirtualBox¹ mit der Version 6.1.18 r142142 (Qt5.6.3), die frei erhältlich als Open Source Software heruntergeladen werden kann. Die Tests respektive Auswertungen können somit hardwareunabhängig beliebig wiederholt und verifiziert werden. Die Nachfolgende Tabelle 4.2 gibt Aufschluss über die verwendeten virtuellen Gastbetriebssysteme mit deren Spezifikationen. Alle Security- und Forensik-Analysen fanden an den Untersuchungsobjekten mit denselben vPC-Spezifikationen statt. Den nachfolgenden drei vPCs namens Admin- und Forensik-Workstation kommen besondere Funktionen zu. Der MacBook und die Admin-Workstation werden als sogenannte Jumphosts verwendet und führen die Remote-Zugriffe und Security Benchmarks mittels dem Audit-Tool durch. Mit dem MacBook zusammen wurden die forensischen Image-Analysen^{2,3,4} mit den etwas leistungsfähigeren Forensik-Workstations durchgeführt.

¹ORACLE VirtualBox [<https://www.virtualbox.org>]

²Digital Forensics XML and the DFXML Toolset

³Open Source Digital Forensics „Autopsy and The Sleuth Kit“

⁴AccessData „FTK Imager“

Funktion	Hardware	Spezifikationen	Betriebssystem
VBox Gast	vPC	Untersuchungsobjekte Prozessor: 1 CPU Speicher: 512MB vDisk: ATA 64GB Netzwerk: Intel Pro 1Gbs (Bridge)	Ubuntu 18.04.5 LTS (5.4.0-52-generic x86_64)
VBox Gast	vPC	Admin-Workstation Prozessor: 2 CPUs Speicher: 512MB vDisk: ATA 64GB Netzwerk: Intel Pro 1Gbs (Bridge)	Ubuntu 18.04.5 LTS (5.4.0-52-generic x86_64)
VBox Gast	vPC	Forensik-Workstation (Linux) Prozessor: 4 CPUs Speicher: 4GB vDisk: SATA 10GB Netzwerk: Intel Pro 1Gbs (Bridge)	Ubuntu 18.04.3 LTS (5.0.0-37-generic x86_64)
VBox Gast	vPC	Forensik-Workstation (Windows) Prozessor: 4 CPUs Speicher: 16GB vDisk: SATA 100GB Netzwerk: Intel Pro 1Gbs (Bridge)	Windows 10 Pro (v2004-19041.867 x86_64)

Tabelle 4.2.: Spezifikation der virtuellen Maschinen

4.2.3. Images

Bezüglich Security Benchmarking gilt grundsätzlich nur eines der endgültigen SCION-Images „anapaya-SCION-SIX-[x]“ als das zu untersuchende Objekt. Dieses und alle anderen Images wurden vor allem für die forensischen Spurenanalysen verwendet. Die Generation der jeweiligen Images⁵ seitens Anapaya Systems AG startete am 24.09.2020 und wurden final am 29.10.2020 zur Verfügung gestellt und bestmöglich der Realität entsprechend automatisiert aufgesetzt. Das heisst, sie gelten dem damaligen aktuellen Wissens- und Konfigurationsstand bei SIX. Das verfolgte Ziel war, dass die einzelnen SCION-Images für den Betrieb grundsätzlich einsatzbereit und funktionsfähig sind. Für die Untersuchungen sind keine lauffähigen SCION-Services notwendig. Sie können nur gestartet werden, wenn alle erwarteten NICs korrekt konfiguriert und vorhanden sind. Zudem müssen sie im SIG-HA-Cluster-Konstrukt kommunizieren können. Die Begründung, warum hier teilweise mehrere Disk-Image-Versionen aufgelistet sind, folgt später zum gegebenen Zeitpunkt unter im Kapitel 7 „Forensische Analyse“.

MD5 (anapaya-base-disk001.vmdk) = 2928c2f2450323bc78cd42fe30598924

MD5 (anapaya-base.ovf) = dd82d5e2214f057f2861731e99e17158

MD5 (anapaya-configured-SIX-1.ova) = 8275bc6e8a239c603a74a546f13fa01d

MD5 (anapaya-configured-SIX-2.ova) = 4104f4e919b2ce226fe7926c298e3911

MD5 (anapaya-configured-SIX-3.ova) = aec4e1d714619cb035164c9a60f4b349

MD5 (anapaya-SCION-SIX-1.ova) = 275a29c18203513f20a357fc57ab6cc3

MD5 (anapaya-SCION-SIX-2.ova) = 74d2510f8f141fd21659554d08e9a917

MD5 (anapaya-SCION-SIX-3.ova) = 3e746697022c50340a5fcfbacaeb9466

⁵https://anapaya-my.sharepoint.com/:f:/r/personal/bischofberger_anapaya_net/Documents/SIX%20Andreas%20Maure%20r?csf=1&web=1&e=G8NR1u

Die bereitgestellten SCION-Appliance-Konfigurationen „anapaya-configured-SIX-[x]“ sind bereits kundenspezifisch gehärtet und unterscheiden sich zu anderen Kundenkonfigurationen hauptsächlich in den Infrastrukturservices. Beispielsweise sind Diskrepanzen in den üblichen und bekannten Punkten auf Betriebssystemebene wie Host- und Domainnamen, IP-Adressen, Benutzer, Passwörter usw. auszumachen. Selbstverständlich kann es teilweise auch Abweichungen in einigen Hardening-Massnahmen geben, da sie von den firmeneigenen Weisungen abhängig sind. Die eigenen SCION-spezifische Konfigurationen unterscheiden sich bei jedem Kunden grundsätzlich immer, aber haben keinen Einfluss auf die hier ausgearbeiteten allgemeinen Untersuchungen.

4.2.4. Konfigurationen

Die ausgelieferten SCION-Appliances werden seitens Anapaya Systems AG vor der kundenseitigen Auslieferung mittels Ansible Playbooks bestmöglich vorkonfiguriert. Da die vorliegende Thesis möglichst der Realität entsprechen soll, wurden aus Integritätsgründen alle zuvor genannten SCION-Images über die unteren aufgeführten Ansible Playbooks (Tarball) bereitgestellt.

MD5 (ansible.tar) = b42ac46019e98dad0ada766c21f4e5f2

Welche Konfigurationen die unterschiedlichen Images bei der Auslieferung bereits erhalten haben, möchten nachfolgend grob in aufzählender Form deklariert werden. Die Übersicht gibt zudem einen guten Einblick über die einzelnen Konfigurationsschritte der Ansible Playbooks. Genauere Details entnehmen Sie bitte gerne direkt von, den in elektronischer Form abgelegten Playbooks, der beigelegten CD-Rom.

Dem öffentlich erhältlichen Ubuntu-Image wiederfahren direkt nach dem Download und nach der OS-Installation zum sogenannten **Base Image „anapaya-base-disk001“** bereits die folgenden Veränderungen:

- * Admin User Accounts (SSH Keys)
- * Code Repositories
- * APT Packages
- * Docker Engine

Aufgrund von fehlenden Informationen und den vorliegenden Datenabbildern wird, nach Rücksprache mit Anapaya Systems AG, auf eine forensische Untersuchung dieses Installationsschrittes bewusst verzichtet. Der darauffolgende Schritt führt uns mittels den weiteren und eher kundenspezifischen IP-Infrastruktur- und OS-Einstellungen, zum sogenannten teils gehärteten **Anapaya Base SIX Image „anapaya-configured-SIX-[x]“**. Er ist als vorbereitender Zwischenschritt, zur nahezu fertigen SCION-Appliance, anzusehen.

- * SCION Users
- * SSH Configuration
- * Hostname- and Network-Configuration
- * Dynamic IP-Routing Configuration (BGP/Quagga)
- * DNS- and NTP-Configuration
- * Iptables (Firewall/ACLs)
- * Monitoring Tools (process-exporter, node-exporter and blackbox-exporter)

- * Monitoring Scripts
- * Logging (Journald)

Zu guter Letzt erfolgt die Installation und Konfiguration der benötigten SCION-SIG-Services. Nach der erfolgreichen Einrichtung, welche zuvor von einem SCION-Spezialisten in seiner Testumgebung verifiziert wurde, standen die SCION-Services lauffähig zur Verfügung. Die abgeschlossene SCION-Installation, wurde dann im **Anapaya SCION SIX Image** „anapaya-SCION-SIX-[x]“ festgehalten.

- * SCION Border Router (BR) aka posix-router
- * SCION IP Gateway (SIG) aka posix-gateway
- * SCION SIG Confagent
- * SCION Services (dispatcher, sciond and cs)

Mit welchen Konfigurationen und unter welchen Bedingungen die Admin- und Forensik-Workstations liefen, ist hier nicht von Relevanz und werden daher nicht erläutert.

4.2.5. Software

An dieser Stelle möchten die für die Thesis relevanten Softwares mit ihrem Entwicklungsstadium aufgenommen werden. Zu welchem Zeitpunkt die Software-Version massgebend ist, wird in der entsprechenden Beschreibung erwähnt. Detailliertere Programm-Beschreibungen werden hier nicht als angemessen erachtet. Sollten jedoch vertiefte Erklärungen zum Themenschwerpunkt als notwendig erachtet, so werden sie dort direkt aufgenommen und vertieft, ansonsten konsultieren Sie bitte die Hersteller-Webseiten oder Code-Kommentaren.

Tabelle 4.3.: Eingesetzte Analyse- und SCION-Softwarestände

Applikation	Beschreibung	Version
SCION SIG SRV (legacy)	Das SIG wird als Schnittstelle (Gateway) zwischen dem SCION- und IP-Netzwerk verwendet. Der als legacy bezeichnete Softwarestand wird in der SCION-Trainingsumgebung zu Schulungszwecken eingesetzt. Alle Erläuterungen zu den SCION Systemen und Services entstanden auf dieser Basis.	ana-v0.11.7
SCION MON SRV (legacy)	Die SCION-Monitoring-Services werden für das Auslesen der Metriken und zur Visualisierung in Grafana Prometheus eingesetzt. Auch dieser als legacy bezeichnete Softwarestand wird momentan noch in der SCION-Trainingsumgebung zu Schulungszwecken eingesetzt. Alle Erläuterungen zum SCION-Monitoring entstanden auf dieser Basis.	blackb-v0.16.0 node-v0.18.1

Tabelle 4.3: weiter auf nächster Seite

Tabelle 4.3: Weiterführung von vorheriger Seite

Applikation	Beschreibung	Version
BGPv4/v6 Router (legacy)	Die BGP/Quagga-Router-Funktionalität bezüglich dynamischem/statischem IP-Routing wird in der Trainingsumgebung noch zu Schulungszwecken als Services ausserhalb von Containern betrieben. Jegliche Erläuterungen zum Thema dynamischen IP-Routing basieren auf dieser Konfiguration und dem Softwarestand.	quagga-v1.2.4
SCION SIG SRV (SIX)	Beruhend auf diesem SIG-Softwarestand, bestanden die Ausarbeitungen der Security Controls und die daraus resultierten Benchmark-Ergebnisse, sowie forensischen Untersuchungen.	ana-v0.16.1
SCION MON SRV (SIX)	Auch hier wieder, stützen sich die ausgearbeiteten Security Controls und die daraus resultierten Benchmark-Ergebnisse, sowie forensischen Untersuchungen auf diesem Entwicklungsstand.	blackb-v0.17.0 node-v1.0.1
BGPv4/v6 Router (SIX)	In neueren SCION-Releases werden die IP-Router-Funktionalitäten in Containern abgebildet und zusätzlich geschützt. Diesbezügliche Security Controls und die daraus resultierten Benchmark-Ergebnisse, sowie forensischen Untersuchungen basieren auf diesem Entwicklungsstand.	quagga-v1.2.4
Lynis Auditing Tool	Alle erarbeiteten Security Benchmarks werden mit zusätzlichen Audit-Profilen im aktuellen Lynis-Release aufgenommen und durchgeführt. Der daraus resultierende Testbericht wird als Text-Datei auf dem System für die nachträgliche Einsicht abgespeichert.	lynis-v3.0.3
TestDisk Data Recovery	TestDisk ist ein Kommandozeilenprogramm zur Datenrettung auf Festplatten-Partitionen. Daher kann es auch für die reine Analysen von Datenträgern und Partitionen verwendet werden.	v7.1
FTK Imager	Forensic Toolkit (FTK) ist eine Computerforensik Software von AccessData. Es durchsucht eine Festplatte nach verschiedenen Informationen. FTK ist auch mit einem eigenständigen Disk Imaging-Programm namens FTK Imager verbunden. Dieses Tool speichert ein Image einer Festplatte in einer Datei oder in Segmenten, die später möglicherweise rekonstruiert werden.	v4.3.1.1

Tabelle 4.3: weiter auf nächster Seite

Tabelle 4.3: Weiterführung von vorheriger Seite

Applikation	Beschreibung	Version
Autopsy & The Sleuth Kit	The Sleuth Kit ist eine Sammlung von forensischen Tools. Mit Hilfe dieser ist es möglich, verschiedenste Informationen über ein Computersystem oder ein Speicherabbild zu erhalten.	autopsy-v4.18.0 tsk-v4.10.2
LVM2	Logical Volume Manager kann Partitionen auch über mehrere Festplatten hinweg dynamisch verwalten. Es wird eine zusätzliche logische Schicht (Abstraktionsschicht) zwischen Partitionstabelle und den Dateisystemen hinzugefügt.	v2.02.176- 4.1ubuntu3.18.04.3
Kpartx	Kpartx liest Partitionstabellen auf dem angegebenen Gerät und erstellt Gerätezuordnungen über erkannte Partitionssegmente.	v0.7.4-2ubuntu3
Plaso Tools	Plaso wird für die automatische Erstellung von Super-Timelines verwendet. Es stellt ein einziges Werkzeug dar, das verschiedene Log-Dateien und forensische Artefakte von Computern analysieren kann, um eine einzige korrelierte Zeitleiste zu erstellen.	v20210412- 1ppa1~bionic
Extundelete	Extundelete kann gelöschte Dateien von einer Ext3- oder Ext4-Partition wiederherstellen. Es verwendet die im Journal gespeicherten Informationen, um zu versuchen die gelöschten Dateien wiederherzustellen.	v0.2.4-1ubuntu1
Ext4magic	Ext4magic stellt etwas mehr Funktionen als Extundelete zur Verfügung und soll zudem mit noch mehr Heuristik gelöschte Dateien von einer Ext3- oder Ext4-Partition wiederherstellen. Es verwendet zusätzlich auch die im Journal gespeicherten Informationen, um zu versuchen die gelöschten Dateien wiederherzustellen.	v0.3.2-7ubuntu1
Python Forensik Tools	Für die forensischen Untersuchungen und zur Ermittlung der SCION-Spuren in den jeweiligen Images wurde ein Python-Skript entwickelt. Das Skript schreibt die Spurenbilder in unterschiedliche Dateien, die anschliessend manuell ausgewertet und dokumentiert werden.	pytools-v2.1 ⇒ pe.py ⇒ me.py ⇒ ce.py

Tabelle 4.3: Ende der Tabelle erreicht.

Wie aufgefallen, finden Sie keine Angaben betreffend den Forensik-Tools von NIST. Die Forensik-Workstation wurde von der Universität⁶ bereits vorbereitet und als Open Virtual Appliance namens DFXML⁷ zum Download bereit gestellt. Das darauf enthaltene DFXML-Repository⁸ ist grundsätzlich auf GitHub öffentlich erhältlich. Das verwendete DFXML-Toolset besteht aus einem Satz von Python-Skripts, daher möchte aus Integritätsgründen und zur sichereren Nachvollziehung der Testresultate auf das Image selbst verwiesen werden. Alle anderen Analysetools, die auf der Linux-Forensik-Workstation installiert und eingesetzt wurden, entnehmen Sie bitte der oberen Tabelle 4.3.

⁶Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

⁷<https://fau11-files.cs.fau.de/protected/brap/dfxml.ova>

⁸<https://github.com/simsong/dfxml>

ANAPAYA - APPLIANCE OS SECURITY

Während der Einarbeitungsphase und den unzähligen Gesprächen mit den Spezialisten von Anapaya Systems AG, stellten sich einige interessante Fakten und daraus resultierende Erkenntnisse heraus. Im ISD-SSFN betreibt SIX eine seltene resp. einmalige High-Availability CS-Cluster-Konfiguration und eine vorübergehende befristete Certification Authority. Wie in der Abbildung 1.3 im rot umkreisten Bereich ersichtlich, betreibt SIX eine CA für alle SSFN-Kunden-AS und stellt als Issuer die AS-Zertifikate aus. Ein Kunde sollte einerseits kein Issuer sein und andererseits nicht unterschiedliche Betriebssysteme auf den SCION Appliances betreiben. Das Issuing sollte, wenn immer möglich, eine unabhängige Vertrauensstelle wie z. B. SwissSign AG übernehmen. Eine solche Verantwortung dürfte kein Kunde tragen müssen. Anapaya Systems AG als SCION Integrator empfiehlt, auf ihren Appliances ganz klar, als OS das Ubuntu Linux. Das Ubuntu-Betriebssystem wurde für den Betrieb der SCION Services speziell vorbereitet, geprüft und abgenommen. SIX setzt intern auf Red Hat als Standard-Linux-Distribution und betreibt, mit Rücksprache von Anapaya Systems AG, ausnahmsweise und temporär, im CS-Cluster-Konstrukt einen Red Hat Server. Mit anderen Worten, besteht der CS-Cluster aus zwei Ubuntu-Appliances und einer dedizierten Red Hat-VM. Auf Ubuntu laufen die zwei Border Router mit den Control Services und auf einer dedizierten VM läuft Red Hat mit einer eigenständigen Control Service Instanz. Nur weil SIX die Issuer-Funktion innehat und für Zertifikatsabfragen stets zur Verfügung stehen muss, werden aus Redundanzgründen drei CS-Instanzen gefordert. Wie sie sehen, ist der momentane SSFN-Aufbau bezüglich CA- und CS-Services bei SIX nur von temporärer Bedeutung. Nach der Pilotphase stehen in der Vorbereitungsphase für die SSFN-Produktion konzeptionelle und strukturelle Korrekturen bevor. Abweichend zur initial angedachten Konfiguration, sehen die Techniker seitens Anapaya Systems AG keinen gerechtfertigten Mehrwert mehr bezüglich einer Plattform-agnostischen Überprüfung der Security Controls. Aufgrund dessen einigten wir uns, auf die sinnvolle Beschränkung des empfohlenen Ubuntu-Betriebssystems.

5.1. Einleitung OS Baseline Security

Die Cyber Security setzt sich früh, in der Entwicklung von Applikationen, mit möglichen potenziellen Schwachstellen und Risiken auseinander. Ein sogenanntes Threat Modeling (Bedrohungsmodellierung) wurde seitens ETH Zürich und Anapaya Systems AG bereits umgesetzt und wird in einem laufenden und etablierten Prozess gelebt. Wie heisst es so schön: Vertrauen ist gut und Kontrolle ist besser! Genau nach diesem Motto wurden die Kontrollen generell ausgearbeitet. Grundsätzlich liefert das System ohne abgestimmte Massnahmen eine sehr grosse Angriffsfläche für Angreifer. Ein komplett abgeschottetes System kann seine Dienste nicht wahrnehmen. Trotz den potenziell lodernden Gefahren, müssen funktionsbedingte Vertrauensgrenzen wie für APIs und andere Serviceschnittstellen geschaffen werden und eine minimale Angriffsfläche von innerhalb und ausserhalb des Betreibernetzwerkes gewähren. Grundsätzlich

wird dem OS mit den Bordmitteln selbst das „Vertrauen“ geschenkt und beschränken den Fokus hier auf die abgestimmten SCION Services und minimal notwendigen OS-Konfigurationen. Verständlicherweise ist das erwähnte Vertrauen sehr beschränkt und daher findet ein Vulnerability Management dediziert durch den Systemintegrator Anapaya Systems AG und unserem internen SIX SOC statt. Jegliche OS-relevante Tests sind in unterschiedlichen Lynis-Test-Gruppen abgebildet und dokumentiert. Sie können gerne auf der beiliegenden CD-ROM eingesehen werden. Nachfolgend finden sie die Abweichungen zur momentan bestehenden gehärteten Anapaya-Konfiguration mit entsprechenden Begründungen zu den Empfehlungen und den absolut unverzichtbaren Konfigurationen. Mit der Überprüfung der angehenden Router-Konfiguration, durch die ausgearbeiteten Kontrollen, kann der Angriffsvektor direkt auf das Betriebssystem und die darauf laufenden Applikationsservices möglichst tief gehalten werden. Wenn möglich, werden die Kontrollen mit den verwandten CIS-Empfehlungen im Lynis-Skript¹ referenziert. Die ausgearbeiteten Linux-Härtungsmassnahmen beruhen auf sehr umfangreicher Literatur[1][11][15][32][63][65] und anderen verlässlichen Internet-Quellen[4][9][69]. Offensichtlich sind sich die namhaften Autoren, Softwareentwickler und Sicherheitsexperten weltweit in der Notwendigkeit und den umzusetzenden resp. zu berücksichtigenden Massnahmen einig und kommen meistens auf die gleichen oder sehr ähnlichen Empfehlungen. An dieser Stelle ist es äusserst wichtig anzumerken, dass sich die Kontrollen und Empfehlungen mit ganz klaren Sicherheitsvorteilen für SCION IP Gateways stützen. Bei einem SIG läuft nebst den SCION Services meist auch noch einen dynamischen IP-Routing-Service zumeist z. B. für OSPF oder BGP. Auf einem reinen SCION Border Router, so wie sie momentan bei den ISPs vorzufinden sind, werden keine zusätzliche dynamische Routing-Services betrieben. Das unterliegende IP-Netzwerk zwischen den BRs ist das reine Peering-Subnetz für SCION als Overlay. Unter diesen Umständen könnten wir bei den BRs manche sicherheitsrelevanten Einstellungen gegen Netzwerkangriffe restriktiver handhaben. Der Nutzen der SCION Technologie darf auf keinen Fall beeinträchtigt oder beeinflusst werden. Die Konfigurationsvorgaben müssen unbedingt nachträglich von Spezialisten verifiziert und bei Bedarf in einer Testumgebung getestet werden. Eine direkte Umsetzung wird daher nicht empfohlen. Ausserdem müssen die Kontrollen, nach jeder Änderung am Betriebssystem oder an den darauf betriebenen Applikationen, überprüft und abgestimmt werden. Wie einleitend angesprochen bedeutet dies einen weiteren Schritt im Prozess der Software-Wartung.

5.2. Empfehlungen zur Systemhärtung

In den Test-Skripten und in den nachfolgenden Erläuterungen finden sie einen aus vier Buchstaben zusammengesetzten Präfix, gefolgt von einer fünfstelligen Testnummer. Anhand des Präfixes kann der Name zum Testblock abgeleitet werden und die fünfstellige Testnummer referenziert innerhalb des Test-Skripts die Kapitelnummer der entsprechenden Tests. Die Überschrift im Test-Skript liefert dem Leser einen kurzen Beschrieb und vereinzelt eine zusätzliche Begründung der einzelnen Tests. Gesamthaft geht es hier um mehr als 200 fundierte Linux-Security-Checks, aus denen über 100 Testfälle für die Anapaya Appliance ausgearbeitet und zusammengestellt wurden. Nachfolgend konzentrieren wir uns besonders um erwähnenswerte Kontrollen und um nachzuholende Hardening-Konfigurationen, die von den umfangreichen Testfällen abgeleitet wurden. Direkt darauffolgend an die Testüberschrift finden sie einen Vermerk SCORED oder NOT_SCORED. Mit dieser Kennzeichnung möchte die Wichtigkeit der Empfehlung besonders hervorgehoben und bei der Gesamtbewertung entsprechend berücksichtigt werden.

¹Die Tests befinden sich auf der CD-ROM in der Datei „Auditing/B - lynis-v3.0.3_SCION_VERSION/lynis/include/tests_anapaya_appliance“. Bitte beachten Sie, bei der Durchsicht besonders auf die Kommentare und Querverweise, da sie einige wichtige und hilfreiche Informationen zu den SCION Erweiterungen geben, gewisse Tests bereits in Lynis standardmässig enthalten waren und in die bestehenden Skripts verbaut wurden. Dieser Umstand hat konzeptionelle Gründe und möchte hier nicht weiter erläutert werden.

5.2.1. File System [FILE]

FILE-00111 - Unused Filesystem SCORED

Das Ubuntu Linux unterstützt viele ungebräuchliche Dateisysteme. Es wurde festgestellt, dass viele File System Drivers auf dem System geladen werden können. Um die lokale Angriffsfläche zu minimieren, macht es Sinn, die nicht unbedingt benötigten Dateisysteme zu deaktivieren. Nicht native Dateisysteme können zu unerwarteten Konsequenzen für die Sicherheit und Funktionalität des Systems führen, da sie nicht regelmässig gewartet werden. Ein SCION-Router benötigt für seine Funktionalität grundsätzlich nur wenige Dateisysteme. Das Betriebssystem läuft vor allem auf den für Linux-Betriebssysteme entwickelte Extended File System Version 4 (EXT4). Alle anderen unterstützten Dateisysteme könnten grundsätzlich mit Wohlbedacht deaktiviert werden. Jedoch ist Vorsicht geboten, wenn UEFI anstelle von BIOS eingesetzt wird oder portable USB-Geräte am Router angeschlossen werden sollten. UEFI ist ein eigenes kleines Betriebssystem das wie ältere USB-Speicher auf FAT angewiesen sind. Daher ist es aus betrieblichen Gründen nicht empfehlenswert die beiden FAT/FAT32-Dateisysteme zu deaktivieren.

FILE-00112 - Separate Partitions SCORED

Die Benutzerdaten sowie geteilte Verzeichnisse z.B. für systemweite Funktionen müssen auf separaten Partitionen liegen. Es wurde festgestellt, dass viele Verzeichnisse keine eigene Partition besitzen oder der Temporary File Storage (tmpfs) „/dev/shm“ das Ausführen von Binärdaten erlaubt. Konkret handelt es sich um die Verzeichnisse „/tmp“, „/var“, „/var/tmp“, „/var/log“, „/var/log/audit“ und „/home“. Einerseits bietet es einen erhöhten Schutz vor Erschöpfung der Speicherressourcen, der Auditdaten und vor unberechtigter Ausführung von Applikationen in Benutzerverzeichnissen oder Systempartitionen. Durch strenge Mount-Optionen kann die Verwendung der Verzeichnisse besser definiert und das Ausführen von Schadsoftware vermindert resp. verhindert werden. In vereinzelten Fällen, müssen jedoch operative Arbeiten im temporären Verzeichnis wie z.B. „/var/tmp“ ausgeführt werden und machen eine kurzzeitige Ausführung von Test-Anwendungen oder Skripts unumgänglich. Aus diesem Grund kann bei vereinzelten Verzeichnissen eine begründete Ausnahme bestehen.

FILE-00113 - World-writable Directories SCORED

Auf einem gehärteten System ist es essenziell wichtig, zu verhindern, dass andere Benutzer in fremden Verzeichnissen gewisse Daten modifizieren können. Das Setzen vom Sticky-Bit in weltweit beschreibbaren Verzeichnissen verhindert, dass Benutzer fremde Dateien im Verzeichnis nicht löschen oder umbenennen können. Bei einem kurzen Test wurde festgestellt, dass auf dem Verzeichnis „/var/tmp/cores“ das Sticky-Bit fehlt. Eine Verifikation und Bereinigung ist daher nötig.

FILE-00115 - Disable USB Storage SCORED

Zusätzlich zum deaktivierten Automounting von externen USB-Geräten wird auf den Server- und Router-Systemen empfohlen, den USB-Zugriff zu verhindern. Diese Massnahme verringert zusätzlich zu den gut überwachten und gesicherten Datacentern die physikalische Angriffsfläche. USB-basierte Malware ist ein einfaches und weit verbreitetes Mittel zur Netzwerkinfiltration. Erst recht ist bei SCION eine gewisse erhöhte Vorsicht geboten, da alle vertrauenswürdigen AS-Informationen auf den Geräten präsent sein müssen. Selbstverständlich ist es nicht immer einfach und sehr umständlich, wenn auf den Datenaustausch mittels USB verzichten muss. Jedoch sollte es im täglichen Betrieb nach der erfolgreichen Inbetriebnahme ein Leichtes sein darauf verzichten zu können und die notwendigen Daten über das gesicherte Netzwerk zu transportieren. Eine zukünftige temporäre Aktivierung wird durch diese Vorsichtsmassnahme nicht ausgeschlossen.

5.2.2. Software Updates [SWUP]

SWUP-00211-13 - Software Updates and Security Patches NOT SCORED

Es dürfen nur Sicherheitsupdates aus vertrauenswürdigen Repositories verwendet werden, die von den Anbietern bereitgestellt und für die produktive Nutzung freigegeben wurden. Nach Möglichkeit sollten die neuesten Sicherheitsupdates, die von Ubuntu zur Verfügung gestellt wurden, auch installiert werden. Insbesondere müssen als „kritisch“ eingestufte Vulnerabilities, aus verlässlichen Quellen^{2,3}, schnellst möglich wieder geschlossen werden. Der interne SIX-CERT-Prozesses muss befolgt werden. Die Kontrollen stellen lediglich die vertrauenswürdigen Repositories sicher. Unser Linux-Plattform-Team führt regelmässig und mindestens einmal im Jahr auf den Linux-Servern die Updates durch. Wie schon einmal erwähnt, ist Ubuntu nicht unser Standardbetriebssystem und es scheint noch kein vereinbarter und regulärer Prozess für einen geregelten und gehärteten Supply Chain zu geben. Jegliche Komponente dürfen nicht direkt in das Internet kommunizieren. Jegliche Updates müssen über einen Proxy abgeholt werden. Wir in der SIX stellen den bevorzugten SmartProxy von JFrog Artifactory oder den WebProxy von Bluecoat zur Verfügung. Da wir grundsätzlich Ubuntu nicht unterstützen, muss der Punkt mit der geregelten und gehärteten Supply Chain, zwischen Anapaya Systems AG und SIX AG noch vor dem produktiven Einsatz geklärt werden.

5.2.3. Superuser Rights [SUDO]

SUDO-00312 - Sudo commands use PTY SCORED

Auf einem SCION-Router dürfen die Administratoren ihre Befehle nicht direkt mit erhöhten oder anderen Benutzerberechtigungen z. B. als Superuser ausführen. Eine erweiterte Sicherheitsrichtlinie, die in „/etc/sudoers“ spezifiziert wird, muss also bestimmen, welche Berechtigungen die einzelnen Benutzer besitzen. In Abhängigkeit der Policy wird nach der Befehlsausführung eine weitere Authentifizierung abgefragt. Auf dem SCION-Router ist das Sudo-Plugin installiert und aktiviert, aber leider wird das Pseudo-PTY (Pseudoterminal) nicht verwendet. Aus Sicherheitsgründen, muss verhindert werden, dass ein mit Sudo ausgeführtes Programm, das wiederum einen Hintergrundprozess startete, nach Beendigung bestehen bleibt. Ein Angreifer könnte sich dieses Verhalten mit einem Schadprogramm zunutze machen.

SUDO-00313 - Seperate sudo log file SCORED

Standardmässig werden alle Audit-Logininformationen in die Datei „/var/log/audit.log“ geschrieben. Während oder nach einem Sicherheitsvorfall erleichtert es dem Administrator unter gewissen Umständen die Loganalysen, wenn alle Sudo-Befehlsausführungen in einem separaten Audit-Log beispielsweise „/var/log/sudo.log“ abgelegt werden. In der SIX müssen aus regulatorischen Gründen ohne Ausnahme alle Loginformationen jeglicher Art auf unterschiedliche Logserver eingeliefert werden. Es haben zwar alle Administratoren einen Logserverzugriff, aber sollten die Logs z. B. einmal nicht richtig eingeliefert werden, ist beim Vorfinden einer kondensierten und übersichtlichen Log-Datei auch geholfen. Ausserdem vereinfacht es möglicherweise bei einem Router-Ausfall oder nach einer Sicherheitsverletzung die forensische System-Analysen.

SUDO-003xx - Allowed sudo commands NOT SCORED

Auf dem SCION-Router geniessen momentan alle persönlichen Benutzerkonten den höchsten privilegierten Status (Sudoers rights). Zukünftig muss diesbezüglich restriktivere Berechtigungen herrschen, denn nur System-Administratoren sollen Superuser-Rechte besitzen.

²<https://ubuntu.com/security/cve>

³https://www.cvedetails.com/vulnerability-list/vendor_id-4781/product_id-20550/version_id-236205/Canonical-Ubuntu-Linux-18.04.html

5.2.4. File System Integrity [FINT]

FINT-00411 - File Integrity Monitoring SCORED

In einem Enterprise Unternehmen wie SIX ist es unabdingbar ein File Integrity Monitoring zu betreiben. Es ist kein IDS/IPS und kann keine Angriffe in Echtzeit selbst verhindern, jedoch erkennt es nicht autorisierte Änderungen am System. Durch die periodische Überprüfung und Überwachung des Dateisystemstatus können verdächtige Dateien erkannt werden. Die Gefährdung durch versehentliche oder böswillige Fehlkonfigurationen, sowie geänderte Binärdateien können so durch ein aktives Monitoring verhindert oder zumindest begrenzt werden. Eine Alarmierung kann z. B. direkt in ein SIEM erfolgen, welches vom SOC rund um die Uhr 7x24h überwacht wird. Wir in der SIX setzen auf den Integrity Monitor von Tanium™ oder Tripwire und falls einer von diesen Agenten auch auf den SCION-Routern seine Dienste verrichtet, kann dieser Test ignoriert/ausgeklammert werden. Für alle anderen Systeme ohne File Integrity Monitoring empfiehlt es sich das Linux-Tool „AIDE“ als Lösung einzusetzen und eine Corporate Policy zu definieren und bei Verletzungen entsprechend zu alarmieren.

FINT-004xx - Malware Protection NOT_SCORED

Ein in sich sehr stark gehärteten Router wie beispielsweise von den namhaften Router-Herstellern (Cisco, Huawei, Juniper usw.) unterstützen keine Schadsoftwarescanner. Das ist nicht unbedingt notwendig, da keine verifizierten, zertifizierten oder fremde Applikation auf dem System installiert und/oder ausgeführt werden können. Mit diesem Ansatz kann eine Kompromittierung faktisch ausgeschlossen werden. In unserem Fall handelt es sich um ein frei erhältliches, unbehandeltes und offenes Open Source Betriebssystem. Mit dieser Tatsache und aus diesem Blickwinkel lässt sich die Notwendigkeit eines Schadsoftwarescanners wohl diskutieren, ist aber käumlich wegzudenken. Unter Ubuntu gibt es einige bekannte Malware Scanner wie ClamAV, Rkhunter oder Chkrootkit. Wenn ein RHEL-Server in der SIX nicht PCI-relevant ist, wird auf Anti-Malware-Programme verzichtet, aber andererseits ist ein wiederkehrender Systemscan gefordert.

5.2.5. Secure Boot [BOOT]

BOOT-00511 - Permissions on Bootloader SCORED

Die Grub-Konfigurationsdatei „/boot/grub/grub.cfg“ enthält Informationen zu Starteinstellungen und Kennwörtern zum Entsperren von Bootoptionen. Nur am Superuser „root“ sollte Lese- und Schreibberechtigungen gewährt werden. Nicht-root-Benutzer (Other und Group) sollten die Startparameter nicht einmal lesen dürfen, da sie mögliche Sicherheitslücken beim Start erkennen und ausnutzen könnten. Bei der Überprüfung wurde festgestellt, dass die GRUB-Berechtigungen für Nicht-root-Benutzer „Access: (0444/-r-r-r-) Uid: (0/ root) Gid: (0/ root)“ ungenügend gesetzt sind. Es wird eine Berichtigung „Access: (0400/-r---) Uid: (0/ root) Gid: (0/ root)“ empfohlen.

BOOT-00512 - Bootloader password is set SCORED

Nicht autorisierte Benutzer sollen ohne Passwort keine Boot-Parameter eingeben oder die Boot-Partition ändern können. Mit einem zusätzlichen Bootloader-Benutzer mit Passwort wird erschwert, dass böswillig die System-Sicherheit herabgesetzt wird. Beim Starten können viele sicherheitsrelevante GRUB-Funktionen wie z. B. AppArmor, die unterstützten Dateisysteme (/etc/modprobe.d/ blacklist.conf) usw. deaktiviert werden. Auf dem SCION-Router wurde kein GRUB-Benutzer mit Passwort aufgefunden. Es handelt sich hier um eine schützenswerte Anapaya Appliance und solche Modifikationen dürfen nicht von Kunden vorgenommen werden können, daher wird eine zusätzliche Berichtigung diesbezüglich dringendst empfohlen. Je nach Linux-Distribution ist für jeden Systemneustart anschliessend die Eingabe des Passworts erforderlich. Im Ubuntu-Linux dürfte dies nicht der Fall sein, ansonsten lässt sich eventuell von dieser

Schutzmassnahme wieder abkommen.

BOOT-00513 - Single User Mode SCORED

Der Single User Mode wird für die Systemwiederherstellung verwendet, wenn das System beim Booten ein Problem festgestellt hat oder wenn die Auswahl manuell im Bootloader getroffen wurde. Mit gleicher Begründung wie vorhin, empfiehlt es sich, einer Authentifizierung auch in diesem Modus. Nur so können autorisierte Benutzer das System im Single User Mode neu starten und es wird verhindert, dass unautorisierte Benutzer ohne Anmeldeinformationen keine Root-Berechtigungen erhalten. Auf der Appliance wurde für Root kein Passwort gesetzt und daher könnte das System gefährdet sein. Grundsätzlich ist es empfehlenswert Root zu deaktivieren und einen anderen ebenbürtigen Benutzer zu nutzen. Lediglich für den privilegierten Benutzer „anapaya“ ist ein in SHA512 verschlüsseltes Passwort gesetzt. Bei den finalen Entscheidungen von diesem und letzten Punkt, müssen klar die betrieblichen Aspekte mit den möglichen zusätzlichen Herausforderungen mitberücksichtigt werden.

5.2.6. Process Hardening [HDME]

HDME-00612 - Address Space Layout Randomization (ASLR) SCORED

Bezüglich Memory- und Process-Hardening gibt es unterschiedliche und einfache, nützliche Bordmittel, um den reservierten virtuellen Prozessspeicher (Stack) gegen gängige Buffer Overflow Vulnerabilities/Attacks besser zu schützen und abzuschwächen. Der Kernel unterstützt mit No Execute (NX)⁴ die sogenannte Data Execution Prevention. Eine weitere Technik namens Address Space Layout Randomization (ASLR) platziert die virtuellen Speicherbereiche zufällig und erschwert so das gezielte Beschreiben der Speicherseiten von bösartiger Software. Auf dem SIG-System sind die beiden Funktionen aktiv, aber noch nicht abschliessend konfiguriert. Gemäss CIS-Empfehlung fehlt noch einen fixen Sysctl-Eintrag „kernel.randomize_va_space=2“ in der Kernel-Konfigurationsdatei.

HDME-00614 - Memory Core Dump SCORED

Ein Speicherauszug wird erzeugt, wenn ein ausgeführtes Programm zum Abbruch oder zu einem kompletten Systemabsturz führt. Er wird allgemein dafür verwendet, um herauszufinden warum ein Programm abgebrochen wurde. Ein Angreifer könnte es auch dazu verwenden, um vertrauliche Informationen aus einem Core-Dump herauszulesen. Die Core-Dumps werden in ein separates Dateisystem geschrieben und sind für SUID-Binärdateien deaktiviert. Auf dem SIG-Router ist diese Möglichkeit deaktiviert und soll so belassen werden, denn es besteht ein Verbot seitens PCI-DSS Regulatorien.

5.2.7. Mandatory Access Control [AMAC]

AMAC-00712 - Mandatory Access Control (MAC) with AppArmor SCORED

Die Kernel-Erweiterung „AppArmor“ ist ein MAC-Verfahren, um gewissen Programmen einen begrenzten Satz von Ressourcen zu gewähren. Dieses Sicherheitsmodell bindet die Zugriffssteuerungsattribute eher an Programme als an die Benutzer. Ubuntu installiert und startet AppArmor initial mit einigen default Profilen und kann je nach Sicherheitsbedarf erweitert werden. Die AppArmor-Sicherheitsrichtlinien definieren, auf welche Systemressourcen die Anwendungen zugreifen dürfen, und mit welchen Berechtigungen sie dies tun können. Damit wird ein weiterer Schutzmechanismus zur Schadensbegrenzung eingeführt, um potentiell verursachte Schäden durch Applikationen an Systemdateien zu verhindern oder zumindest zu minimieren.

⁴Das NX-Bit liegt als zusätzliches Steuerbit in den Deskriptoren und Sicherungsbits für Speicherseiten. Setzt das Betriebssystem dieses Bit für den Stack-Bereich, erzeugt das Ausführen von Code auf dem Stack einen Ausnahmezustand in der CPU und informiert so das Betriebssystem.

Für die Benutzer gilt immer noch das gleiche, altbekannte und konfigurierte Berechtigungsmodell. Zusätzlich zum Discretionary Access Control (DAC) kommen einfach die AppArmor-MAC-Richtlinien hinzu. Schlussendlich müssen also die DAC-Berechtigungen und MAC-Regeln erfüllt sein.

5.2.8. Command Line Warning Banners [CLWB]

CLWB-00811 - Command Line Message/Warning Banners SCORED

Eine einfache und relativ wichtige Sache ist, die Anzeige einer Nachricht resp. einer Warnmeldung vor der Benutzeranmeldung via CLI. Solche Meldungen können bei der Verfolgung von Systemeindringlingen hilfreich sein, da sie von Gesetzes wegen gefordert sind. Wichtig dabei ist nur, dass keine sensitiven Informationen über das System herausgegeben werden. Ansonsten könnten Angreifer diese Informationen ausnutzen und versuchen mit bestimmten Exploits in das System einzudringen. Auf dem System sind momentan keine Banner eingerichtet und daher wird dringend empfohlen dies nachzuholen.

5.2.9. Disable/Enable OS Services [DSVC]

DSVC-00913 - Internal Domain Name Resolution and Time Synchronisation SCORED

Jegliche Netzwerkkomponente in einem Unternehmensnetzwerk müssen meist mit anderen Teilnehmern oder Services eine Netzwerkverbindung aufbauen. Die Kommunikation sollte, wenn immer möglich, über einen Domänennamen und nicht über die IP-Adresse direkt erfolgen. Obwohl Server-IP-Adressen mehrheitlich statisch konfiguriert sind, ändern sie sich oft im Serverlebenszyklus. Ein weiterer sehr wichtiger Service ist, die Zeitsynchronisation aller Netzwerkkomponenten, damit auf jedem Gerät die identische Zeit sichergestellt ist. Der zeitliche Aspekt hat nicht nur eine sehr hohe applikatorische Bedeutung, sondern auch bezüglich Threat Detection und Incidents Response Management ist sie essenziell und nicht mehr wegzudenken. Alle Netzwerkteilnehmer sollten im Corporate Network immer die vertraulichen internen Server ansprechen. Die internen Server sind vielmals vertrauenswürdiger und zuverlässiger als öffentliche externe Services. Ausserdem verfügt das Unternehmen über ihre Kontrolle und kann das Verhalten nach ihrem gut dünkten steuern. Der erhöhten Sicherheit zugute, wird empfohlen, diese Services von SIX selbst zu beziehen und die Konfiguration entsprechend anzugleichen.

DSVC-00926 - File Synchronisation Service „Rsync“ over network SCORED

Das Remote-File-Synchronisationstool ist unter den Linux-Administratoren aufgrund der einfachen und schlanken Bauweise und Benutzerfreundlichkeit sehr beliebt. Jedoch birgt Rsync potentielle Risiken. Standardmässig überträgt Rsync die Daten unverschlüsselt, aber es bietet die Möglichkeit, die Daten z. B. durch einen SSH- oder VPN-Tunnel zu transportieren. In Enterprise Netzwerken sollte dieses Protokoll nicht eingesetzt und auf alternativen wie SCP oder SFTP ausgewichen werden. Auf dem SCION-Router könnte Rsync noch aktiv genutzt werden und daher wird eine Deaktivierung empfohlen.

DSVC-01014 - Insecure Client Service „Telnet“ NOT SCORED

Telnet ist ein Client-Server-Netzwerkprotokoll, das auf einem ungeschützten und zeichenbasierten Datenaustausch spezialisiert ist. Es erlaubt das Remote Management von Systemen und die Datenübertragung erfolgt in Klartext. Für unberechtigte Benutzer ist es leicht die Anmeldeinformationen zu stehlen und weiter zu missbrauchen. Auf dem SCION-Router ist der Telnet-Client installiert und kann aktiv genutzt werden. Er wird momentan noch für die Administration von Quagga (BGP-Router) verwendet und oftmals wird das einfach gestrickte Telnet-Protokoll auf den Routern verständlicherweise zu Troubleshootingzwecken verwendet. Damit die Administratoren nicht zum Nutzen des Protokolls verleitet werden, wird jedoch trotzdem dringendst empfohlen auf eine sichere Client-Alternative wie SSH auszuweichen.

DSVC-01015 - Insecure Client Service „FTP“ SCORED

FTP ist ein Client-Server-Netzwerkprotokoll, das auf einem ungeschützten und zeichenbasierten Datenaustausch basiert. Es erlaubt den Datenaustausch zwischen Netzwerkteilnehmern und die Datenübertragung erfolgt in Klartext. Für unberechtigte Benutzer ist es leicht die Daten- und Anmeldeinformationen zu stehlen und weiter zu missbrauchen. Auf dem SCION-Router ist das FTP-Protokoll aktiv und daher wird dringendst empfohlen auf eine sichere Alternative wie SCP oder SFTP auszuweichen.

5.2.10. Disable Network Services [DNWS]**DNWS-01111 - Insecure Network Service/Parameter „ICMP Redirects“ SCORED**

ICMP Redirect Nachrichten werden bezüglich IP-Routing dazu verwendet, um den Netzwerkkomponenten im selben Subnetz mitzuteilen, dass ein anderes und besseres Gateway zum Ziel zu verwenden ist. Die IP-Datenpakete werden anschliessend direkt zum preferierten Gateway gesendet. In unserem Corporate Network, so wie wir das BGP-Routing betreiben, nämlich mit kleinen und direkten BGP-Peering-Netzwerken, sollten ICMP Redirect Nachrichten im Netzwerk nicht vorkommen. Auf dem SCION-Router, wurden diesbezüglich, unzulängliche Konfigurationen festgestellt. Es wurde festgestellt, dass ICMP-Requests nicht akzeptiert werden und daher sollte auch das Senden von ICMP-Redirects unterbunden werden. Grundsätzlich genügt eine allgemeine Deaktivierung aller Schnittstellen „all“, jedoch empfehlen die Literaturen auch eine Deaktivierung auf der default Schnittstelle.

DNWS-01113 - Log and Drop suspicious and unroutable sources SCORED

Durch Aktivieren des Reverse Path Filtering mit dem zusätzlichen Protokollieren ins Kernel-Logfile sollen IP-Spoofing-Angriffe verhindert und protokolliert werden. Die Kernelfunktion detektiert die Unzulänglichkeit anhand der Routing-Tabelle und verhilft dem SOC mögliche Angriffe zu erkennen und gewisse Gegenmassnahmen einzuleiten. Bei erlaubtem asymmetrischem IP-Routing, wie es in unserem Fall mit zwei internen Netzwerkschnittstellen vorkommen kann, muss der Kernel-Parameter auf 2 gesetzt werden. Bei der Analyse wurde festgestellt, dass die empfohlenen RPF-Funktionen zur Erkennung, Verhinderung und Protokollierung nicht aktiv sind.

DNWS-01117 - IPv6 Router Advertisements (RA) SCORED

Die Router Advertisements werden dazu benötigt, um in einem IPv6-Netzwerk Router anzukündigen. Angreifer könnten diese Funktion ausnutzen und über sogenannte „rogue“ RAs den Verkehr umleiten. Gegen IPv6-MITM-Angriffe gibt es relativ einfache Gegenmassnahmen. Einerseits sollten wie in unserem Netzwerkdesign möglichst kleine Subnetze, VLANs oder physische Netzwerkverbindungen zwischen den Routern verwendet und eine statische Adressierung erzwungen werden. Aus Sicherheitsgründen muss dennoch auf einem IP-Router die Akzeptierung von IPv6 Router Advertisements deaktiviert werden. Auf unseren SCION-Router ist diese Vorsichtsmassnahme noch nachzuholen.

DNWS-01118 - Service protection with TCP Wrapper NOT SCORED

Zusätzlich zu einer Firewall bietet der TCP-Wrapper den Schutz vor unerwünschten Zugriffen auf Ebene der Netzwerkservices (z. B. zusätzliche Sicherheit für SSH). Der TCP-Wrapper ist als Daemon namens „tcpd“ implementiert und bietet über Access Control Lists einen einfachen und guten Schutzmechanismus für unterstützende Services. Alle Services, die den TCP-Wrapper unterstützen, benutzen die Bibliothek „libwrap.so“. Bei der Systemüberprüfung wurde festgestellt, dass drei Services „opensm“, „sshd“ und „rcpbind/rpc.statd“ den Schutzmechanismus unterstützen würden. Lediglich beim Service „sshd“ würde es einen minimalen sicherheitstechnischen Mehrwert geben. Aus betrieblichen Gründen wurde daher auf den zusätzlichen Einsatz vom TCP-Wrapper verzichtet.

5.2.11. Disable Network Protocols [DNWP]

DNWP-01211 - Uncommon Network Protocols SCORED

Der Linux Kernel unterstützt standardmässig einige ungebräuchliche und anfällige Netzwerkprotokolle. Auf dem SCION-Router kommen manche Protokolle nicht zum Einsatz und daher empfiehlt es sich zur Verringerung der Angriffsfläche die unnötigen Netzwerkprotokolle dauerhaft abzuschalten. Die zu deaktivierenden Netzwerkprotokolle wie DCCP, SCTP, RDS und TIPC sind zwar nicht gestartet, aber könnten auf dem untersuchten SCION-Router grundsätzlich genutzt werden. Auf dem Router müssen die Kernel Module noch dauerhaft deaktiviert werden.

5.2.12. Mandatory Firewall Configuration [MFWC]

MFWC-01311 - Firewall against external and internal threats SCORED

Zum Schutz gegen interne und externe Bedrohungen werden auf dem SCION-Router die bewährten Iptables eingesetzt. Sie sind sehr einfach zu handhaben und ermöglichen einen Basisschutz gegen nicht autorisierte Verbindungen, um das Eindringen zu erschweren. Mittels Access Control Lists werden restriktive Firewall Regeln nur auf erlaubte und bewusst laufende Netzwerkservices implementiert und zugelassen. Die Kommunikationsverbindungen sollten also, wenn immer möglich nur zwischen bekannten IPv4/IPv6-Adressen stattfinden können. In SCION erscheint dies relativ einfach und schlank bezüglich Host-System umzusetzen zu sein, da die Kommunikation hauptsächlich über das Overlay abgewickelt wird und sich nur unter vertrauten und bekannten Partnern erfolgt. In diesem Zusammenhang sprechen wir hier von einem Gateway, der vor allem für das Forwarding von IP- und SCION-Datenpaketen zuständig ist und keine Perimeter-Firewall verkörpert oder ersetzen soll. Jeder Kunde im SSFN muss auf deren eigenen Perimetern für angemessene Kontrollen sorgetragen. Damit möchte gesagt werden, dass hier keinen Datenverkehr von und nach SCION gefiltert wird, aber dennoch muss unbedingt vermieden werden, dass reiner IP-Datenverkehr über das SIG weitergeleitet werden kann. Auf dem SIG muss verständlicherweise das IP-Forwarding aktiv sein und deshalb muss dafür gesorgt werden, dass keinesfalls ein Angreifer über IP in das Corporate Network eindringen kann.

MFWC-01312 - Firewall Stealth Rule SCORED

Einen Router besitzt resp. benötigt üblicherweise keine Restriktionen auf den Routing-Schnittstellen, da die Router-Hersteller wie beispielsweise Cisco, Huawei, Juniper usw. kein handelsübliches Betriebssystem verwenden und schon sehr stark in sich einschränken und härten. In unserem Fall empfiehlt es sich jedoch, eine Stealth Rule für jede Filter-Chain „INPUT“, „OUTPUT“ und „FORWARD“ zu verwenden und anschliessend mit restriktiven Regeln wieder zu öffnen. Bei SCION wird mit den standardisierten Chains gearbeitet und ein IPv4/IPv6-Default-Deny erfolgt leider nicht. Im SSFN nutzt SIX bekanntlich zwei SIGs. Ein SIG pro Datacenter mit unterschiedlicher IP-Anbindung. Im Hauptrechenzentrum sind wir über IPv4 und im Backuprechenzentrum sind wir über IPv6 zu den Providern angebunden. Auf den SCION-Gateways ist IPv6 grundsätzlich immer aktiv und daher ist es um so wichtiger alle Chains standardmässig auf Block zu setzen, auch wenn IPv6 ausgeschaltet wäre. Die SCION-Services laufen in Docker-Container und erlauben, unabhängig der gesetzten Regeln, in den genannten Filter-Chains den vollen Zugriff auf die Container-Services. Dafür sorgt Docker standardmässig vor. Docker stellt zwei zusätzliche Chains zur Verfügung. Iptables werden von Docker normalerweise automatisch in die Chain „DOCKER“ hinzugefügt und lassen alle externen Verbindungen bidirektional zu. Diese Chain „DOCKER“ wird als erstes vor allen anderen abgearbeitet. Benutzerdefinierte Modifikationen können über die zweite Chain „DOCKER-USER“ erfolgen und regeln so die benutzerdefinierten Containerzugriffe.

MFWC-01313 - Internal Loopback Traffic SCORED

Intern auf dem Router kommunizieren die Prozesse über das Loopback-Interface. Diese Kommunikation ist meist kritisch und darf keinesfalls unterbunden werden. Auf dem untersuchten SCION-Router wurden solche Kommunikationsverbindungen noch nicht berücksichtigt und müssen zusätzlich erfasst werden. Es empfiehlt sich, die interne Kommunikation innerhalb der beiden Chains „INPUT“ und „OUTPUT“ generell auf Schnittstellenebene (lo - Loopback) zu erlauben und eingehende externe Verbindungen auf das reservierte Netzwerk 127.0.0.0/8 zu blockieren.

MFWC-01315 - Restrictive Firewall Rules are configured SCORED

Eine restriktive eingehende oder ausgehende Kommunikation vom SCION-Host schützt vor Angriffen. Es verkleinert die Angriffsfläche von ausserhalb dem Internet/Extranet und innerhalb dem Corporate Network. Zudem erschwert es eine weiterführende Attacke bei einer SCION-Router-Kompromittierung. Bei den Untersuchungen konnten keine restriktiven ausgehenden Regeln aufgefunden werden. Die beiden Chains „adminips“ und „custships“ werden lediglich auf der INPUT-Chain angewendet und benötigen eine service-abgestimmte Überarbeitung. Bei der zukünftigen Anwendung von spezifischen Regeln müssen die Schnittstellen mitberücksichtigt werden. Solche Regeln geben einen erweiterten Schutz vor IP-Spoofing. Um ein Back-Door zu verhindern müssen unbedingt alle eingehenden und ausgehenden Verbindungen mit der Aussenwelt komplett unterbunden werden. Jegliche Kommunikationsverbindungen mit Services ausserhalb des Corporate Networks müssen authentifiziert und proxifiziert stattfinden. Direkte Verbindungen benötigen eine Begründung und eine temporäre Ausnahmegewilligung von Corporate Security und Enterprise Architecture Security.

MFWC-013xx - Logging Firewall Rules NOT_SCORED

Aus Performancegründen wird auf Routern normalerweise auf ein extensives Logging verzichtet. Das Logging von Access Control Lists liefern interessante Informationen in das SIEM ein, aber aufgrund der hier behandelten Router-Funktion wird auf ein Logging auf der Netzwerkebene vorerst verzichtet. Mit einem wiederkehrenden Review der restriktiven Zugriffsregeln und dem definierten System- und Audit-Logging kann die Sicherheit des SCION-Routers gesichert und hochgehalten werden.

5.2.13. Enable Audit Logging [ENLA]**ENLA-01411-29 - Auditing and Data Retention Configuration** SCORED

Im IT-Security-Umfeld sind sehr vielfältige Informationen über ein System von grossem Interesse. Werden erst die sicherheitsrelevanten Loginformationen zentral auf einem SIEM korreliert und ausgewertet, unterstützen sie bezüglich proaktiver und reaktiver Hinsicht, also während oder nach einem möglichen Cyber-Angriff sehr. Das Incident Response und Forensics Team sind demnach auch auf Audit-Logs angewiesen. Auf dem untersuchten SCION-Router wurde kein aktives Audit-Logging festgestellt und daher wird dringend empfohlen eine angemessene Konfiguration zu aktivieren. Das Audit-Logging kann je nach Einstellungen sehr ressourcenintensiv ausfallen und daher benötigt es nach der Bestimmung der Konfiguration gewisse Acceptance Tests in der Testumgebung. Aufgrund der Signifikanz des Audit-Logging, folgt eine stichwortartige Auflistung der wichtigsten und zu prüfenden Punkte:

- Der Audit-Daemon „auditd“ ist installiert und aktiviert.
- Das Audit-Logging wird für unterstützende Prozesse ermöglicht, auch wenn der Audit-Service noch nicht vollständig gestartet wurde.
- Das Backlog wurde für die im vorangegangenen Punkt erwähnten Prozesse gemäss den Best-Practice-

Empfehlungen angehoben.

- Die Audit-Konfiguration wurde korrekt anhand den Firmenvorgaben umgesetzt.
- Jegliche System- und Datei-Modifikationen, die Hinweise über mögliche Angriffsversuche liefern könnten, sind aktiv und werden in Log-Dateien abgespeichert.
- Alle Programme mit gesetztem Setuid- und/oder Setgid werden überwacht und bei Ausführung durch einen unautorisierten Benutzer umgehend alarmiert.
- Die Lese- und Schreibberechtigungen auf Audit-Konfigurationsdateien wurden entsprechend gesetzt.

Konkret sprechen wir hier von ca. 20 Prüfungspunkte im Zusammenhang mit dem bewährten Linux-Service „audit“, die einen signifikanten Sicherheitsmehrwert liefern. Um sich einen grösseren Überblick zu verschaffen oder genauere Informationen einzusehen, kann gerne das OS-Test-Skript „tests_anapaya_appliance“ eingesehen werden.

5.2.14. Enable Logging Service [ELOG]

ELOG-01511-16 - Logging Services Configuration SCORED

Ein Protokollierungsdienst muss so konfiguriert sein, dass Informationslecks verhindert und die Protokollierungen auf einem Remote-Server z. B. SIEM zusammengefasst, aufbereitet und ausgewertet werden. Im Falle einer möglichen Systemkompromittierung kann der Vorfall nur so effektiv überprüft und die allgemeine Protokollanalyse vereinfacht werden. Nicht nur aus betrieblichen, sondern auch aus regulatorischen und gesetzlichen Gründen, müssen die Logging-Informationen über einen längeren Zeitraum sicher und unveränderlich abgespeichert und abrufbar zur Verfügung stehen. Einerseits müssen die Log-Konfigurationen und Log-Informationen auf dem SCION-Router geschützt werden und andererseits aufgrund von Segregation of Duties gehört es sich die Informationen an unterschiedlichen Orten abzulegen. Für das Logging empfiehlt es sich direkt an die bereits bestehenden SIX-Logging-Services wie Splunk und Qradar anzubinden. Diese Tools sind beim Network-, Security- und SOC-Team für den Infrastrukturbetrieb in regem Gebrauch. Bei der Untersuchung des SCION-Routers wurde kein aktiviertes Logging festgestellt und muss für die komplette Integration in die SIX-Infrastruktur entsprechend aufgesetzt werden. Bezüglich SCION-Monitoring setzt Anapaya Systems AG vor allem auf bewährte Open Source Produkte. Zum Einsatz kommen beispielsweise Prometheus und Grafana, die auf dem System bereits als Container vorinstalliert sind und genutzt werden können. Bestimmt bieten auch diese Produkte bezüglich Logging eine variable Lösung. Die Empfehlungen bezüglich Host-OS-Logging richten sich jedoch auf die weit bekannten und bewährten Logging-Daemons „rsyslog“ und „journal“.

5.2.15. Enable Monitoring Service [EMON]

EMON-10xxx - Capacity Management/Performance Monitoring and Alerting NOT SCORED

Das Capacity Management gehört nicht direkt ins System-Hardening, aber möchte trotzdem aufgrund der Bedeutsamkeit erwähnt werden. Für den täglichen Betrieb ist das Capacity Management nicht wegzudenken, da mit dem richtigen Monitoring proaktiv auf mögliche eintretende Fehler frühzeitig Einfluss genommen werden kann. Im SCION-Umfeld sprechen wir vor allem die Überwachung der Bandbreite, Systemressourcen, Paketverluste in der Datenübertragung an. Wie angesprochen, wird im SCION-Umfeld bezüglich Monitoring und Alerting auf Prometheus und Grafana gesetzt. Auch wir in der SIX benutzen diese effektiven Tools. Bisher haben wir nur positive Erfahrungen gemacht, und sie bieten für uns den genügenden

und richtigen Mehrwert. Wie wir in einem vorangegangenen Test festgestellt hatten, ist das Monitoring mittels SNMP auf dem SCION-Router deaktiviert. Die Alerts können auch mit Grafana-Erweiterungen an Alarmierungssysteme weitergeleitet werden. Es stellt sich jedoch die Frage, ob eine zusätzliche Integration in unsere Netzwerk-Überwachungsumgebung, die mit dem Network Operations Management (NOM) und Cacti realisiert wurden, sinnvoll wäre. Das ist selbstverständlich eine Designfrage im Bereich der Infrastrukturüberwachung und möchte hier nicht bearbeitet oder beantwortet werden. Jedoch ist eine einheitliche und zentrale Lösung immer gut und anstrebenswert und jeder weitere uns noch unbekannte Service erhöht den Aufwand bezüglich Vulnerability Management und eröffnet eine weitere Angriffsfläche.

5.2.16. System Jobs and Automation Tasks [SJAT]

SJAT-01611-13 - System Automated Tasks SCORED

Alle Systeme verfügen über systemeigene Wartungsjobs, auch wenn möglicherweise keine Benutzerjobs auf dem System ausgeführt werden müssen, kann es für die Sicherheitsüberwachung nötig sein, gewisse Routinen mit dem Cron-Daemon auszuführen. Es ist wichtig das System auch für zukünftige Erweiterungen bereitzustellen. Der Cron-Daemon ist demnach auch auf dem SCION-Router aktiv und es empfiehlt sich die Berechtigungen und Autorisation bereits richtig zu setzen. Momentan können alle Benutzer die Konfigurationen einsehen und Jobs ausführen. Bereits das Einsehen der Cron-Konfigurationen können sehr viel über das System verraten und missbräuchlich benutzt werden. Die Ausführungsberechtigung könnte dafür missbraucht werden, um nicht-privilegierten Benutzer die Möglichkeit zu geben, nicht autorisierte erhöhte Berechtigungen zu erlangen. Es wird empfohlen die Punkte entsprechend nachzuholen.

5.2.17. Configuration Secure Shell [CSSH]

CSSH-01711-14 - Secure SSH Configuration SCORED

In den vorangegangenen Tests hatten wir sichergestellt, dass keine unsicheren Übertragungsprotokolle mehr verwendet werden können. Die Ablösungen von Telnet, FTP, Rlogin, RSH und RCP wurden durch das sichere SSH-Protokoll erreicht. Die Wartung eines SCION-Routers und der administrative Datenaustausch ist künftig nur noch über SSH gestattet. Nach der OpenSSHServer-Installation benötigt die Standardkonfiguration einen Feinschliff. Damit nicht nur die Datenübertragung bestmöglichst abgesichert wird, müssen auch noch einige Einstellungen bezüglich Dateizugriffsberechtigungen, Authentifizierung, Zugriffsberechtigungen, Auditing und Tunneling-Mechanismen überprüft und vorgenommen werden. Bei den Untersuchungen sind einige zu bereinigende und optimierende Punkte aufgetaucht. Beispielsweise sollte das SSH-Auditing detailliertere Informationen einliefern, in den Crypto-Einstellungen⁵ dürfen keine unsichere Message Authentication Codes (MACs) z. B. mit MD5 und SHA1 und Schlüsselaustauschmethoden z. B. mit SHA1 verwendet werden können. Des Weiteren muss das TCP-Forwarding deaktiviert werden, denn nur so können alle SSH-Verbindungen transparent für das Auditing gemacht werden. Es darf keine Möglichkeit geben irgendwelche Verbindungen zu verstecken. Wird die Weiterleitung jedoch aus applikatorischen Gründen benötigt, so muss es mindestens lokal auf dem SCION-Router mit der Option „PermitOpen localhost:* 127.0.0.1:*“ und „PermitOpen localhost:* :1:*“ gehalten werden. In einer sicheren Umgebung ist die Transparenz das A und O. Der letzte wichtige und erwähnenswerte Punkt ist, dass der direkte Root-Login via SSH unterbunden werden muss. Das Login mit Passwort wird zwar erzwungen, aber sollte trotzdem für zukünftige Änderungen schon mitberücksichtigt werden. Jeder Benutzer darf nur über seinen eigenen Account mittels Sudo arbeiten können. Auch hier steht die Transparenz fast an vorderster Stelle. Jegliche

⁵Bei uns in der SIX stellt das Enterprise Security Architecture Team ein Dokument „Cipher Suites Principles“ zur Verfügung, um uns allgemeine Leitlinien bezüglich der zu verwendenden Algorithmen zu bieten.

Abweichungen von diesen Empfehlungen müssen wir im Sicherheitsdokument erwähnen und meist zusätzlich über eine Exception separat bewilligen lassen und risikomitigierende Massnahmen definieren und umsetzen.

5.2.18. Configuration Pluggable Authentication Module [CPAM]

CPAM-01811-12 - Pluggable Authentication Modules (PAM) Configuration SCORED

Es gibt unterschiedliche Arten von Möglichkeiten die Passwortsrichtlinien in der Firma durchzusetzen. Wir in der SIX benutzen KEINE persönlichen Benutzer auf den Systemen selbst, sondern lagern sie für gewöhnlich immer an eines von unseren externen Active Directories (AD) aus. Demnach befinden sich diese Benutzerrichtlinien auch auf diesen Systemen. Faktisch alle ADs sind mit dem Identity Access Management (IAM) verbunden und bilden jegliche Prozesse wie Joiners, Movers, und Leavers (JML - Eintritte, Wechsel und Austritte) ab. Für alle anderen spezielleren Konten wie z. B. für System-, Technical- und den Root-Account befinden sich die Passwörter immer noch lokal auf dem System und können aus unterschiedlichen Gründen nicht ausgelagert werden. Technische Benutzerkonten dürfen sich auch nicht selbst am System anmelden können. Grundsätzlich dürfte sich nur Root oder ein äquivalenter Benutzer wie „anapaya“ mit einem starken Passwort auf dem SCION-Router befinden. Dieses Passwort darf keinesfalls ablaufen und NICHT den Administratoren bekannt sein. Solche Passwörter sind nur für Notfälle gedacht und können nur mittels Incident-Tickets bei unserem 7x24 Operation Control Center (OCC) ausgelöst werden. Nach Gebrauch ist das Passwort unverzüglich zu ändern und wieder „versiegelt“ dem OCC auszuhändigen. Demnach sehen wir die Notwendigkeit eine lokale Passwortsrichtlinie zu erzwingen. Es gibt dafür unterschiedliche Bibliotheken wie z. B. „pam_cracklib.so“ oder „pam_pwquality.so“, die wir für diesen Zweck verwenden könnten. In unserem Fall ist eine derartige Policy nicht vorhanden und muss nachgeholt werden. Manche weiterführenden Sicherheitsempfehlungen (z. B. Passworterneuerung, Benutzerkontoblockierung usw.) wurden bewusst nicht umgesetzt, da wie schon erläutert alle persönlichen Benutzerkonten in ein AD ausgelagert wurden und durch das gezielte Logging potenzielle Brute-Force-Angriff via Qradar und/oder Splunk in das SOC alarmiert wird.

5.2.19. Configuration User Accounts and Environment [CUAE]

CUAE-01911-15 - User Accounts and Environment Configuration SCORED

Obwohl einige sicherheitsrelevante Passwortsteuerungsparameter ins PAM verschoben wurden, bleiben gewisse Standardeinstellungen für die System- und Benutzerkonten in der Shadow-Kennwort-Umgebung bestehen. Wird z. B. ein Benutzer erstellt, werden ihm gewisse Standardvorgaben wie die maximale Passwortlebensdauer, Benutzerinaktivität usw. übergeben. Auch die Standard-Dateiberechtigungen bei der Erstellung kann vorgegeben werden. Meistens macht es Sinn, dass vom Administrator erstellte Dateien nicht unbedingt von allen Benutzern gelesen werden dürfen. Diese Parameter und weitere werden in der Datei „/etc/login.defs“ definiert. In der SIX besteht bekanntlich die Vorgabe, dass keine persönlichen Benutzerkonten auf dem System sein dürfen und die Durchsetzung über die ADs stattfindet. Daher müssen einige lokalen Einstellungen nicht beachtet werden oder können für die wenigen speziellen Konten gelockert werden. Bei der Prüfung konnten vor allem zwei vermisste und empfehlenswerte Limitierungen festgestellt werden. Die Standard-Dateiberechtigungen sollten für Verzeichnisse auf 750 (rwxr-x-) und für Dateien auf 640 (rw-r--) verschärft werden. Des Weiteren, muss über die SU-PAM-Konfigurationsdatei „/etc/pam.d/su“ den Gebrauch von „su“ unterbunden werden, denn alle Benutzer müssen strikte „sudo“ nutzen und dürfen nicht unter anderen Benutzernamen gewisse Befehle absetzen können.

CUAE-019xx - Local User/Administrator Accounts NOT SCORED

Bei den Untersuchungen wurden wie bereits angesprochen persönliche lokale Administratorenkonten aufgefunden und diese sollten nach Möglichkeit auf ein AD ausgelagert sein. In Verbindung mit der vereinfachten SSH-Key-Authentifizierung können sie zurzeit nur lokal gehalten werden. Gemäss interner Regelung „Appendix 8 to Security Regulation S2: Information Security, Section 2.2“ ist der Einsatz von kryptographischen Schlüsseln zur passwortlosen Authentifizierung zwar nicht verboten, aber sie benötigen ein geeignetes Verfahren für das Schlüsselmanagement. Grundsätzlich sind SSH-Schlüssel sicherer als Passwörter anzusehen, jedoch ist bei den lokalen Benutzern das Identity and Access Management nicht durchgehend gewährleistet. Bei den regulatorischen Audits könnte diese Art von Authentifizierung ohne durchgehenden Prozess gewisse Diskussionen auslösen. Solange in der SIX kein zentraler Prozess diesbezüglich definiert und umgesetzt wurde, wird eine Benutzerauthentifizierung mittels Benutzernamen und Passwort empfohlen. Gemäss der SSFN-Kommunikationsmatrix wird erfreulicherweise die SCION-Administration nur über einen Jumpserver mit MFA ermöglicht.

5.2.20. System Maintenance and File Permissions [SMFP]**SMFP-02011 - Integrity Check of installed sytem packages via package manager** NOT SCORED

Der Installationsstatus der installierten Systempakete in Verbindung mit der Dateintegrität gibt nützliche Angaben auf geänderte Programm- und Konfigurationsdateien. Bei der Überprüfung tauchten nur bewusst angepasste und daher erwartete Konfigurationsdateien auf. Diese Kontrolle mit diesen nützlichen Angaben können als zusätzliche Sicherheitsmassnahmen angesehen werden und in manchen Belangen sehr von Interesse sein. Die Pakete können sich bei Release-Änderungen und Updates stark verändern und einen ausgiebigen Rapport generieren. Diese Prüfung kann leider nicht automatisiert und ohne manuelle Überprüfung gewertet werden.

SMFP-02012 - File permissions to account information SCORED

Die Account-Informationen (Benutzernamen, Gruppenzugehörigkeiten und Passwort-Hashes) müssen auf dem System entsprechend geschützt werden. Einerseits dürfen nur Administratoren Schreibberechtigungen haben und andererseits dürfen unberechtigte Benutzer die Informationen nicht einsehen können. Mit diesen sensiblen Informationen könnten Angreifer unter anderem Schlupflöcher ausfindig machen und missbrauchen oder sogar durch Passwort-Cracker über Hashes an die Passwörter zu gelangen. Auf dem SCION-Router wird daher empfohlen das Need-to-know-Prinzip besser durchzusetzen.

SMFP-02013-14 - World-writable and orphan files SCORED

Sind Dateien oder Verzeichnisse auf dem System von allen beschreibbar, können unter gewissen Umständen die Administratoren unbewusst das System gefährden. Weltweit beschreibbare Dateien können von jedem Benutzer im System geändert werden und sind möglicherweise die Ursache einer möglichen System-Kompromittierung. Solche Daten wurden auf dem SCION-Router nicht vorgefunden und müssen unbedingt stets aufgedeckt werden. Auch sehr wichtig zu vermeiden sind sogenannte verwaiste Dateien ohne Benutzer- und/oder Gruppenzuordnungen. Gefährlich kann es werden, wenn unbewusst neue Benutzer oder Gruppen plötzlich auf die Daten gewisse Berechtigungen kriegen, die sie nicht innehaben dürfen. Solche Dateien können ungewollt entstehen, wenn versehentlich der Administrator eine Account-Anpassung vornimmt und anschliessend die Dateien nicht bereinigt. Das kann so weit reichen, dass gewisse Benutzer auf sensitive Informationen Zugriff haben oder sogar die System-Integrität kompromittieren könnten. Auf dem SCION-Router befinden sich einige verwaiste Daten zur Bereinigung, die mit hoher Wahrscheinlichkeit durch das aufsetzen des Routers entstanden.

SMFP-02015 - Root path environment variables SCORED

Durch falsche Pfadverweise in den Environment Variablen könnte es z. B. einem Angreifer ermöglicht werden einen Schadcode auszuführen und die Systemintegrität zu gefährden. Es muss darauf geachtet werden, dass keine Dateien, leere Verzeichnisse oder zusammenhängende Pfade referenziert werden und vor allem nicht gerade das aktuelle Verzeichniss „/“ in dem sich der Administrator mit „root“ gerade befindet. Auf dem SCION-Router konnten keine Auffälligkeiten diesbezüglich vorgefunden werden. Wie es mit vielen Konfigurationen ist, können solche Unschönheiten sich im Laufe vom Betrieb durch Änderungen einschleichen und daher ist auch hier eine kontinuierliche Prüfung sehr empfohlen.

SMFP-02016 - Owner and permission of \$HOME directory SCORED

Die Überprüfung der HOME-Verzeichnisse haben ergeben, dass nicht alle Benutzer wie „sionly“ ein eigenes Verzeichnis besitzen und jeder Benutzer auf dem System sie lesen darf. Es wird empfohlen eine restriktivere Berechtigung auf diesen Verzeichnissen empfohlen. Alle Berechtigungen müssen auf mindestens 750 herabgesetzt werden. Alleine schon mit der Leseberechtigung ermöglicht es einem böswilligen Benutzer die Daten anderer Benutzer zu stehlen. Mit Schreiben könnte es ihnen unter besonderen Umständen möglich sein, die Systemberechtigungen eines anderen Benutzers zu erlangen.

SMFP-02017 - Hidden files and directories SCORED

Oftmals werden Dateien und Verzeichnisse aus unterschiedlichen Gründen vor anderen Benutzern versteckt. In diesem Zusammenhang sollten die Daten auch die entsprechenden Zugriffsberechtigungen aufweisen und dürfen vor allem nicht von allen Systembenutzern beschreibbar sein. Auf jeden Fall ist es sicherlich zu vermeiden, dass die Integrität von sensiblen Informationen bewahrt wird und nicht abfließen. Durch Modifikationen könnten allenfalls andere Systemberechtigungen erlangt werden. Bei den Untersuchungen wurden mit hoher Wahrscheinlichkeit nur temporäre Dateien, die durch die SCION-Service-Installationen entstanden, aufgefunden. Oftmals fordert es wie hier nach dieser Prüfung einen manuellen Eingriff zur Korrektur oder Bereinigung.

SMFP-02018 - Duplicate user and/or groups SCORED

Der letzte Test überprüft die Account-Informationen auf doppelte Benutzer- oder Gruppeneinträge. Solche Einträge wurden auf dem SCION-Router nicht vorgefunden. Diese Szenarios sind hoffentlich eher unwahrscheinlich, aber trotzdem einen wichtigen Prüfungspunkt. Da die Listen immer von oben herab abgearbeitet werden, könnte ein Benutzer über seine Anmeldeinformationen mit falschen Berechtigungen ausgerüstet werden. Im normalen Betrieb führt es zu auffallenden und ungewollten Verhaltensweisen, aber mit böswilliger Absicht stellt es erhebliche Sicherheitsprobleme dar.

5.3. Erkenntnisse

Durch die ausgiebigen Sicherheitsüberprüfungen der SCION-Appliance, die Anapaya Systems AG bereitstellte, konnten einige sicherheitsrelevante Optimierungspunkte aufgedeckt werden. Die SCION-Appliance steht grundsätzlich als ein solides und relativ sicheres Serversystem da, das hinter einer firmenkonformen Firewall in einer internen Zone gut geschützt steht. Einen externen Server- oder Applikationszugriff erfolgt heutzutage immer mindestens über eine UTM-Firewall und bestenfalls noch zusätzlich über einen separaten Applikationsproxy. Ein SCION-Router steht meistens ohne zusätzlichen Firewallschutz ausgeliefert in der sogenannten Access Platform (AP). Die AP terminiert alle Anbindungen zur Aussenwelt (Extranet/Internet) der SIX. Aus diesem Grund ist es sehr wichtig einige Härtungsmassnahmen mehr vorzunehmen, um externen Zugriffen über Hintertüren (Backdoor) noch besser entgegenzuwirken und aussergewöhnlichen und verdächtigen Machenschaften schneller erkennen zu können. In der SIX bestehen für gewöhnlich

keine Zugriffsfiler auf Serversystemen. Jedoch lassen wir implizit bei allen Netzwerkkomponenten auf die produktiven Schnittstellen (Forwarding Interfaces) nur die absolut notwendigen Netzwerkservices wie z. B. BGP, BFD, PIM-SM und IGMP zu. Auch die Managementzugriffe sind nur mit den erlaubten Crypto-Einstellungen verschlüsselt und von einer beschränkten Anzahl von Admin-Jumpservern mittels SSH gestattet. Ein SSH-Tunneling (SSH-Port-Forwarding) ist für das Management nur lokal gestattet. Über den SCION-Router heraus ist ein SSH-Tunneling verboten. Mit anderen Worten benötigt der SCION-Router eine Justierung der SSH-Konfiguration und ein restriktiveres Regelwerk aller drei Chains (Input, Output und Forwarding). Am Ende der Regelwerke müssen wirksame Stealth Rules stehen. Als einzige ist es der Forwarding-Chain vorbehalten, einen generelleren, grosszügigeren und offeneren bidirektionalen ACCEPT-Filter, der nur auf Ebene der Netzwerkschnittstellen den Verkehr beschränkt. Ein SCION-Router muss immer in der Lage sein die gelernten und konfigurierten Netzwerke, ohne hohem administrativen Aufwand, weiterzuleiten. Bezüglich Benutzer- und Adminzugriffen müssen auch noch einige konzeptionelle Anstrengungen und strengere Einschränkungen vorgenommen werden. In der SIX müssen persönliche Accounts, wenn immer möglich auf ein AD ausgelagert werden. Eine SSH-Key-Authentifizierung ist nicht verboten, aber wenn kein verlässliches und sicheres Schlüsselmanagement besteht, nicht empfohlen. Ein PCI- oder SWIFT-Auditor würde dies vermutlich kritisieren. Den Gebrauch von „su“ muss unterbunden werden, da unter gewissen Umständen die Audittransparenz verloren geht. Auf dem SCION-Router sollten mehrere Admin-Profile mit unterschiedlichen Berechtigungen vorzufinden sein. Bestehen bleibt bestimmt der Superuser „anapaya“ für Emergency-Fälle. Dazu kommen mindestens zwei weitere Admin-Profile wie beispielsweise „sysadmin“ und „scionadmin“. Die Profilnamen sind betreffend Berechtigungen selbstredend und können über Sudo-Commands einfach geregelt werden. Einen weiteren und letzten sehr wichtigen Aspekt kommen dem Auditing, Logging und Monitoring hinzu. Das Audit-Logging scheint nicht korrekt umgesetzt zu sein und eine Integration in die SIX Logging-Infrastruktur fand noch nicht abschliessend statt. So wie das zentrale Logging sollte auch das teilweise bestehende Monitoring- und Alerting in die SIX-Infrastruktur künftig besser integriert werden. Die ausgearbeiteten Empfehlungen kommen teilweise aus der Security Community, den SIX-Weisungen. Andere wurden wiederum für den SCION-Router spezifisch entwickelt. Aufgrund der gegebenen SIG-Funktionen konnten manche Empfehlungen nicht oder nur teilweise berücksichtigt werden. Im Testskript befinden sich jedoch unter den einzelnen Tests die finalen und gewünschten Endresultate und Empfehlungen, damit die SCION-Appliance weiterhin den Anforderungen gerecht werden kann und wir als SIX den bestmöglichen Sicherheitsvorteil bezüglich Cyber Security (Protection, Detection and Response) herausholen konnten. Nur eine ganzheitliche Sicherheitskonfiguration mit einem entsprechenden Logging, Monitoring und Alerting stärken die SCION-Applikationen gegen Cyber Angriffe effektiv. Selbstverständlich können nicht alle gerechtfertigten Verbesserungsvorschläge ohne Weiteres direkt umgesetzt werden. Wie gesehen, könnten einige Massnahmen das System mehr auslasten und womöglich negativ beeinflussen oder unter Umständen den operativen Betrieb durch die Administratoren markant erschweren. Somit könnte die Umsetzung einer Massnahme nicht mehr gerechtfertigt werden. Wichtig erscheint, dass jedes Instrument vor der Implementierung nochmals genauestens angeschaut und beurteilt wird. Ein anschliessender und ausgiebiger Acceptance Test mit der finalen Konfiguration muss unbedingt stattfinden. Nur so entsteht eine gehärtete und stabile SCION-Plattform. Auffallend waren manche Vorschläge, die keine direkte Schutzfunktion haben, sondern „lediglich“ die Bedrohungserkennung und Post-mortem-Analyse unterstützen. Im Cyber-Security-Umfeld gehören auch solche Werkzeuge zum System-Hardening. Kann oder möchte ein Vorschlag nicht berücksichtigt werden, benötigt es eine schriftliche dokumentierte Begründung. Die Auditoren bestehen auf solche Exceptions mit zusätzlichen mitigierenden Massnahmen. Nur so können auch Dritte zu einem späteren Zeitpunkt die Ausnahmen verständlich nachvollziehen und gegebenenfalls kann das SIX SOC eine spezifische Überwachung einrichten. All diese Kontrollen müssen laufend an der neuen Situation angepasst werden, denn sie unterstützen die Systemsta-

bilität und die Systemintegrität. Ausserdem sollten diese Kontrollen wiederkehrend z. B. im halbjährlichen Zyklus stattfinden. Es gibt auch einige Kontrollen, die nicht komplett abgeschlossen sind und erweitert werden können. Andere Kontrollen wie z. B. die Firewall-Regeln benötigen eine Justierung nach Abschluss des endgültigen Aufbaus. Bei manchen Kontrollen benötigt es eine zusätzliche und manuelle Verifikation durch einen SCION-Spezialisten, denn nicht alle Kontrollen können komplett automatisiert durchgeführt werden. Abschliessend zu diesem Schwerpunkt möchten nochmals ein paar wichtige und unerwähnte Punkte auf den Weg zur Erfolgreichen SCION-Integration bei SIX mitgegeben werden:

- * SCION Appliance Cleanup (Keep the system tidy)⁶
- * SCION Appliance Backup und Restore
- * SCION Appliance Full Disk Encryption
- * SCION Management Interface dediziert in Admin-Zone
- * SCION Appliance mit Integrated Lights-Out (ILO)
- * SCION Implementation of Hardening Measures
- * SCION Release Acceptance Test (Integration- und Produktions-Umgebung)
- * SCION Centralized and remote log collection service (SIEM)
- * SCION Use Cases für Security Operations Center (SOC)
- * SCION Hardened Operating System with Tripwire (Ubuntu und „Red Hat“)
- * SCION Endpoint Security (e.g. Tanium and AV-Software)
- * SCION Lightweight Anapaya Operating System (Linux-Distribution)

Die obere Liste ist keinesfalls vollständig. Sie verfolgt lediglich das Ziel noch weitere offene und unvollendete Punkte anzudeuten, um die SCION-Infrastruktur noch sicherer und widerstandsfähiger gegen Cyberattacken zu gestalten. Bevor wir anschliessend direkt zu den weiterführenden SCION-Kontrollen kommen, findet eine vertiefte Einführung in die SCION-Docker-Umgebung statt. Diese zusätzlichen Informationen erklären und veranschaulichen die SCION-Services wie sie in den Docker-Containern abgebildet sind und wie sie untereinander vernetzt sind. Danach wird wie sie es von diesem Kapitel her kennen, vertieft in das SCION-Service-Hardening eingetaucht.

⁶Ist ein System über längere Zeit in Betrieb, kann es leider vorkommen, dass sensitive Daten unabsichtlich an ungeeigneten Orten zwischengespeichert und nicht mehr entfernt wurden. Es können sogenannte Dark Data entstehen, die ein hohes Sicherheitsrisiko darstellen können.

DOCKER SECURITY

Mit dem vorangegangenen Kapitel 5 wurde eine sicherere Basis für die SCION Services geschaffen. Auf der gehärteten Plattform (SCION Appliance) werden nun die SCION Services installiert und möglichst sicher betrieben. Das Container-Verhalten könnte schon viel früher in der Entwicklungskette böswillig beeinflusst werden. Ein potenzieller Angreifer könnte das Container-Image durch einfügen von Malicious Code beeinflussen und in die Produktion bringen. Im umgekehrten Fall wäre es möglich, eine abgeänderte Version über die Container Image Registry in die Entwicklung einzuschleusen. Es muss also auch sichergestellt werden, dass wirklich immer auf dem letzten, registrierten Build gearbeitet wird. Auch der Benutzerzugriff auf das Repository muss nach dem Least Privilege Prinzip ordnungsgemäss gesteuert und kontrolliert werden. Nicht nur der eigene Code kann Mängel aufweisen und daher müssen im Software-Lifecycle zu Beginn an die Abhängigkeiten von Drittanbietern mitberücksichtigt werden. Es führt nichts um eine wiederkehrende Überprüfung auf bekannte Flaws (Vulnerabilities) in den inkludierten, fremden Applikationen. Solche Arten von Supply Chain Angriffen und Schwächen können mit diesem Kapitel nicht merklich erschwert oder verhindert werden. Gegen diese Angriffsarten benötigt es Vorkehrungen innerhalb des Entwicklungsprozesses bei Anapaya Systems AG und sind nicht Teil dieser Thesis. Das ist auch einer der Gründe, weshalb man sich künftig vertiefter mit dem Thema „Penetrationtest“ auseinander setzen muss. Dies verschafft die Möglichkeit solche Arten von Schwachstellen auch von ausserhalb des Codes aufzufinden.

Ist einmal der SCION Code geschrieben, wird er anhand einer Konfiguration in ein Container Image verpackt. Nicht nur beim Starten und Ausführen von Containern vergrössert sich die Angriffsfläche. Schon in der Image-Build-Phase könnten sich auf viele unterschiedlichen Arten potentielle Schwachstellen einschleusen, die später ein Angreifer ausnutzen könnte. In diesem Kapitel wird vor allem die SCION Container Umgebung betrachtet und erweitert so, im direkten Zusammenhang mit Docker, das Benchmark Tool mit geeigneten Checks. Zum Überprüfen von Containern finden gängige und bewährte Sicherheitsmethoden, abgestützt durch die grosse Docker Community aus der Industrie, statt. So kann sichergestellt werden, dass die Security Principles auch wirklich und bestmöglich eingehalten wurden. Wenn immer möglich richten wir uns als SIX und hier an die weltweit anerkannten CIS Empfehlungen und erweitern sie gegebenenfalls mit PCI-DSS und SWIFT Sicherheitskontrollen. Es werden hier bewusst nicht auf alle empfehlenswerten Überprüfungen eingegangen oder im Tool komplett zu Beginn berücksichtigt. Der Fokus liegt ganz klar auf der technischen Überprüfung (Technical Security Audit) selbst, nämlich den Security Controls, die aus Sicht des Autors am wichtigsten und als erwähnenswert erscheinen. Auch hier werden auf einheitliche und bewährte Open-Source-Tools gesetzt und erweitern sie gegebenenfalls mit SCION-spezifischen Kontrollen.

Für die weiteren Themenbereiche ist ein vertieftes und technisches Verständnis über den SCION-Funktionsumfang notwendig. Nur so können die Weiterführenden und geeigneten Security Controls abgeleitet, ausgearbeitet und verstanden werden. Bei den forensischen Spurenuntersuchungen verhält es sich ähnlich, denn ohne vorherige Anwendungsanalyse wird es schwierig oder verunmöglicht die aufgefundenen Artefakte

richtig zu deuten und zuzuordnen. Zunächst erfolgt also zuerst die entsprechende Aufarbeitung des SCION-Know-Hows. Besteht das nötige SCION-Hintergrundwissen bereits, können die einleitenden Unterkapitel übersprungen werden. Die Empfehlungen der SCION Container Hardeningmassnahmen beginnen ab dem Abschnitt 6.3. Die folgenden Erläuterungen basieren auf den bekannten SCION Kursunterlagen[28][29], dem SCION Buch[52], aus den Gesprächen und Diskussionen mit den Anapaya Entwicklern und besonders aus dem erlangten Verständnis und daraus resultierten Wissen der Anwendungsanalysen in der Trainingsumgebung.

6.1. SCION Networking Stack

Bevor wir tiefer in die technischen Details eintauchen können, müssen noch einige wichtige grundlegende Punkte und Funktionalitäten geklärt werden. Alle Applikationen sowie die SCION Services, welche über das Netzwerk kommunizieren, benötigen einen sogenannten Protokollstapel (Networking Stack). Der Datenaustausch über das Netzwerk wird von den jeweiligen Netzwerkprotokollen im Stack nach dem anderen verarbeitet. Jedes Netzwerkprotokoll entfernt beim Empfang oder fügt beim Versenden seine Steuerinformationen hinzu, die für das jeweilige Protokoll selbst bestimmt sind. Anschliessend übergibt es die verbliebenen Daten dem nachfolgenden Netzwerkprotokoll. Jedes Datenpaket, unabhängig von der Internet Architektur, trägt auf der Leitung sämtliche Headers der darüberliegenden Schichten.

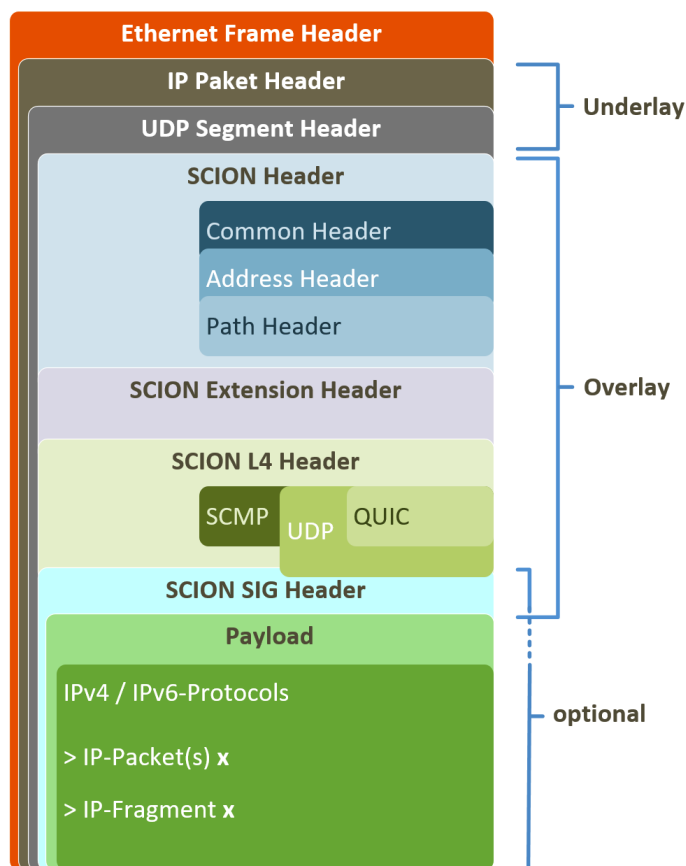


Abbildung 6.1.: SCION Packets on the wire

In der Abbildung 6.1 können sie die einzelnen Headers komplett einsehen. Die äusseren drei altbekannten Headers werden momentan noch immer für die Point-to-Point-Verbindungen zwischen den Border Routern

benötigt. Je nachdem welche IP-Version eingesetzt wird, bringt das UDP-Tunneling leider einen kleinen Overhead, bezüglich Paketgrösse von maximal 40 Byte und in der Verarbeitungszeit. Das zukünftige Ziel ist selbstverständlich die Elimination des Underlay-Protokolls, aber vorerst findet die SCION-Kommunikation (SCION Traffic) über das verbindungslose UDP/IP-Protokoll statt. Alle Daten werden also innerhalb der SCION-Insel immer über das UDP getunnelt. Jedoch muss erwähnt werden, dass dieses Verfahren vor allem in der Einführungsphase auch seine bereits erwähnten und bekannten Vorteile hat. Kommen wir nun zum interessanteren SCION Header. Er ist ein zusätzlicher Layer3-Header und innerhalb des Headers werden momentan die Layer4-Protokolle SCMP/SCION, UDP/SCION und QUIC/SCION unterstützt. Trifft ein SCION-Datenpaket auf ein Interface, wird über die SCION-L4-Protokoll-Informationen versucht den Service zu erkennen. Kann die SCION-Applikation eruiert werden, so wird das Datenpaket entsprechend zur Verarbeitung weitergeleitet, ansonsten wird es umgehend verworfen. Hier wird über eine systeminterne oder externe Weiterleitung zum entsprechenden Control Service gesprochen. Müssen legacy IP-Netzwerke miteinander kommunizieren, benötigt es einen SIG Service. Die SCION SIG Headers kommen nur zwischen ASes mit SIG-Services vor. Native SCION-Applikationen benötigen keinen SIG Header und können die volle Payload für ihre Daten nutzen. Zusätzlich zum SIG Header kommen die originalen L3/L4-IP-Header-Informationen hinzu. Sie wiederfinden sich im Payload und werden für den Transport im legacy IP-Netzwerk wiederverwendet. Wie in der Abbildung 1.3 gezeigt, kommunizieren die Finanzunternehmen SIX und SNB innerhalb vom SSFN-Netzwerk über einen SIG-Tunnel. Für das grundlegende Verständnis wird keine detailliertere Header-Beschreibung benötigt und daher wird an dieser Stelle auf die bereits referenzierte Literatur verwiesen.

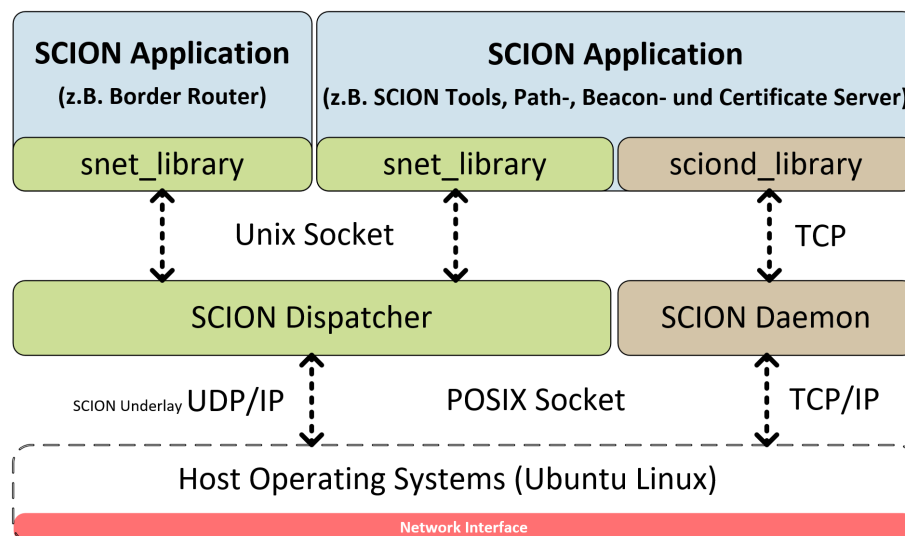


Abbildung 6.2.: SCION Network Stack (nach [28])

Muss eine SCION Applikation über das Netzwerk kommunizieren, ist sie vorwiegend auf den SCION Dispatcher und Daemon angewiesen. Zwischen den verschiedenen SCION Applikationen ermöglichen die Unix Sockets¹ mittels der snet-Bibliothek die Interprozesskommunikation. Auf dem Underlay-Netzwerk empfängt und versendet der Dispatcher über seinem UDP/IP-Listener dem POSIX Socket² die SCION Datenpakete und ordnet die Daten den korrespondierenden Services basierend dem L4-Header z. B. durch die

¹Unix Sockets ermöglichen die Kommunikation zwischen zwei verschiedenen Prozessen auf demselben oder verschiedenen Computern. Genauer gesagt können Sie mit Standard-Unix-Dateideskriptoren mit anderen Computern kommunizieren. Unter Unix wird jede I/O-Aktion durch Schreiben oder Lesen eines Dateideskriptors ausgeführt. Ein Dateideskriptor ist nur eine Ganzzahl, die einer geöffneten Datei zugeordnet ist. Es kann sich um eine Netzwerkverbindung, eine Textdatei, ein Terminal oder etwas anderes handeln. ©Tutorials Point

²Das Portable Operating System Interface (POSIX) ist eine gemeinsam vom IEEE und der Open Group für Unix entwickelte standardisierte Programmierschnittstelle, welche die Schnittstelle zwischen Anwendungssoftware und Betriebssystem darstellt.

Portadressen zu. Der Hintergrundprozess namens SCION Daemon ist für die Control Plane Interaktionen zuständig. Jegliche Intra-AS-Control-Abfragen wie z. B. Path Lookups oder AS Informationen erfolgen direkt und ausschliesslich mittels dem TCP/IP-Protokoll und die Inter-AS-Control-Kommunikation erfolgt mittels dem zuverlässigen und sicheren QUIC/SCION³ über das UDP/IP-Underlay. Wie bestimmt festgestellt, erfolgen sie über den SCION Dispatcher via Border Router. Weitere Details entnehmen sie bitte den nachfolgenden Unterkapiteln.

6.2. Container Bundels

Im vorangegangenen Kapitel 5 wurde die momentan bestehende Situation und anstehenden Korrekturen kurz erläutert. Bei der Implementation von neuen Technologien und Architekturen kann es in frühen Projektphasen immer wieder zu unverhofften und unvorhergesehenen Fragestellungen und Schwierigkeiten kommen. An die geänderten Gegebenheiten folgten konkrete Anpassungen und manchmal behelfen sich die Techniker mit Workarounds. Konkret sprechen wir hier über die SIX CA und das High-Availability-Setup. Der Kundenrouter beinhaltet alle SCION Services, die für dieses Projekt resp. Arbeit benötigt und in den Fragestellungen behandelt werden. Der Fokus liegt daher bei der momentan empfohlenen SCION Border Router Konfiguration auf der Endkundenseite.

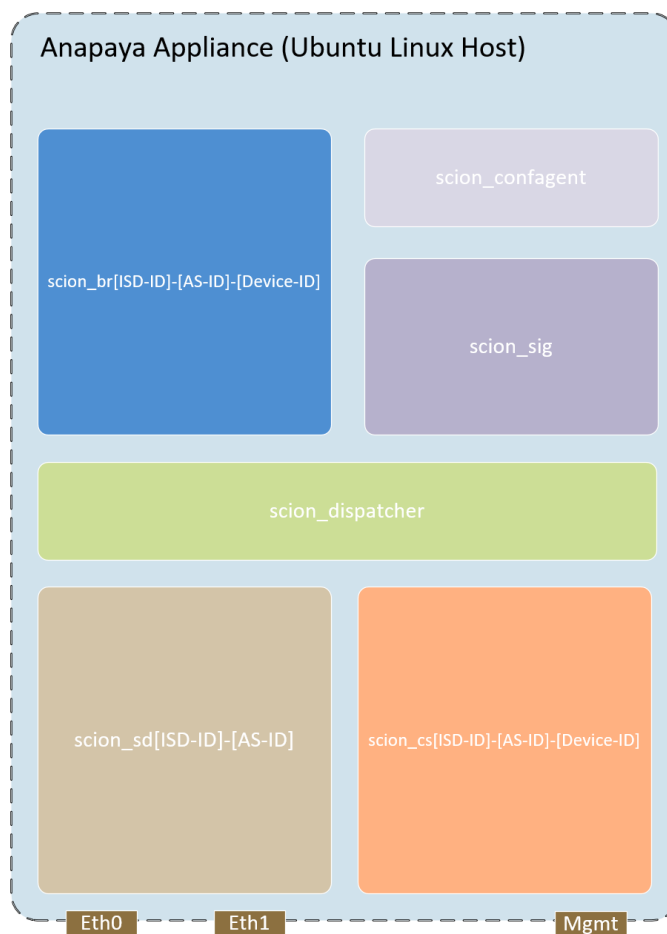


Abbildung 6.3.: Customer SCION Border Router - Container Overview

³https://de.wikipedia.org/wiki/Quick_UDP_Internet_Connections

Wie die Abbildung 6.3 zeigt, können und werden üblicherweise alle SCION Services bei den Kunden auf einer Appliance betrieben. In naher Zukunft, ist es angedacht, gewisse Services in einem einheitlichen Container zu verschmelzen. Sie laufen wie erwähnt in einzelnen Docker Container und sind teilweise stark voneinander abhängig. Über das bekannte Tool „Docker Compose“ werden die Docker-Anwendungen mit mehreren Containern auf dem System definiert, gesteuert und ausgeführt. Die YAML-Datei „docker-compose.yml“ ist eine Konfigurationsdatei, die es erlaubt, die Dienste der Anwendungen zu kombinieren und gleichzeitig zentral zu konfigurieren. In diesem Setup gibt es zwei unterschiedliche Verzeichnisse resp. Konfigurationsdateien. Die grundlegenden SCION Services wie der Dispatcher, Daemon, Control Service und Border Router werden gemeinsam über die YAML-Datei im Verzeichnis „/etc/docker-compose/scion/“ und die SIG Services im Verzeichnis „/etc/docker-compose/sig/“ definiert. Anhand der oberen Abbildung werden nachfolgend die einzelnen Container in ihrer Funktionalität mit ihren Abhängigkeiten detailliert beschrieben. Zusätzlich werden die direkt exponierten externen Services auf der Netzwerkschnittstelle ersichtlich gemacht. Hier wird ein Kundenrouter bezeichnet als SCION IP Gateway (SIG) betrachtet, genau so wie in der Abbildung 1.1 sehr vereinfacht veranschaulicht, kommt er kundenseitig bei SNB und SIX zum Einsatz. Er verbindet die legacy IP-Netzwerke über die SCION-Infrastruktur miteinander und ermöglicht über einen SCION-Tunnel die IP-Kommunikation der Kundenanwendungen. Da die meisten Applikationen kein natives SCION unterstützen ist das SIG die wichtigste Komponente und einzige Möglichkeit sich über die SCION-Insel zu verbinden. Er stellt sozusagen das IP-Routing über SCION zwischen den Kunden sicher.

Bevor wir in die einzelnen Funktions- und Servicebeschreibungen eintauchen, werden zuerst die standardisierten SCION Kommunikationsports mit ihren reservierten Bereichen aufzeigen und grob umschreiben. Die oben aufgezeigten SCION Elemente (Container) kommunizieren mittels unterschiedlicher Protokolle und kommunizieren über unterschiedliche Serviceports. Diese Informationen sind nicht nur hier von Interesse. Unter den Cyber Security Themenbereichen „Penetration Testing“ und „Vulnerability Management“ haben sie eine besondere Relevanz, da die Services z. B. mittels Fuzzing Traffic und Scans auf ihre Robustheit resp. Sicherheitslücken getestet werden.

Tabelle 6.1.: Übersicht der verwendeten Protokollen und Services

Beschreibung	Protokoll	Portbereich
Die Data Plane ist vor allem für die Weiterleitung von SCION Paketen auf dem Underlay verantwortlich. Jedem SCION Element wie dem Dispatcher, BR und SIG ist ein spezifischer Service Port fix zugeordnet. Sie sind konzeptionell vordefiniert und mit einer Ausnahme, nämlich dem Dispatcher, nicht hartkodiert. Die anderen könnten über die entsprechenden Konfigurationsdateien frei bestimmt werden. Beim Dispatcher und BR sprechen wir über den Underlay-UDP/IP-Port und im Spezialfall des SIGs handelt es sich um einen UDP/SCION-Port, der als Serviceadresse zu verstehen ist und zwischen der Applikation „SIG“ und dem Dispatcher fungiert.	UDP/IP oder UDP/SCION	30'0xx

Tabelle 6.1: weiter auf nächster Seite

Tabelle 6.1: Weiterführung von vorheriger Seite

Beschreibung	Protokoll	Portbereich
Die Control Plane ist vor allem für die SCION Control Services verantwortlich. Jedem SCION Element wie dem SCIOND, CS, BR oder SIG ist ein spezifischer Service Port fix zugeordnet. Sie sind konzeptionell vordefiniert, aber nicht hartkodiert und könnten grundsätzlich über die entsprechenden Konfigurationsdateien frei gewählt werden. Die Control Services innerhalb des AS werden direkt über TCP/IP angesprochen. Alle anderen Ports sind als Serviceadressen zu verstehen und fungieren zwischen der Applikation und dem Dispatcher.	TCP/IP oder UDP/SCION oder QUIC/SCION	30'2xx
Das Monitoring der SCION Services findet über HTTP statt. Jedes SCION Element wie der Dispatcher, SCIOND, CS, BR oder SIG besitzt ein spezifischer TCP/IP Service Port. Der Bereich ist konzeptionell vordefiniert, aber nicht hartkodiert und könnten grundsätzlich über die entsprechenden Konfigurationsdateien frei gewählt werden.	TCP/IP	30'4xx
Der SIG Confagent wird momentan nur im Zusammenhang mit dem SIG verwendet und unterstützt unterschiedliche Funktionalitäten. Er kann beispielsweise die SIG Services neu starten oder Änderungen an der SCION IP Gateway Konfiguration (z. B. Remote Networks oder Traffic Policy) vornehmen. Jegliche Interaktionen finden über das Protokoll „gRPC“ ⁴ statt. Die SCION Elemente wie der Confagent und das SIG kann demnach von Remote z. B. via dem Organization Manager provisioniert werden. Diese TCP/IP Service Ports sind konzeptionell vordefiniert, aber nicht hartkodiert und könnten grundsätzlich über die entsprechenden Konfigurationsdateien frei gewählt werden.	TCP/IP	31'xxx und 32'xxx

Tabelle 6.1: Ende der Tabelle erreicht.

Wie die obere Tabelle andeutet, gibt es auf einem SCION-Host eine Vielfalt von laufenden Services. Grundsätzlich könnte das auf dem High-Level gezeigte SCION-Gateway auch auf unterschiedlichen separierten Hosts laufen. Jedoch macht es konzeptionell, resourcentechnisch und finanziell keinen Sinn, die SCION-Services getrennt zu betreiben. Zur vereinfachten Veranschaulichung und für eine vereinfachte Erläuterung erscheint es jedoch vernünftig die Services getrennt aufzuzeichnen. Es ist wichtig die zuvor beschriebenen Konzepte verstanden zu haben, ansonsten könnte es ohne Vorwissen schwierig sein, die essenziell wichtigen funktionellen Zusammenhänge auf Kommunikationsebene zu erkennen.

In der Abbildung 6.4 wird versucht aufzuzeigen, auf welche SCION-Elemente die einzelnen SCION-Komponenten zumindest angewiesen sind, um ihre Funktionen wahrzunehmen. In der Praxis werden alle SCION-Komponenten auf einem Host betrieben und die gleichen Container, Komponenten und Schnittstel-

⁴<https://grpc.io/faq/>

- **scion_sd[ISD]-[AS-ID]**

Der SCION Daemon ist ein Hintergrundprozess auf dem Endhost und behandelt SCION Control Plane Nachrichten und bietet die API-Schnittstelle zwischen den Applikationen und der SCION Control Plane. Er behandelt beispielsweise die Pfadanfragen (Path Lookups) und stellt die AS-spezifische Informationen wie MTU, ISD-AS, interne Border Router und Control Server Adresse (Topology Infor-

mation) bereit. Zudem hält er den eigenen Trust Store (Trust Management) aktuell und teilt über die sciond-Library die notwendigen Informationen den SCION Applikationen mit. Der Informationsaustausch geht üblicherweise intern via Loopback-Adresse 127.0.0.1 und TCP-Port 30'255 vonstatten. Die AS-spezifischen und statischen Daemon-Konfigurationen erfolgen manuell über die Datei „sd.toml“. Sie befindet sich im Verzeichnis „/etc/scion/sd[ISD]-[AS-ID]-[Device-ID]/“ und bei jeglichen Änderungen benötigt es einen Serviceneustart.

- **scion_dispatcher**

Der SCION Dispatcher kann als Mediator zwischen den SCION-Applikationen und dem UDP/IP-Underlay-Netzwerk angesehen werden und ist für die Einkapselung und Entkapselung bezüglich UDP/SCION, QUIC/SCION, SCMP/SCION und künftig BFD/SCION verantwortlich. Ausserdem registriert und leitet er die empfangenen Datenpakete anhand der Serviceportadresse an die richtige SCION-Anwendung (z. B. dem Beacon-, Path-, Certificate und SIG-Service) weiter. Wenn der BR beispielsweise eine Certificate Service Anfrage oder PCBs bekommt leitet er sie intern an den Certificate-, Beacon- oder Path-Server weiter. Pakete mit den Serviceadressen 30'056 oder 30'256 werden vom BR direkt zum SIG-Dispatcher weitergeleitet. Die SCION-Portadresse 30'056 signalisiert dem SIG im Payload eingekapselte Applikationsdaten, die vor der IP-Weiterleitung zuerst wieder entpackt werden müssen. Um den Status des gegenüberliegenden SIGs festzustellen, findet zwischen den Gateways ein sogenanntes Probing statt. Probing-Pakete erkennen wir am SCION-Port 30'256. Bei allen SCION-Netzwerk-Komponenten hört der Dispatcher auf allen Schnittstellen und seinem standardisierten Underlay-UDP/IP-Port 30'041 auf Anfragen oder entsendet die selbst generierten SCION-Pakete mit dessen Source-Port.

Die AS-spezifischen und gleichbleibenden Dispatcher-Konfigurationen erfolgen auch hier manuell. Die Datei „dispatcher.toml“ befindet sich im Verzeichnis „/etc/scion/dispatcher/“ und wie gewohnt benötigt es bei allen Änderungen einen Serviceneustart.

6.2.2. Control Services

Die Control Services sind in einem eigenen gemeinsamen SCION-Element integriert und sind zusätzlich auf die beiden bereits besprochenen SCION-Elemente angewiesen. Sie können demnach nicht eigenständig auf einem Host betrieben werden. Die CS interagieren und stellen ihre Services insbesondere den Endhosts, SIGs und Border Routern zur Verfügung.

Containers:

- **scion_sd[ISD]-[AS-ID]**

Damit die Abhängigkeiten aufgezeigt werden können, wurde dieser Container zur Vollständigkeit aufgeführt. Genauere Details entnehmen sie bitte den Beschreibungen aus dem Unterabschnitt 6.2.1.

- **scion_dispatcher**

Damit die Abhängigkeiten aufgezeigt werden können, wurde dieser Container zur Vollständigkeit aufgeführt. Genauere Details entnehmen sie bitte den Beschreibungen aus dem Unterabschnitt 6.2.1.

- **scion_cs[ISD]-[AS-ID]-[Device-ID]**

Der Control Service implementiert also in einem Container zusammengefasst die bereits in der Einleitung geschilderten SCION Control Plane Aufgaben (Keep-Alive-, Beacon-, Path-, und Certificate-Server). Er nimmt alle Intra-AS-Anfragen ausnahmslos über das klassische IP-Netzwerk entgegen, da alle Netzwerkteilnehmer innerhalb vom AS auch über IP erreichbar sein müssen, macht es keinen

Sinn den CS über SCION anzusprechen. So nimmt beispielsweise ein SCION-Host die Path Requests über den TCP/IP-Port 30'252 entgegen und beantwortet sie dementsprechend. Control Services interagieren AS-übergreifend zwangsläufig über den SCION-Stack und sind auf den Dispatcher angewiesen. Die Control Informationen gehen über UDP/SCION (QUIC) und werden mittels der Portadresse 30'252 gekennzeichnet. Bei einem eingehenden SCION-Paket, mit einer Serviceportadresse 30'252 im SCION-L4-Header, leitet der BR dieses über das interne BR-Interface an den Control Server weiter. Der Dispatcher nimmt es auf dem Underlay-UDP/IP-Port 30'041 entgegen und übergibt es dem entsprechenden Control Server zur Verarbeitung. Nur am Rande erwähnt, auch in einem CS-High-Availability-Setup verständigen und synchronisieren sich die Cluster-Members über das IP-Netzwerk miteinander.

Die AS-spezifischen und fixen CS-Konfigurationen erfolgen auch manuell und finden über die Datei „cs.toml“ statt. Sie befindet sich im Verzeichnis „/etc/scion/cs[ISD]-[AS-ID]- [Device-ID]/“ und benötigen nach Anpassungen einen Serviceneustart.

6.2.3. Border Router

Einem Border Router ergeht es ähnlich wie den Control Services und benötigen zusätzlich den Dispatcher, um seine wenigen Kontrollfunktionen wahrzunehmen. SCION-native-Endhosts kommunizieren nach der Pfadabfrage direkt über SCION via dem internen Border Router Interface. Aus Redundanz- und Performancegründen kann ein BR mehrere physische und logische Schnittstellen aufweisen. Per Design ist im Moment nur ein Intra-AS-Link vorgesehen und implementierbar. Innerhalb vom eigenen AS müssten für Redundanzzwecke mehrere BRs bestehen. Inter-AS-Links können mehrere logische Schnittstellen zu Remote-ASes konfiguriert werden. Gewisse Optimierungen sind bereits in der Pipeline. Eine genauere Erläuterung zu SCION-Interfaces folgt nach den Container-Erläuterungen.

Containers:

- **scion_dispatcher**

Damit die Abhängigkeiten aufgezeigt werden können, wurde dieser Container zur Vollständigkeit aufgeführt. Genauere Details entnehmen sie bitte den Beschreibungen aus dem Unterabschnitt 6.2.1.

- **scion_br[ISD]-[AS-ID]-[Device-ID]**

Der Border Router implementiert die sogenannte SCION Data Plane Forwarding (Fastpath), mit der Hauptfunktionalität die erhaltenen SCION-Datenpakete schnellstmöglich weiterzuleiten. Unter den SCION-Datenpaketen verstehen wir vor allem den in SCION eingekapselten, applikatorischen Datenverkehr zwischen den Endhosts. Ein BR nimmt alle SCION-Pakete auf dem internen und externen Interface des spezifizierten Underlay-UDP/IP-Ports 30'042 entgegen. Handelt es sich um ein Data Plane Paket leitet er es zustandslos und umgehend dem nächsten BR weiter. Wie erklärt, stehen dank PCFS alle notwendigen Informationen für die Paketweiterleitung schon im SCION-Header in den Hop Fields (HFs). Die ankommenden Datenpakete nimmt er entgegen und liest für die Weiterleitung und Verifikation (z. B. Ingress Interface, Source-Underlay-IP, HF Lifetime, HF MAC) nur den für ihn relevanten HF-Bereich seines ASes aus. Dafür ist er auf einen bereits gesetzten Pointer (Offset) angewiesen, der auf das aktuelle HF zeigt. Der Pointer wird initial vom ersten Router im Pfad gesetzt und jeder darauffolgende und ausgehende Router inkrementiert ihn entsprechend nach der Verarbeitung. Bevor das Datenpaket den Router endgültig verlässt, folgt nach dem Pointer-Update die bekannten Anpassungen des Ethernet-Header und die eher unkonventionellen Anpassungen des UDP/IP-Headers. Im Ethernet-Header werden wie gewohnt die Layer2-Informationen

(MAC-Adressen) und zusätzlich die Layer3/4-Informationen (UDP/IP-Underlay) anhand dem ausgehenden Punkt-zu-Punkt-Netzwerkes angepasst. SCION ist momentan noch auf das UDP/IP-Underlay angewiesen, aber zukünftig sollte es auch direkt auf der L2-Ethernet-Ebene ausgeführt werden können, wenn eine direkte Verbindung zwischen Border Routern gegeben ist.

Die Keep-Alives und PCBs gehören zu SCION-Control-Datenpaketen, die auf dem internen BR-Interface entgegengenommen werden und anschliessend zu den benachbarten ASes via den externen Interfaces weitergeleitet. Auch diese Control Plane Pakete nimmt er vom CS, mit dem Source-Underlay-UDP/IP-Port 30'041, auf dem Underlay-UDP/IP-Port 30'042 entgegen. Muss der BR aus irgendwelchen Gründen einen Service für einen Update anfragen, so muss er z. B. ein Beacon für ein TRC-Update über seinen Dispatcher beim Control Service abfragen. Die Überprüfung des Nachbarstatus mittels versenden von Keep-Alives oder das Informieren der Sender, mit selbst generierten oder weitergeleiteten SCMP-Replies über ungültige Pfade, findet über den im Border Router integrierten Control Process (Slowpath) statt. Die Keep-Alive-Nachrichten werden in regelmässigen Abständen, mit der entsprechenden Schnittstellenkennung, an seinen benachbarten Router versendet. Der Remote-AS-BR leitet wiederum diese Nachricht an alle Beacon-Server in seinem AS weiter. Das Intervall zwischen diesen Keep-Alive-Nachrichten ist im Voraus bekannt, sodass ein Beacon Server eines AS verpasste Nachrichten erkennen kann. Nach einer bestimmten Anzahl verpasster Nachrichten kann ein Master-Beacon-Server die Schnittstelle als inaktiv betrachten und sie werden dann nicht mehr zu neuen PCBs hinzugefügt. Eine inaktive Schnittstelle könnte auch alle anderen Pfade, die Informationen zur Schnittstelle enthalten, widerrufen.

Die AS-spezifischen und relativ festen BR-Konfigurationen erfolgen wie vertraut manuell. Die Datei „br.toml“ befindet sich im Verzeichnis „/etc/scion/br[ISD]-[AS-ID]-[Device-ID]/“ und wie üblich benötigen auch sie bei Konfigurationsanpassungen einen Serviceneustart.

SCION Interfaces:

Jedes SCION Interface benutzt eine unique IP:Port-Zuordnung auf dem Underlay (UDP/IP). SCION Interfaces auf dem selben Physical Port (Port-1) und dem selben Virtuellen Network Interface (VNI-1) können identische IP-Adressen aufweisen und unterscheiden sich somit nur über den UDP-Port. Auf unterschiedlichen Routern im selben AS dürfen sie zudem die identischen IP-Adressen verwenden, weil wir hier bekanntlich nur von lokalen Punkt-zu-Punkt-Verbindungen sprechen und sie lediglich zwischen den Routern gültig sind. Würden wir jedoch SCION als Overlay in einem gerouteten Netzwerk betreiben, dürften allerdings die Peer-Netzwerke an denen SCION terminiert nur einmalig im Internet vorkommen. Bei den internen IntIF- und externen ExtIF-SCION-Interfaces könnte eine Adressierung wie folgt aussehen:

Der Border Router besitzt im unteren Fall lediglich eine physikalische und virtuelle Schnittstelle (One-Armed-Router / Router-on-a-Stick).

Ingress Interface: *Eth0/VNI-1/IntIF-1 = 10.1.0.1:30000*
Egress Interface: *Eth0/VNI-1/ExtIF-1 = 10.1.0.1:50000*

Der Border Router besitzt jeweils zwei physische und virtuelle Schnittstellen. Gegenüber dem vorhergehenden Beispiel wird so die Bandbreite erhöht. Im Moment wird nur ein eingehendes und ein ausgehendes physisches Interface unterstützt. Deshalb zeigt das folgende Beispiel die ausgehende Redundanz über zwei unterschiedliche ExtIF-SCION-Interfaces.

Ingress Interface: *Eth0/VNI-1/IntIF-1 = 10.1.0.1:30000*
Egress Interfaces: *Eth1/VNI-2/ExtIF-1 = 10.2.0.1:50001*
 Eth1/VNI-2/ExtIF-2 = 10.2.0.1:50002

Der Border Router besitzt auch hier wieder jeweils zwei physische und virtuelle Schnittstellen, jedoch wurde die Hardwareabstraktion durch zwei getrennte externe VNIs erweitert. Dieses erweiterte Konzept verschafft nicht mehr Bandbreite, aber dem Netzwerkadministrator mehr Kontrolle über die Infrastruktur.

Ingress Interface: *Eth0/VNI-1/IntIF-1 = 10.1.0.1:30042*
Egress Interfaces: *Eth1/VNI-2/ExtIF-1 = 10.2.0.1:30042*
 Eth1/VNI-3/ExtIF-2 = 10.3.0.1:30042

6.2.4. SCION IP Gateway

Eines der wohl wichtigsten SCION Komponente im Netzwerk ist das SIG, um die Interoperabilität zwischen SCION und dem legacy IP-Netzwerk herzustellen. Zwischen legacy IP-Netzwerken wird die Konnektivität mittels SIG-Tunnels erreicht. Die SIGs werden wie IP-Router an das IP-Netzwerk gehängt und mit der SCION-Insel verbunden. Die auf dem SIG statisch konfigurierten oder dynamisch gelernten Routes (IP-Prefixes) müssen noch zusätzlich auf dem Remote SIG manuell konfiguriert werden. Künftig sollen die IP-Prefixes, welche über ein dynamisches IP-Routingprotokoll wie BGP oder OSPF gelernt wurden, auch automatisch und authentifiziert in den SIGs integriert werden. Die Authentifizierung erfolgt künftig wie gewohnt über die Signierung des jeweiligen CP AS Zertifikates. Die zusätzliche Einkapselung, wie in der Abbildung 6.1 ersichtlich, erfolgt obendrauf von UDP/SCION mit einem zusätzlichen SIG Frame Header und muss aus Effizienzgründen verbindungslos (stateless and unreliable) bleiben. Würde ein verlässliches Protokoll dazu verwendet werden, könnte es zu erhöhten Retransmissions führen und unnötig die Bandbreite schmälern. Wie vermutlich bemerkt, ist dieser Prozess sehr Ressourcenintensiv, da alle Pakete zwangsläufig über den Slow Path laufen wie beim BR. Wenn immer möglich, sollte unbedingt auch auf Fragmentierung, verursacht durch Jumbo Frames, verzichtet werden. Das Gateway bietet eine Vielzahl an Kombinationen von Arten wie der Datenverkehr gesteuert werden kann. Über Traffic Policies, können sogenannte Path Policies statisch oder dynamisch, auf den Datenfluss direkten Einfluss nehmen. Statische Definitionen bestimmen mittels Black- und Whitelists über welche ISDs, ASes, SCION-Interfaces und/oder Shortest Paths der Datenfluss gehen darf. Sogar mittels sich verändernden Messwerten wie Latency, Jitter und/oder Loss kann dynamisch auf den Datenfluss eingegriffen werden. Das kann nur durch eine konstante Überwachung mit aktiven Tests des Netzwerkes erfolgen. Die vielfältige Steuerung des Datenverkehrs schafft eine erhöhte Verlässlichkeit und Sicherheit des Datentransfers. Ein SIG ist wie ein SCION Host auf die Unterstützung der beiden SCION-Elemente den Dispatcher und Daemon angewiesen. Für den Betrieb reicht also der SIG-Container alleine nicht aus, denn jeglicher Datenverkehr muss wie gewohnt vom Dispatcher bearbeitet und über einen BR gesendet oder von einem BR entgegengenommen werden.

Containers:

- **scion_sd[ISD]-[AS-ID]**

Damit die Abhängigkeiten aufgezeigt werden können, wurde dieser Container zur Vollständigkeit aufgeführt. Genauere Details entnehmen sie bitte den Beschreibungen aus dem Unterabschnitt 6.2.1.

- **scion_dispatcher**

Damit die Abhängigkeiten aufgezeigt werden können, wurde dieser Container zur Vollständigkeit aufgeführt. Genauere Details entnehmen sie bitte den Beschreibungen aus dem Unterabschnitt 6.2.1.

- **scion_confagent**

Der Configuration Agent ist optional und dient zur vereinfachten Konfiguration und Steuerung des SIGs durch den Netzwerkadministrator. Über gRPC können die Remote Networks und die erwähnten

Traffic Policies konfiguriert oder über Docker-Compose die SCION Services neu gestartet werden. Der Agent nimmt die Anfragen auf dem TCP/IP-Port 32'256 entgegen.

Bei SIG-Konfigurationsänderungen wird die Datei „sig.json“, welche sich im Verzeichnis „/etc/scion/sig/“ befindet, entsprechend angepasst. Anschliessend stösst der Agent einen Neustart des SIG-Dienstes an, damit die neue SIG-Konfiguration aktualisiert wird. Der Confagent bietet noch weitere wertvolle Funktionen, die im Entwicklungsprozess laufend erweitert werden. Zukünftig soll er auch auf den anderen SCION-Komponenten zum Einsatz kommen. Der Confagent selbst lässt sich nur manuell über die Konfigurationsdatei „confagent.toml“, welche sich im Verzeichnis „/etc/scion/confagent/“ befindet, steuern.

- **scion_sig[ISD]-[AS-ID]-[Device-ID]**

Der SIG-Container funktioniert wie eine typische SCION Applikation und ist daher wie schon angedeutet auf die Dispatcher- und Daemon-Funktionalität angewiesen. Denn wie sonst könnte das Datenpaket ohne Pfad resp. SCION-Header und Hop Fields gesteuert an ihr Ziel gelangen. Bevor das SIG das SCION-Datenpaket zusammenstellt, muss er die möglichen Pfade, falls er sie noch nicht im Cache hat, beim Control Service mit Hilfe dem Daemon abfragen. Die Abfrage erfolgt wie bekannt über TCP/IP auf dem Control Service Port 30'252. Danach stellt er den SCION- und SIG-Header anhand der Traffic Policy zusammen und sendet das Paket mit den Pfadinformationen über den Dispatcher zu seinem nächsten BR. Der SIG versendet also alle Datenpakete mit dem UDP/IP-Sourceport 30'041 auf den UDP/IP-Destinationport 30'042 zum BR und umgekehrt als Paketempfänger. Nach gewohntem Prozedere, gelangt nun z. B. eine HTTP-Nachricht über den SIG-Tunnel zum Remote-AS-SIG, der das Datenpaket wieder entpackt und dem zugehörendem Zielserversystem z. B. einem Webserver weiterleitet. In der Abbildung 6.4 ist ein TCP-Listener 31'256 vermerkt. Über diesen Port nimmt das SIG die Steuerungsanfragen und Konfigurationen vom Confagent entgegen. Direkte Ansteuerungen von ausserhalb sind momentan konzeptionell nicht angedacht. Im Unterabschnitt 6.2.1 SCION Host wurde schon etwas betreffend SIG-Serviceportadressen vorgegriffen und daher hier nochmals kurz zur Erinnerung. Der im UDP/SCION referenzierte Serviceport 30'056 signalisiert dem Dispatcher den im SIG-Tunnel eingekapselten Datenverkehr und mittels dem Serviceport 30'256 findet das SIG-Probing (Health Checks) zwischen den Gateways statt.

Die AS-spezifischen SIG-Konfigurationen sind in zwei unterschiedliche Teilbereiche aufgeteilt. Den automatisierten und eher dynamischen Teil spielt sich über den bereits kennengelernte Confagent ab und der manuelle und eher feste Teil erfolgt über die Datei „sig.toml“, die sich im selben Verzeichnis „/etc/scion/sig/“ befindet.

6.2.5. Common Configuration

Wie wir zuvor gesehen haben, gibt es auf allen SCION-Netzwerkteilnehmern jeweils eine AS-spezifische und relativ einheitliche, auf das jeweilige SCION-Element, abgestimmte Konfiguration. Zusätzlich zu diesen eher servicebezogenen Konfigurationen benötigt es weitere funktionelle und sicherheitsrelevante Einstellungen und Schlüsselmaterialien. Auf allen Netzwerkteilnehmern innerhalb demselben AS müssen sie absolut identisch sein. Das AS-globale Konfigurationsverzeichnis „/etc/scion/common[ISD]-[AS-ID]/“ könnte theoretisch, vor allem in der initialen Aufbauphase, zwischen den Teilnehmern synchronisiert werden. Im normalen Betrieb findet dann eine Aktualisierung der Zertifikate und TRCs automatisch statt.

Die Konfigurationsdatei „topology.json“ befindet sich im Basisverzeichnis „/etc/scion/common[ISD]-[AS-ID]/“ und definiert die Netzwerktopologie aller im AS befindlichen SCION-Services. Konkret sprechen wir hier über die Komponenten SIG, BR und CS. In dieser Spezifikation sind für die Kommunikati-

on notwendige AS-spezifische Informationen wie Attribute, Komponentennamen, lokale und remote ISD- und AS-IDs, Underlay-IP-Adressen und Ports, MTU, Bandbreite etc. eingetragen. Im tieferliegenden Verzeichnis „/etc/scion/common[ISD]-[AS-ID]/keys“ befinden sich zwei verschiedene Schlüsseltypen, der AS-eigene Private Key „cp-as.key“ und mindestens ein AS-lokaler Master Key „master[ID].key“. Um einen unterbrechungsfreien Schlüsselaustausch zu gewährleisten, bestehen normalerweise zwei Schlüssel, die während eines kurzen Zeitraums in der Übergangsphase (Grace Period) beide gültig sind. Wie in der Einleitung bereits erwähnt, findet die Schlüsselableitung (Key Derivation Function) on-the-fly über den DRKey-Mechanismus statt. Der zum AS korrespondierende Private Key wird für die PCB-Signierung verwendet und kann anhand des gültigen TRCs⁵ über den Public Key validiert werden. Wie bekannt liegt die Verteilung der symmetrischen Schlüssel innerhalb dem AS selbst. Innerhalb des AS wird mindestens ein Master Key verteilt, der dazu verwendet wird, um effizienter andere Schlüssel abzuleiten. Es wird z. B. ein Schlüssel zur Erstellung und Überprüfung von Hop Fields (HF) oder Erweiterungen verwendet. In einem anderen Unterverzeichnis „/etc/scion/common[ISD]-[AS-ID]/certs“ befindet sich das AS-Zertifikat „cp-as.crt“ und „cp-as.pem“ und die relevanten TRCs beispielsweise mit dem Namen „ISD[ISD]-B1-S1.trc“. Im TRC-Namen steht das B für die Base Number⁶ und das S steht für die Serial Number⁷. Das initiale TRC, auch genannt als Base-TRC⁸, so wie im Beispiel genannt, muss zu Beginn immer die Nummer 1 aufweisen.

6.2.6. AS-spezifische Service Konfigurationsoptionen

Die genauen Service-Konfigurationsoptionen für die statischen und dynamischen Bereiche sind zu diesem Zeitpunkt nicht bekannt und in diesem Themenschwerpunkt nicht sicherheitsrelevant. Das wurde so dem Autoren von den Anapaya Spezialisten⁹ mitgeteilt und versichert. Aus diesem Grund werden sie hier nicht weiter aufgegriffen und berücksichtigt. Sie sind jedoch in den internen Dokumentationen bei Anapaya Systems AG detailliert beschrieben und dementsprechend vermerkt.

6.3. Einleitung Container Baseline Security

Die einleitenden Fakten, sollen wie unter Abschnitt 5.1 erwähnt, einfach in angepasster Form, auch für diesen Themenschwerpunkt gelten und möchten hier nicht nochmals wiederholt werden. Jegliche SCION-relevanten Tests sind in einer separaten und neunten Lynis-Test-Gruppe abgebildet und dokumentiert. Sie können gerne auf der beiliegenden CD-ROM eingesehen werden. Wie gewohnt, finden sie nachfolgend die Abweichungen zur momentanen bestehenden gehärteten Anapaya-Konfigurationen mit entsprechenden Begründungen zu den Empfehlungen und den bereits gehärteten und absolut unverzichtbaren Container-Konfigurationen. Mit Hilfe der ausgearbeiteten Kontrollen, fand eine Überprüfung der angehenden SCION-Router-Konfiguration statt. Dadurch kann der Angriffsvektor direkt auf die SCION-Applikationsservices möglichst tief gehalten werden. Die verwandten Kontrollen, werden falls möglich mit den CIS-Empfehlungen im Lynis-Skript¹⁰ direkt referenziert. Die ausgearbeiteten SCION-Härtungsmassnahmen beruhen auf sehr umfangreicher Literatur[26][25][27][39][43][54][66] und anderen verlässlichen Internet-Quellen[42][38]

⁵Der TRC Payload ist ein sogenannter signierter Container, der die Zertifikats- und Policy-Informationen beinhaltet. Die Daten sind gemäss den Regeln von ITU-T X.690 nach ASN.1 codierte und signiert als eine Sammlung von X.509 v3 Zertifikaten.

⁶Die Base Number zeigt den Startpunkt der TRC-Update-Kette an.

⁷Die Serial Number zeigt die Subsequenz der TRC-Update-Kette an. Bei jedem TRC-Update wird es inkrementiert.

⁸Kann initial von SCION nicht überprüft werden und muss von einem vertrauenswürdigen System kommen.

⁹Wurde am Zwischenstatusmeeting vom 22.10.2020 mit Sam Hitz besprochen.

¹⁰Die Tests befinden sich auf der CD-ROM in der Datei „Auditing/B - lynis-v3.0.3_SCION_VERSION/lynis/include/tests_anapaya_services“. Bitte beachten Sie, bei der Durchsicht besonders auf die Kommentare, da sie einige wichtige und hilfreiche Informationen zu den SCION Erweiterungen geben.

[16][46][61]. Auch hier, sind sich offensichtlich die namhaften Autoren, Softwareentwickler und/oder Sicherheitsexperten weltweit einig, wie notwendig zusätzliche Container-Sicherheitsmassnahmen sind und kommen sehr oft auch zu den gleichen oder sehr ähnlichen Empfehlungen. An dieser Stelle, ist es nochmals äusserst wichtig anzumerken, dass hier der Fokus auf Kontrollen oder Empfehlungen mit ganz klaren Sicherheitsvorteilen für ein SCION IP Gateway (SIG) liegt. Bei einem SIG läuft nebst den SCION-Services meist auch noch ein dynamischer IP-Routing-Service z. B. OSPF oder BGP, denn auf einem reinem SCION Border Router befinden sich im Normalfall keine derartige dynamische Routing-Services. Das unterliegende IP-Netzwerk zwischen den BRs ist mehrheitlich nur noch das Peering-Subnetz für das SCION-Overlay. Die effektive SCION-Technologie darf auf keinen Fall beeinträchtigt oder beeinflusst werden. Somit besteht die Anforderung einer vor- und nachträglichen Empfehlungsprüfung durch SCION-Spezialisten und einer Verifizierung der optimierten SCION-Konfiguration in der Testumgebung. Eine direkte Umsetzung wird daher nie empfohlen. Ausserdem müssen die Kontrollen, nach jeder Änderung am Betriebssystem oder an den laufenden Applikationen, überprüft und abgestimmt werden. Wie schon mehrfach erwähnt, wird ein derartiger Prozessschritt in der Softwarewartung ein wichtiger Bestandteil.

6.4. Empfehlungen zur Containerhärtung

Durch die detaillierte SCION-Router-Einführung konnte erklärt und aufgezeigt werden, wie und wo (in welchem Docker-Container) die SCION-Funktionen ihre Dienste verrichten. Es ist wichtig zu wissen und zu verstehen, dass die SCION-Services in Containern laufen und in welchem Zusammenhang sie zueinander stehen. In diesem Kapitel vertiefen wir uns daher noch zusätzlich mit der Container-Security und machen Überlegungen zu weiteren Schutzmassnahmen, um die Netzwerk-Infrastruktur und die SCION-Services selbst noch besser vor Cyber-Angriffen zu schützen. Aufgrund der Virtualisierung gilt das zuvor behandelte Thema Anapaya - Appliance OS Security als Grundbedingung und daher ist es sehr nah verwandt und oftmals verständlicherweise überschneidend oder sehr ähnlich. Die damaligen Prinzipien gelten grundsätzlich auch für diesen Themenschwerpunkt. Daher werden gewisse Punkte und weiterführende Prozesse wie z. B. Software Updates und Security Patches nicht mehr besprochen und behandelt. Es möchte eine gewisse Doppelspurigkeit vermieden werden resp. sie kleinstmöglich zu halten und konzentrieren uns hier nur noch um Massnahmen, die nicht von allgemeiner Bedeutung sind und noch nicht exakt in diesem Sinne kontrolliert wurden. Es empfiehlt sich also meistens die Kontrolle des OS-Hardening vorzuziehen und darauffolgend mit den zusätzlichen Checks für die Container fortzufahren. Nur mit beiden Berichten (Testreports) zusammen, welche übrigens auch auf der beiliegenden CD-ROM eingesehen werden können, erlangt man eine Gesamtsicht resp. Wertung über das Router-Hardening. Nach dem bekannten Schema, konzentrieren wir uns und dokumentieren nun wieder die besonders erwähnenswerten Kontrollen und die nachzuholenden Hardening-Konfigurationen. Auch sie wurden von den umfangreichen Testfällen abgeleitet. Direkt darauffolgend an die Testüberschrift folgt ein Vermerk SCORED oder NOT_SCORED. Mit dieser Kennzeichnung möchte ich die Wichtigkeit der Empfehlung besonders hervorheben und bei der Gesamtbewertung entsprechend berücksichtigen.

6.4.1. File System [FILE]

FILE-10111 - Separate Container Partitions SCORED

Wie unter dem Thema „Appliance Hardening“ bereits besprochen, müssen wir auch bei Container Security sorgetragen, dass die Docker-Daten nicht das unterliegende Betriebssystem beeinflussen oder sogar unbrauchbar machen könnten. Eine Überwachung und Alarmierung des Partitionsspeicherplatzes gehören

selbstverständlich als Ergänzung dazu. Während der Prüfung wurde festgestellt, dass die Docker bezogenen Daten nicht auf einer separaten Partition abgelegt sind. Daher möchte diese Empfehlung in den nächsten Releases berücksichtigt werden.

FILE-10112 - Control Docker Daemon SCORED

Mit der Berechtigung den Docker-Daemon zu steuern, könnte ein potenzieller Angreifer über einen gestarteten Container erhöhte Privilegien erlangen und die Kontrolle über den SCION-Router übernehmen. Daher ist es essenziell die Teilnehmer der Docker-Gruppenberechtigung wiederkehrend zu überprüfen oder zu überwachen. Auf unserem System besitzen nur SCION-Router-Admins die entsprechende Berechtigung und daher besteht kein Handlungsbedarf.

6.4.2. Enable Docker Auditing [ENDA]

ENDA-10211 - Auditing Docker Daemon SCORED

Zusätzlich zur Überwachung des Router-Betriebssystems muss die Docker-Umgebung auch hinzugenommen und berücksichtigt werden. Bekanntlich wird der Docker-Daemon mit Root-Rechten ausgeführt und sein Verhalten hängt von einigen Dateien und Verzeichnissen ab. Auch auf diese Audit-Informationen ist das Incident Response und Forensics Team angewiesen, um entsprechend und angemessen zu reagieren oder zu agieren. Auf dem untersuchten SCION-Router wurde kein aktives Docker-Audit-Logging festgestellt und daher wird dringend empfohlen, eine angemessene Konfiguration zu aktivieren. Das Audit-Logging kann je nach Einstellungen sehr ressourcenintensiv ausfallen und daher benötigt es auch hier nach der Bestimmung der Konfiguration gewisse Acceptance Tests in der Testumgebung.

6.4.3. Secure Docker Daemon [SDOD]

SDOD-10311 - Restricted traffic on the default network bridge SCORED

Die Container-Instanzen auf einem Host können standardmässig uneingeschränkt miteinander kommunizieren. Auf dem SCION-Router findet die Netzwerkkommunikation über den Host-Driver statt und die Bridge-Schnittstelle ist keiner Instanz zugewiesen. Um zukünftige Schwachstellen zu vermeiden, wird empfohlen die Inter-Container-Communication (ICC) per se zu verbieten und zukünftig, falls notwendig über benutzerdefinierte Netzwerkschnittstellen zu realisieren.

SDOD-10313 - Allow Docker to change Iptables NOT SCORED

Die Iptables werden bekanntlich zur IP-Paketfilter-Regelung im Linux-Kernel verwendet. Der Docker-Daemon sollte Änderungen an der Tabelle selbst vornehmen dürfen. Per Default erleichtert die automatisierte Konfiguration die Administration und verhindert unerwünschte Einflüsse durch etwaige Fehlkonfigurationen an der Iptable durch SCION-Admins. Der Docker-Daemon benötigt, bevor er startet, gewisse Regeln. Bei der Untersuchung wurde festgestellt, dass der Dockerd keine Änderungsberechtigungen dafür besitzt. Wie in den vorangegangenen Untersuchungen unter dem Kapitel „Empfehlungen zur Systemhärtung“ festgestellt, wird fälschlicherweise in den Default-Policies der Chains „INPUT“, „FORWARD“ und „OUTPUT“ jeglichen Datenverkehr für alle Protokolle und Service-Ports erlaubt. Aus diesem Grund stellt diese Konfiguration auch kein Problem dar. Das bevorzugte Standard-Docker-Verhalten wurde also in der Docker-Konfiguration ausgeschaltet. In den meisten Fällen ist es jedoch sinnvoll, die Standardeinstellung zu belassen, da Docker zwei eigene Iptable-Chains „DOCKER“ und „DOCKER-USER“ priorisiert vor die Host-basierten Iptables setzt. Die Chain „DOCKER“ wird von Docker selbst gesteuert und darf nicht verändert werden. Das benutzerspezifische Regelwerk muss gemäss den internen Weisungen, sehr leicht mit der Chain „DOCKER-USER“ übersteuert und definiert werden können. Da die Docker-Container-Router

lediglich von der Forwarding-Chain abhängig sind, muss unbedingt darauf geachtet werden, dass wir keinen reinen IP-Verkehr über unseren SCION-Router erlauben und weiterleiten.

SDOD-103xx - General Restriction of SCION related traffic using Iptables SCORED

Im SCION-Umfeld nutzen wir bekanntlich den Ansatz des geteilten Netzwerk-Namespaces (Host Mode) mit dem Host-System, wodurch eine höhere Leistung „Near Metal Speed“ erzielt wird und NAT nicht mehr erforderlich ist. Alle bereitgestellten SCION-Services werden direkt auf den Host-Netzwerkschnittstellen zur Verfügung gestellt und sollten nur auf die relevanten Schnittstellen hören. Wenn immer möglich, müssen die Service-Listener eingeschränkt sein und dürfen nicht auf die Wildcard-IP-Adresse „0.0.0.0“ hören. Dies ist teilweise aus technischen Gründen nicht realisierbar, daher sollte zumindest die eingehende Kommunikation auf die notwendigen Schnittstellen und/oder Netzwerken beschränkt werden. Aufgrund der vorgefundenen ungenügenden Restriktionen, können sie nachfolgend eine Iptable als Vorlage einsehen. Sie soll die grundlegende Idee aufzeigen und den Angriffsvektor massgeblich verkleinern. Auf dem vorliegenden SCION-Image bestanden keine IPv6-Limitierungen und daher liegt der Fokus vorerst auf IPv4. Diese müssen fortan unbedingt miteinbezogen und mit dem selben Masse eingeschränkt werden. Die Iptable enthält Platzhalter in eckigen Klammern und kundenspezifische IP-Adressen, die in Abhängigkeit des Kundendesigns angepasst oder erweitert werden müssen. Sie wurde einfachheitshalber relativ generisch gehalten und zudem sprechen wir hier von einem Router und nicht von einer Firewall. Vor dem produktiven Einsatz bedarf sie einer gründlichen Verifikation, da sie keinesfalls als abschliessend und verifiziert angesehen werden darf. Des Weiteren bedarf sie bei SCION-Funktionserweiterungen eine Überarbeitung. Vorerst muss eine manuelle Überprüfung stattfinden. Künftig soll eine zusätzliche und kundenspezifische Kontrolle für eine automatisierte und wiederkehrende Prüfung entstehen.

```

1  # iptables -S

3  # [DEFAULT] Deny Firewall Policy
4  -P INPUT DROP
5  -P FORWARD DROP
6  -P OUTPUT DROP

8  # [USER-CUSTOM] Defined Firewall Chains
9  -N DOCKER-USER
10 -N custsshps
11 -N ssfninfraips
12 -N admin-services
13 -N ssfn-internal-services
14 -N ssfn-external-services

16 # [LOOPBACK] Traffic Firewall Policy
17 -A INPUT -i lo -j ACCEPT
18 -A INPUT -s 127.0.0.0/8 -j DROP
19 -A OUTPUT -o lo -j ACCEPT

21 # [ESTABLISHED] Connections Firewall Policy
22 -A INPUT -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
23 -A FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
24 -A OUTPUT -m conntrack --ctstate NEW,RELATED,ESTABLISHED -j ACCEPT

26 # [PREDEFINED] Firewall Chains
27 -A INPUT -i [INTERNAL_IF] -p icmp -j custsshps
28 -A INPUT -i [INTERNAL_IF] -j admin-services

```

```

29 -A INPUT -i [INTERNAL_IF] -j ssfn-internal-services
30 -A INPUT -i [EXTERNAL_IF] -p icmp -j ssfninfraips
31 -A INPUT -i [EXTERNAL_IF] -j ssfn-external-services
32 -A FORWARD -j DOCKER-USER
33 -A DOCKER-USER -i [SIG] -o [INTERNAL_IF] -j ACCEPT
34 -A DOCKER-USER -i [INTERNAL_IF] -o [SIG] -j ACCEPT
35 -A DOCKER-USER -j RETURN
36 -A OUTPUT -o [INTERNAL_IF] -j custsshships
37 -A OUTPUT -o [EXTERNAL_IF] -j ssfninfraips

39 # [SOURCE-NETWORKS/SERVICES] Firewall Object Definition
40 -A custsshships -s 10.0.0.0/8 -j ACCEPT
41 -A ssfninfraips -s [SCION_IP/MASK ] -j ACCEPT
42 -A admin-services -s 10.123.20.0/22 -p tcp -m tcp --dport 22 -j ACCEPT
43 -A admin-services -s 10.123.148.0/22 -p tcp -m tcp --dport 22 -j ACCEPT
44 -A ssfn-internal-services -p tcp -m tcp --dport 179 -j ACCEPT
45 -A ssfn-internal-services -p udp -m udp --dport 3784 -j ACCEPT
46 -A ssfn-internal-services -p udp -m udp --dport 3785 -j ACCEPT
47 -A ssfn-internal-services -p tcp -m tcp --dport 30441 -j ACCEPT
48 -A ssfn-internal-services -p tcp -m tcp --dport 30442 -j ACCEPT
49 -A ssfn-internal-services -p tcp -m tcp --dport 30452 -j ACCEPT
50 -A ssfn-internal-services -p tcp -m tcp --dport 30455 -j ACCEPT
51 -A ssfn-internal-services -p tcp -m tcp --dport 30456 -j ACCEPT
52 -A ssfn-internal-services -p tcp -m tcp --dport 31256 -j ACCEPT
53 -A ssfn-internal-services -p tcp -m tcp --dport 32256 -j ACCEPT
54 -A ssfn-internal-services -p udp -m udp --dport 30041 -j ACCEPT
55 -A ssfn-internal-services -p udp -m udp --dport 30042 -j ACCEPT
56 -A ssfn-external-services -p udp -m udp --dport 3784 -j ACCEPT
57 -A ssfn-external-services -p udp -m udp --dport 3785 -j ACCEPT
58 -A ssfn-external-services -p udp -m udp --dport 30042 -j ACCEPT

```

Listing 6.1: General Restriction of SCION related traffic using Iptables

An dieser Stelle möchte nochmals erwähnt werden, dass der direkte Zugang zum Internet oder jegliche Kommunikation zu externen Quellen grundsätzlich untersagt ist. Sollten Zugriffe auf bestimmte Internet-Webserver/Websites erforderlich sein, muss dieser in einem genehmigten Sicherheitskonzept dokumentiert werden. Ausführliche Informationen zu Netzwerkzonen und/oder zur Kommunikation finden sie im SIX-Dokument „Network Security Masterplan (NSM)[41]“.

SDOD-10314 - Docker Private Registry NOT SCORED

Lokal auf dem SCION-Host können Kopien unter dem Verzeichnis „/etc/docker/certs.d/<registry-name>/“ von vertrauenswürdigen Registry-CA-Zertifikaten abgelegt werden. Eine sichere Registrierung verwendet TLS. Eine unsichere Registrierung besitzt kein gültiges Zertifikat oder verwendet kein TLS. Normalerweise sollten keine unsicheren Register verwendet werden, da sie das Risiko des Abfangens und der Änderung des Verkehrs darstellen. Des weiteren kommt, dass unsichere Befehle wie Docker Pull, Docker Push und Docker-Search keine Fehlermeldungen anzeigen. In unserem Fall besteht kein potenzielles Risiko mit der Private Docker Registry¹¹, da wir vertrauenswürdige Quellen haben und es künftig einen geordneten und gehärteten Supply Chain geben wird. Bei der Untersuchung wurden nur die Lokalen „Insecure Registries: [127.0.0.0/8]“ als unsicher erkannt und die stellen für uns kein Sicherheitsproblem dar.

¹¹Viele Anbieter bieten ein öffentliches und privates Docker-Registrierungshosting für die ultraschnelle und sichere Auslieferung der Docker-Container-Images an. Anapaya Systems AG setzt auf die sichere, vollwertige und auf das Cloud-Native-Docker-Management von Cloudsmith.

SDOD-103xx - TLS Authentication for Dockerd NOT_SCORED

Müsste der Docker-Daemon künftig aus irgendwelchen Gründen unbedingt von ausserhalb erreichbar sein, so muss der Zugriff über Iptables und mittels TLS-Authentifizierung limitiert und geschützt werden. Diese Art der Konfiguration beschränkt und sichert die Verbindungen zum Dockerd über das Netzwerk auf eine begrenzte Anzahl von Admin-Clients. Solche Verbindungen sollten auch künftig, wenn immer möglich nicht angeboten werden.

SDOD-10316 - User Namespace Support SCORED

Der Linux-Kernel unterstützt die Funktion „User Namespace“ zur Verbesserung der Sicherheit, indem die Benutzer- und Gruppen-IDs vom Host und Container separiert werden. Der Benutzernamensraum definiert also einen eindeutigen Bereich von Benutzer- und Gruppen-IDs, die ein Prozess resp. ein Container ausserhalb des vom SCION-Host-System verwenden. Dadurch werden die Systemzugriffe durch eine Art von Nachahmung automatisch limitiert. Diese Empfehlung ist vor allem nützlich, wenn das verwendete Container-Image den Root- oder einen vordefinierten Benutzer mit Root-Rechten hat. Gewisse SCION-Services laufen nunmal unter dem Benutzer „scion“, der mit Superuser-Rechten ausgestattet ist. Er ist der Gruppen „adm“ und „sudo“ angehörig, die die höchsten Privilegien geniessen. Die IP-Routing-Services (Quagga BGPD) laufen unter „root/scion“ und die Monitoring-Services starten vorbildlich unter nicht-privilegierten Benutzern „prometheus“, „sigonly“ und „nobody“. Die User-Namespaces-Funktion ist leider noch nicht ausgereift und kann zu unvorhersehbaren Problemen oder Konfigurationsschwierigkeiten führen. Darum müssen vorab die Limitierungen geprüft werden. Aufgrund der Tatsache, dass Privilege Escalation eine sehr beliebte Angriffsmethode ist, wird bei Nichtumsetzbarkeit eine andere Methode anstelle vom User Namespace empfohlen. Überlegenswert kann beispielsweise sein, wenn künftig dem Container-Benutzer „scion“ nur noch strikt limitierte Sudo-Berechtigungen, ganz nach dem Prinzip „Least Privilege“, gewährt werden.

SDOD-103xx - Authorization of Docker Client Commands NOT_SCORED

Jeder Benutzer, der die Zugriffsberechtigung auf den Docker-Daemon hat, kann einen beliebigen Docker-Clientbefehl ausführen. Wird eine bessere Zugriffskontrolle benötigt, kann dies mittels eines Autorisierungs-Plugins¹² und der entsprechenden Docker-Daemon-Konfiguration erreicht werden. Mithilfe eines Autorisierungs-Plugins kann ein Docker-Administrator detaillierte Zugriffsrichtlinien für die Verwaltung des Zugriffs auf dem Docker-Daemon konfigurieren. In unserem Fall, ist diese Massnahme eher von optionaler Bedeutung, da nur eine sehr eingeschränkte Anzahl von SCION-Administratoren einen überwachten Zugriff geniessen.

SDOD-10319 - Centralized and Remote Logging SCORED

Auch für die SCION-Services muss ein Protokollierungsdienst konfiguriert und aktiv sein. Damit die Logintegrität sichergestellt ist und die Logs gegebenenfalls weiter ausgewertet und alarmiert werden können, müssen die Logging-Informationen auf ein Remote-System z. B. Splunk und/oder Qradar weitergeleitet werden. Die Log-Weiterleitung ist eine interne sowie eine regulatorische Anforderung. Docker stellt verschiedene Logging-Methoden zur Verfügung. Für SCION haben wir uns für den Journal-Daemon entschieden und das Journal wird systemintern an den Rsyslog-Daemon weitergeleitet. Eine direkte Übergabe an den Syslog-Daemon wäre auch möglich. Das ist eine Frage des Designs und möchte hier nicht beantwortet werden. Somit ist sichergestellt, dass auch diese Logs auf einem unabhängigen System geschützt und gemäss den geforderten Anforderungen¹³ entsprechend aufbewahrt werden. Die Grundvoraussetzung ist natürlich, dass der SCION-Router bereits die Logs via Syslog weiterleitet. Diese Überprüfung fand bereits im OS-

¹²Twistlock AuthZ Broker: <https://github.com/twistlock/authz>

¹³Das interne Dokument „SIX Logging Standard“ definiert den allgemeinen Umgang, die Prinzipien und Anforderungen aller Log-Informationen. Zusätzlich werden die Rollen und Zuständigkeiten auf den Quell- und Ziel-Systemen geregelt.

Hardening statt. Die Erkennung von Log-Unterbrüchen muss unabhängig und auf dem Log-Receiver selbst überwacht und sichergestellt werden.

SDOD-10320 - Daemon-less Containers SCORED

Docker bietet eine Funktion „Live-Restore“ an, die einerseits die Verfügbarkeit der SCION-Services verbessert und andererseits die System-Administration bei Wartungsarbeiten vereinfacht. SCION sorgt und steht bekanntlich auch für Reliability und Availability. Daher wird diese Funktion empfohlen und sollte auch genutzt werden. Kommt der Docker-Daemon einmal zum Erliegen, dann sind automatisch auch alle SCION-Services nicht mehr erhältlich. Spätestens im nächsten Release sollte diese Funktion, wenn möglich aktiv sein.

SDOD-10321 - Experimental Features SCORED

Experimentelle Funktionen dürfen auf einem produktiven SCION-Router nicht aktiv sein. Soweit bekannt existieren auch keine derartige Funktionen. Auch in „stabilen“ Versionen sind solche Funktionen oft unvollständig getestet und garantieren keine API-Stabilität. Wenn möglich sollten aufgrund der Systemstabilität auf den Einsatz von experimentellen Funktionen z. B. Ipvlan¹⁴ verzichtet werden.

SDOD-10322 - Acquiring new privileges SCORED

Standardmässig sind die Container während der Laufzeit immer wieder dazu in der Lage zusätzliche Berechtigungen über „setuid“ oder „setgid“ einzufordern. Ein Prozess kann das no_new_priv-Bit im Kernel setzen. Das Bit bleibt über sogenannte Forks, Clones and Execve hinweg bestehen. Der Prozess und seine untergeordneten Child-Prozesse kriegen also keine zusätzlichen Berechtigungen mehr über suid- oder sgid-Bits. Um die Sicherheitsrisiken für einen Ausbruch aus einem Container, durch untergraben von privilegierten Binärdateien zu verringern, empfiehlt es die Berechtigungen stark einzuschränken. Bei den Untersuchungen wurde festgestellt, dass nicht alle Linux Kernel Capabilities per se freigeschaltet sind. Jedoch haben die Container keine Security Option gesetzt und daher verfügen sie über die vielen standardmässigen Capabilities. Die SCION-Anwendungen sind somit in der Lage, privilegierte Aktionen auf einem Host resp. der SCION-Appliance auszuführen. Es wird nochmals empfohlen das Berechtigungskonzept der Container zu hinterfragen und gegebenenfalls anzupassen. Einige Funktionen sind aus Sicherheitsgründen von hohem Belangen, da sie im Zusammenhang mit Container als gefährlich¹⁵ eingestuft werden.

```

1 # docker ps --quiet --all | xargs docker inspect --format '{{{ .Name }}}: SecurityOpt={{{ .HostConfig.SecurityOpt }}}
2 Capabilities={{{ .HostConfig.Capabilities }}} {{{ .HostConfig.CapAdd }}} {{{ .HostConfig.CapDrop }}}}'

4 /anapaya-confagent: SecurityOpt=[] Capabilities=[] [] []
5 /anapaya-posix-gateway: SecurityOpt=[] Capabilities=[] [NET_ADMIN] []
6 /anapaya-cs70-9025-2: SecurityOpt=[] Capabilities=[] [] []
7 /anapaya-sd70-9025: SecurityOpt=[] Capabilities=[] [] []
8 /anapaya-br70-9025-2: SecurityOpt=[] Capabilities=[] [] []
9 /anapaya-dispatcher: SecurityOpt=[] Capabilities=[] [] []
10 /blackbox-exporter-sigonly: SecurityOpt=[] Capabilities=[] [net_raw] [ALL]
11 /blackbox-exporter: SecurityOpt=[] Capabilities=[] [net_raw] [ALL]
12 /node-exporter: SecurityOpt=[] Capabilities=[] [] [ALL]
13 /anapaya-quagga-bgpdp: SecurityOpt=[] Capabilities=[] [SETUID SETGID NET_ADMIN SYS_ADMIN NET_BROADCAST] []
14 /anapaya-quagga-zebra: SecurityOpt=[] Capabilities=[] [SETUID SETGID NET_ADMIN SYS_ADMIN NET_BROADCAST] []

```

Listing 6.2: Security Options and Capabilities of Containers

¹⁴<https://github.com/docker/docker-ce/blob/master/components/cli/experimental/vlan-networks.md>

¹⁵<https://raesene.github.io/blog/2017/08/27/Linux-capabilities-and-when-to-drop-all>

6.4.4. Protect Docker Daemon Configuration [PDOD]

PDOD-10411-12 - Ownership and Permissions of Docker Daemon configuration files SCORED

Für das sichere und korrekte Funktionieren vom Docker-Daemon ist es wichtig, die Docker-bezogenen Dateien, sowie Verzeichnisse entsprechend zu schützen. Gewisse Dateien wie z. B. `docker.service` und `docker.socket` können vertrauliche Parameter enthalten, die das Verhalten des Docker-Daemons beeinflussen. Daher muss sichergestellt sein, dass die Eigentümer und Benutzer mit ihren Berechtigungen korrekt gesetzt sind. Nur privilegierte Admin dürfen in der Lage sein, die notwendigen Konfigurationen vornehmen zu dürfen. Es muss verhindert werden, dass nicht privilegierte Benutzer, wie potenzielle Angreifer, das Verhalten von Docker beeinflussen können. Auf dem SCION-Router sind die Daten entsprechend geschützt.

PDOD-10413-14 - Ownership and Permissions of Docker Daemon sensitive files SCORED

Das Docker-Verzeichnis `„/etc/docker/“` beinhaltet weitere sensitive Informationen wie die Docker-Daemon-Konfiguration `„daemon.json“` und falls benötigt, kommen die Zertifikate und Schlüssel bezüglich Registries dazu. In unserem Fall werden keine Repository-Zertifikate benötigt und daher fehlen gewisse darunterliegende Verzeichnisse. Eine Überprüfung wird aus Vollständigkeitszwecken und zum Schutz der Konfiguration trotzdem empfohlen.

PDOD-10415 - Docker Server and SCION certificates and configuration files SCORED

Zertifikate und Konfigurationen sind meistens sehr schützenswert, da sie teilweise sensitive Informationen enthalten und andererseits unbedingt vor Manipulationen und des Missbrauchs geschützt werden müssen. Im SCION-Umfeld hatten wir einleitend erfahren, dass wir auf einem SCION-Router von vielen Container-Konfigurationen, Zertifikaten und Schlüsselmateriale abhängig sind. Das Hauptverzeichnis `„/etc/scion/“` gehört vermutlich zum wichtigsten SCION-Verzeichnis. Eine Überprüfung und Durchsetzung der minimalen und korrekten Berechtigungen sind nicht wegzudenken. Bei der Verifikation wurde festgestellt, dass die Control-Plane-Keys wie der AS-Private- und die Master-Keys richtig geschützt sind. Die SCION-Verzeichnisse und -Konfigurationen wie die Trust Root Configuration (`*.trc`) und SCION-Service-Spezifikationen (`*.json` und `*.toml`) scheinen noch besser geschützt werden zu können. Oft sind die Verzeichnisse und Konfigurationen aller Benutzer einsehbar. Um den SCION-Router noch besser zu schützen, empfiehlt sich daher die Verzeichnis- und Dateiberechtigungen zu überdenken.

PDOD-10416 - Docker Socket and Compose permissions SCORED

Der Docker-Daemon wird als Root ausgeführt und die Standard-Unix-Sockets¹⁶ gehören demnach dem Root-Benutzer. Um unprivilegierten Benutzern oder Prozessen die Interaktion mit dem Docker-Daemon resp. den Containern zu verbieten, müssen die Berechtigungen entsprechend dem Standard gesetzt sein. Es wird empfohlen die Standard-Gruppe `„docker“` beizubehalten. Alle an der Gruppe angehörenden Benutzer, könnten in der Lage sein, mit den Containern zu interagieren. In unserer SCION-Umgebung kommt zur Vereinfachung und Automation das Tool `„Docker Compose“` hinzu. Compose definiert und führt mehrere SCION-Anwendungen in mehreren Containern gleichzeitig aus. Die Services werden gemeinsam in einer oder mehreren YAML-Dateien `„docker-compose.yml“` konfiguriert. Damit nicht alle Benutzer auf dem SCION-Router die Services über Compose steuern oder beeinflussen können, müssen wir auch hier für eine konforme Berechtigung besorgt sein. Daher ist die Empfehlung auch für Docker Compose die Berechtigung etwas mehr einzuschränken.

PDOD-10417 - Docker and SCION configuration permissions SCORED

Unter dem vorangegangenen Kontrollpunkt wurden die Abhängigkeiten der SCION-Services etwas ange-

¹⁶Ein Socket ist eine spezielle Datei für die Kommunikation zwischen Prozessen, die die Kommunikation zwischen zwei Prozessen ermöglicht. Zusätzlich zum Senden von Daten können Prozesse mithilfe der Systemaufrufe über die Dateideskriptoren `„sendmsg()“` und `„recvmsg()“` eine Unix-Domain-Socket-Verbindung senden.

deutet. Wie bekannt, ist der SCION-Router aka SIG noch von weiteren Drittanbieterservices abhängig. Der Übergang von SCION auf das legacy IP-Netzwerk erfolgt beispielsweise über einen BGP-Router¹⁷ (Quagga BGPD). Die interne Paketübergabe erfolgt über einen universellen Netzwerktreiber¹⁸. Der Treiber erstellt virtuelle Netzwerkschnittstellen für den Paketaustausch zwischen unseren Prozessen dem SIG und BGP-IP-Router. Nebst den Docker- und SCION-Anwendungen müssen natürlich auch diese Komponenten dementsprechend gesichert sein. Dazu kommt jegliche mit SCION verbundenen Konfigurationen, sind als vertraulich und problematisch bezüglich Cyber Angriffen anzusehen. Die Docker-Daemon- und Docker-Compose-Konfigurationsdateien¹⁹ und Verzeichnisse sind optimal berechtigt. Die BGP-Router-Konfigurationen scheinen auch genügend von Zugriffen unberechtigter Benutzer geschützt zu sein, aber zum Beitrag der einheitlichen Sicherheitskonfiguration möchte das Verzeichnis „/etc/quagga/“ noch bezüglich der weltweiten Leseberechtigung zurückgestuft werden.

6.4.5. Secure Container Runtime Configuration [SCRC]

SCRC-10511 - Kernel Security Modules are enabled SCORED

AppArmor ist ein Mandatory Access Control System (MAC) und schützt wie schon erfahren das Linux-Betriebssystem und die Anwendungen vor verschiedenen Bedrohungen, indem eine Sicherheitsrichtlinie mittels eines AppArmor-Profiles durchgesetzt wird. Die SCION-Container können auch mittels AppArmor^{20,21} geschützt werden. Es ist möglich, ein eigenes Profil gemäss den firmeninternen Sicherheitsrichtlinien zu definieren oder wie in unserem Fall das Standard-AppArmor-Profil für Docker anzuziehen und zu verwenden. Dieser Präventivschutz soll Anwendungen vor noch nicht öffentlich bekannten Sicherheitslöchern (Zero-Day-Exploits) schützen. Am schützenswertesten sind vor allem Programme, die mit dem Netzwerk verbunden sind, da sie die wahrscheinlichsten Ziele von entfernten Angreifern sein können. Das vordefinierte Profil ist sehr allgemein gehalten und eher weniger restriktiv, damit es für die meisten Anwendungen ohne Einschränkungen passt. Um die SCION-Appliance noch sicherer zu gestalten, empfiehlt es sich künftig ein eigenes SCION-spezifisches AppArmor-Profil zu kreieren.

Ein weiteres Kernel-Sicherheitsmodul bekannt unter Secure Computing Mode oder abgekürzt als Seccomp^{22,23}, ist eine weitere Linux-Kernelfunktion, die verschiedene Sicherheitsfunktionen in einer Docker-Umgebung einbringt. Die Erweiterung soll also noch mehr Sicherheit im Umgang mit Containern bringen. Es ähnelt einer Sandbox-Umgebung (isolierter Bereich), die nicht nur als Firewall für Systemaufrufe (Syscalls) fungiert, sondern es auch ermöglicht, die in den Docker-Containern verfügbaren Aktionen auf den Linux-Kernel des Hosts zu beschränken. Docker selbst baut ständig die unterstützten Systemaufrufe aus und mittlerweile werden von über 300 Systemaufrufen etwa 51 signifikante Systemaufrufe standardmässig blockiert. Der Grund dafür ist, weil sie schlichtweg nicht in der sogenannten Whitelist stehen. Das Standard-Seccomp-Profil ist demnach als sogenannte Whitelist anzusehen, in der die zulässigen Systemaufrufe angegeben sind. Besteht Bedarf, um das Default-Profil²⁴ kundenspezifisch anzupassen, so kann es

¹⁷Der hostbasierte BGP-Routing-Service wurde mittlerweile virtualisiert und durch einen Container ersetzt.

¹⁸TUN/TAP stellt den Paketempfang und die Paketübertragung für User-Space-Programme bereit. Es kann als einfaches internes Punkt-zu-Punkt- oder als Ethernet-Schnittstelle angesehen werden, das anstatt Pakete von physischen Medien empfängt. Um den Treiber verwenden zu können, muss ein Programm die Komponente „/dev/net/tun“ öffnen und ein entsprechendes ioctl() ausgeben, um ein Netzwerkgerät beim Kernel zu registrieren. Ein Netzwerkgerät wird anhand der ausgewählten Optionen als „tunXX“ oder „tapXX“ angezeigt. Wenn das Programm den Dateideskriptor schliesst, verschwindet das Netzwerkgerät und alle entsprechenden Routen.

¹⁹Die JSON-Datei „/etc/docker/daemon.json“ definiert die globale Docker-Daemon-Konfiguration, welche in unserem Fall wegen Docker Compose nur minimal in Anspruch genommen wird. Durch die YAML-Dateien in den Verzeichnissen „/etc/docker-compose/*/docker-compose.yml“ definieren wir die SCION-Container-Konfigurationen.

²⁰<https://cloud.google.com/container-optimized-os/docs/how-to/secure-apparmor>

²¹<https://appfleet.com/blog/advanced-docker-security-with-apparmor/>

²²<https://appfleet.com/blog/hardening-docker-container/>

²³<https://docs.docker.com/engine/security/seccomp/>

²⁴<https://github.com/moby/moby/blob/master/profiles/seccomp/default.json>

mittels eigener Profile übersteuert werden. Das Default-Profil bietet eine breite Anwendungskompatibilität und daher wird von einer Aufweichung grundsätzlich abgeraten. Der vorliegende SCION-Router unterstützt grundsätzlich die Kernel-Sicherheitsfunktion und eine Ausschaltung (`-security-opt seccomp=unconfined` / `-privileged=true`) konnte bei der Untersuchung nicht festgestellt werden. Der Kernel genießt demnach den zusätzlichen Schutz durch Seccomp.

```
1 grep SECCOMP /boot/config-$(uname -r)
2 CONFIG_SECCOMP=y
3 CONFIG_HAVE_ARCH_SECCOMP_FILTER=y
4 CONFIG_SECCOMP_FILTER=y
```

Listing 6.3: Protect host system against insecure containers with Seccomp

SCRC-10512 - SSHD within a container is prohibited SCORED

Die Komplexität muss immer so einfach wie möglich gehalten werden, daher muss sichergestellt sein, dass das Remote-Verbinden direkt in einen Container z. B. mittels SSH nicht gestattet ist. Möchten Abfragen in einem Container gemacht werden, soll es ausschliesslich über den Befehl „`docker exec`“ erfolgen. Das Security Management würde zusätzlich massiv erschwert werden, denn die Zugriffsbeschränkungen, Passwörter, Schlüsselmaterialien und Updates/Patches müssten für die Container zusätzlich gemanagt werden. Fehlkonfigurationen und Sicherheitsrichtlinienverletzungen wären vorprogrammiert. Es sind nur applikatorische Zugriffe zugelassen und erwünscht!

SCRC-10513 - System ressource consumptions SCORED

Die Container nutzen wie alle anderen Applikationen auf dem System dieselben Ressourcen. Mit den vorangegangenen Kontrollen, haben wir unter anderem, den persistenten Speicher geschützt und begrenzt. Auch die dynamischen CPU- und Memory-Ressourcen müssen kontrolliert und limitiert werden. Standardmässig sind alle Container gleichberechtigt und könnten den zur Verfügung stehenden Arbeitsspeicher und/oder die Prozessorzeit grundsätzlich komplett für sich beanspruchen. Wir müssen einen Denial-of-Service bezüglich CPU und Memory unbedingt verhindern und die weitere Funktion anderer Anwendungen und des Systems sicherstellen. Um die Systemstabilität auch bei einem Memory Leak zu bewahren, empfiehlt es sich künftig den SCION-Services nur den notwendigen Speicherbedarf zuzuweisen. Ähnlich sieht es bei der Prozessorlaufzeit aus. Über die Container-Priorisierung verhindern wir, dass Container mit niedriger Priorität fälschlicherweise die CPU-Ressourcen absorbieren, die möglicherweise von anderen SCION-Prozessen benötigt werden. Momentan findet keine adäquate CPU-Priorisierung statt. Die Festlegung der CPU-Prioritäten erscheint nicht nur für die SCION-Services ein grosses Unterfangen zu sein. Dennoch empfiehlt es sich künftig ein Soft-Limit²⁵ für die SCION-Services konzeptionell auszuarbeiten und einzuführen.

SCRC-10514 - Principle of immutable infrastructure NOT SCORED

Durch Aktivieren der Root-Filesystem-Option „`-read-only [ReadonlyRootfs=true]`“ werden Container zur Laufzeit gezwungen, ihre Datenschreibstrategie explizit zu definieren. Wie in unserem Fall werden die benötigten Daten grundsätzlich vom Host-System mit den benötigten Berechtigungen in den Container gebunden. Das Container-Root-Dateisystem sollte als Golden-Image angesehen werden und daher nicht veränderbar sein. Dies reduziert direkt die Container-Angriffsvektoren, da das Dateisystem der Containerinstanz nur manipuliert oder beschrieben werden kann, wenn es explizite Lese-/Schreibberechtigungen für seinen Dateisystemordner und seine Verzeichnisse hat. Es gibt jedoch Gründe solche Schreibzugriffe

²⁵Das CPU-Share wird nur erzwungen, wenn die CPU-Zyklen eingeschränkt sind. Solange genügend CPU-Zyklen verfügbar sind, können alle Container so viel CPU verbrauchen, wie sie benötigen. Auf diese Weise wird kein bestimmter CPU-Zugriff garantiert oder reserviert.

trotzdem zu gewähren. Wir bei der SIX müssen teilweise Schreibzugriff auf das Root-Dateisystem haben, um ein laufendes Produktionssystem vorübergehend reparieren zu können. Die permanente Korrektur wird dann ordnungsgemäss zu dem Container hinzugefügt, der in der nächsten Version bereitgestellt werden soll. Bei den Überprüfungen des SCION-Routers wurde festgestellt, dass kein Schreibschutz für das Root-Dateisystem aktiv ist und daher wird empfohlen dies nochmals zu hinterfragen.

SCRC-10515 - SCION container restart policy SCORED

Damit ein SIG ordnungsgemäss funktioniert, müssen einige Core-Router-Services in der korrekten Reihenfolge starten, da gewisse SCION-Services direkt voneinander abhängig sind. Bei den Untersuchungen wurde festgestellt, dass die SCION-Services z. B. bei einem Fehler, laufend und ohne Obergrenze neu starten. Laufend wiederstartende Prozesse können vor allem in einer Multi-Container-Umgebung, wie wir es auf unserem SCION-Router vorfinden, leicht zu einer Denial-of-Service führen. Es empfiehlt sich, einerseits die SCION-Services zu überwachen und bei Bedarf zu alarmieren, damit die Fehleranalyse und -behebung schnellst möglich stattfindet. Als weitere Massnahme sollte sich eine Limite der Anzahl maximalen Neustarts überlegt und eingeführt werden. In der SIX-Umgebung legen wir keine allgemeingültige Zahl fest, denn je nach Anwendungsfall kann die maximale Anzahl zulässiger Wiederholungsversuche variieren.

SCRC-10516-20/23 - SCION container isolation SCORED

Wie wir gesehen haben, sind die SCION-Services vom Host-Linux-Kernel abhängig und nicht vollumfänglich voneinander isoliert. Docker verwendet für die Separierung resp. den Schutz zwischen dem Host und den Container sogenannte Kernel-Namespaces. Beim Start eines Containers erstellt Docker mehrere sogenannte Isolationsschichten. Jeder Aspekt eines Containers wird in einem separaten Namespace ausgeführt und beschränkt seinen Zugriff auf diesen Bereich. Bei keiner durchgängigen und sicheren Konfiguration der Abtrennungsmechanismen wird einem Angreifer potentiell ermöglicht, gewisse Systeminformationen zu gewinnen oder auf das Host-Betriebssystem zu zugreifen und zu kompromittieren. Wir sprechen hier von den Namespaces:

- * Der **PID-Namespace** isoliert die Host- und Container-Prozesse auf Prozessebene untereinander. Gleiche Prozess-IDs stellen keine Risiken oder Probleme dar, da sie keinen Zusammenhang untereinander haben und sich nicht sehen und demnach nicht beeinflussen können.
- * Der **NET-Namespace** isoliert gleichermassen die Netzwerkschnittstellen zwischen dem Host- und den Containern. Jeder Container sollte auf seiner eigenen logische Netzwerkschnittstelle eine eigene IP-Adresse, Service-Port, Routing-Tabelle usw. besitzen, ansonsten wird kein separater Networkstack in den Containern platziert.
- * Der **IPC-Namespace (POSIX/SysV IPC²⁶)** isoliert unter UNIX die Interprozesse-Kommunikationsmechanismen und dürfen nicht zwischen dem Host- und den Container geteilt werden. Jeder Container besitzt demnach seine eigenen IPC-Mechanismen.
- * Der **MNT-Namespace** isoliert die Dateisysteme zwischen dem Host- und den Containern. Die eingehängten Volumes sollten sparsam und so restriktiv wie immer möglich in die Container eingebunden werden. Auf die Einbindung von sensitiven Verzeichnissen wie „/, /boot, /dev, /etc, /lib, /proc, /sys, /usr“ sollten wenn überhaupt, nur mit Leserechten zugegriffen werden können. Bei allen anderen Volumes darf der Mount-Propagierungsmodus nicht auf shared stehen, denn dies würde den gemeinsamen Nutzen der Volumes erlauben.

²⁶SystemV IPC ist der Name für drei Interprozess-Kommunikationsmechanismen (Message Queue, Semaphore und Shared Memory), die unter UNIX-Derivaten weit verbreitet sind. [<https://man7.org/linux/man-pages/man7/sysvipc.7.html>]

- * Der **UTS-Namespace** isoliert zwei Systemkennungen (Hostnamen und dem NIS-Domänennamen) zwischen dem Host- und den Containern. Das wird verwendet, um den Hostnamen und die Domäne festzulegen, die für die Ausführung von Prozessen im Namespace sichtbar sind. Normalerweise müssen die Container diese Informationen nicht kennen.

Bei den SCION-Router-Untersuchungen fielen keine Auffälligkeiten oder Ungereimtheiten, ausser beim NET-Namespace, auf. Unsere SCION-Services leben sozusagen direkt ausserhalb vom Container und das könnte möglicherweise gefährlich sein. Ein Container bekommt dadurch keine eigene IP-Adresse zugewiesen und kann über die Host-IP-Adresse angesprochen werden. Durch die Netzwerkeinbindung mit der Option „host“ könnte der Container zudem auf Netzwerkdienste wie den D-Bus²⁷ zugreifen und möglicherweise unerwünschte Aktionen ausführen. Ein SCION-Router ist jedoch auf diese Netzwerkfunktion angewiesen, da es die Leistung optimiert, dadurch keine NAT (Network Address Translation) erforderlich ist und für jeden Serviceport kein Userland-Proxy²⁸ erforderlich wird.

SCRC-10521 - Direct access to host devices SCORED

Die Docker Container sind mittlerweile auch ohne hohe Privilegien in der Lage, die Host-Geräte in einen Container direkt einzubinden und zu manipulieren. Zusätzlich wäre ein Container sogar in der Lage, die Blockgeräte vom Host abzuhängen. Ein SCION-Router benötigt keine direkte Gerätezugriffe. Sollte dies jedoch künftig einmal notwendig werden, so sollten die Freigabeberechtigungen sorgfältig überlegt und gewährt werden. Auch hier könnten fatale und böswillige Folgen daraus resultieren, die zu einem kompletten Systemausfall führen könnten.

SCRC-10522 - Default system resource limits SCORED

Der Linux-Kernel definiert und bietet Kontrolle über die Ressourcenlimite (ulimits), die den Prozessen und Containern zugewiesen und zur Verfügung gestellt werden können. Gut konzipierte Ressourcenbeschränkungen können das System vor einer Überlastung schützen. Nicht korrekt gesetzte Werte könnten den Host überbeanspruchen und zu einem Komplettausfall führen. In den meisten Anwendungsfällen, wie in unserer SCION-Umgebung, genügen die auf der Docker-Daemon-Ebene festgelegten Standardeinstellungen. Sie können für eine bestimmte Containerinstanz die Werte justieren, aber sollten mehrere SCION-Services künftig die Ulimit überschreiten, so wird empfohlen, eine allgemeine, konstante und auf das zugrundeliegende System abgestimmte neue Standardeinstellung zu definieren.

SCRC-10524 - Limit of concurrently running processes SCORED

Die SCION-Services, bestehen grundsätzlich nur aus einem Binary und andere Funktionen wie der BGP-Router (Quagga), der von einem Drittanbieter stammt, verfügt innerhalb vom Container über mehrere ausführbare Anwendungen. Auch wenn es vielleicht in manchen Situationen nicht notwendig erscheint, macht es dennoch Sinn, die SCION-Plattform standardisiert aufzusetzen. Daher empfiehlt es sich, eine Maximalobergrenze z. B. von 100 für die gleichzeitige Ausführung von Prozessen innerhalb vom Container zu definieren. Sollte es jemals einem Angreifer gelingen, mit einem einzigen Befehl im Container weitere Prozesse zu starten oder sich rekursiv zu replizieren, könnte dies in einer sogenannten Forkbomb enden. Alle verfügbaren Systemressourcen wären dann aufgebraucht und das System steht. Nach dem SCION-Router-Absturz würde nur noch einen Neustart weiterhelfen, um ihn wieder funktionsfähig zu machen.

²⁷Die D-Bus-Architektur auf Ubuntuusers [<https://wiki.ubuntuusers.de/D-Bus/>] kurz erklärt.

²⁸Ein Docker-Proxy arbeitet im User Space und empfängt alle Datenpakete auf den spezifizierten Serviceports des Hosts. Die Datenpakete, die der Kernel nicht verworfen oder weitergeleitet hat, leitet der Proxy an den Port des Containers weiter.

SCRC-10525 - Default network interface is not used SCORED

SCION verwendet die virtuelle Standard-Bridge-Schnittstelle „Docker0“ nicht und soll auch künftig nicht verwendet werden, da auf dieser Schnittstelle keine Filterung angewendet wird, ist sie anfällig auf ARP-Spoofing- und MAC-Flooding-Angriffe.

SCRC-10526 - Docker socket is not mounted SCORED

Der Docker-Socket darf keinesfalls in einem Container bereitgestellt werden. Die Container internen Prozesse wären so in der Lage die Docker-Befehle auszuführen. Dem Angreifer könnte es so effektiv die vollständige Kontrolle über den Host ermöglichen. Die SCION-Services werden keinen Docker-Socket-Zugriff gewähren.

6.4.6. Docker Container Security Operations [DCSO]**DCSO-10611 - Keep the system tidy** SCORED

Eine Docker-Container-Umgebung kann schnell dazu verleiten, dass sie nicht umgehend aufgeräumt wird und mit der Zeit etwas verwahrlost. Noch nicht eingesetzte Container vorrätig auf dem Host abzuspeichern sind auch zu vermeiden. Solche unbereinigten Hosts könnten zu betrieblichen Sicherheitsproblemen führen. Deshalb verhilft dieser Kontrollpunkt zu einer mehr bereinigten, übersichtlicheren und fehlermindernden SCION-Plattform. Mit einer simplen Überprüfung kann verifiziert werden, wie viele Container aktiv laufen und wie viele gestoppt wurden. Bei einer Diskrepanz der beiden Werte sind entsprechende Massnahmen zu treffen.

DCSO-106xx - Monitor SCION usage, performance, and metering NOT SCORED

Die Systemüberwachung bezüglich CPU, Memory und Network Traffic ist in fast allen IT-Umgebungen ein sogenannter Dauerbrenner und ein sehr wichtiger Bestandteil vom Capacity Management, sowie der Cyber Security Strategie. Im SCION-Umfeld bezüglich Monitoring und Alerting wird vor allem auf Prometheus und Grafana gesetzt. Wir in der SIX betreiben schon heute für etliche Applikationen mit sehr unterschiedlichen Anforderungen eine hochverfügbare OpenShift-Plattform. Nicht nur im Netzwerk, sondern auch in unserer Container-Umgebung, benötigen wir gewisse Überwachungsmaßnahmen. Um für SIX die richtige Überwachungsstrategie bezüglich SCION zu finden, macht es freilich Sinn die bestehenden Synergien effektiv zu nutzen, damit anschliessend die Ergebnisse im Konzept der SIX-Infrastrukturüberwachung aufgenommen und entsprechend umgesetzt resp. eingeführt werden können.

6.4.7. Disable Cluster Operation Threats [DCOT]**DCOT-10711 - Docker container cluster management** SCORED

Die einzelnen laufenden SCION-Container dürfen schon fast als Micro-Services auf dem Host angesehen werden und sie laufen bekanntlich auch auf den benachbarten und redundanten SIGs. Auf den separaten Routern, nicht als Cluster-Einheit verbunden, laufen also die SCION-Services mehr oder weniger voneinander getrennt und unabhängig. Ein Docker-Container-Image kann sehr unterschiedlich eingesetzt werden. Unsere SCION-Services sind schon relativ schlank als Binaries konzipiert, aber im Docker-Umfeld kann es Container mit noch servicespezifischeren Eigenschaften genannt Tasks geben. Sie sind damit die kleinste Einheit, die innerhalb eines Service läuft. Diese Tasks können aus Ressourcentechnischen- und/oder Redundanz-Gründen auf unterschiedlichen Hosts als Cluster betrieben werden. Dafür wird ein geeignetes Docker Container Cluster Management System namens Swarm benötigt. Da Container als Prozesskapsel nichts vom Docker Swarm und dessen Serviceabstraktion wissen, fungiert der Task als Verbindungsstück zwischen Swarm und Container. Wir benötigen die Swarm-Funktion nicht und stellen somit sicher, dass wir

auch künftig keine Angriffsfläche übers Netzwerk auf die Cluster Management and Node Communication Serviceports bieten.

6.5. Erkenntnisse

Infolge ausgiebiger Sicherheitsüberprüfungen der SCION-Services, die durch Anapaya Systems AG bereitgestellt wurden, konnten einige sicherheitsrelevante Punkte mit Optimierungspotenzial aufgedeckt werden. Grundsätzlich darf gesagt werden, dass der SCION-Router schon heute aus ganzheitlicher Sicherheitsbetrachtung relativ gut gehärtet betrieben wird. Dennoch gibt es einige essenzielle und sicherheitsrelevante Punkte, die nochmals überarbeitet, justiert oder angemessen aktiviert werden müssen. Ein massgeblicher zusätzlicher Beitrag an die Sicherheit resp. Systemstabilität gäbe ein adäquates aktives Docker-Audit-Logging, restriktivere Zugriffsregeln auf die SCION-Services durch eine Filterung²⁹ mit Iptables, strengere Container-Berechtigungen (Privileges/Capabilities), strengere Dateizugriffsberechtigungen auf die SCION-Service-Spezifikationen und eine Begrenzung des Systemressourcenverbrauchs durch die SCION-Services. All diese Massnahmen könnten das System mehr auslasten, womöglich negativ beeinflussen oder bedingt den operativen Betrieb erschweren. Somit könnte die Umsetzung einer Empfehlung nicht im vorgeschlagenen Masse gerechtfertigt sein und mit einer angebrachten Dokumentation kann der Entscheid in Zukunft von Dritten nachvollzogen werden. Wichtig erscheint jedoch, dass jedes Instrument vor der Implementierung von den Entwicklern nochmals genauestens angeschaut und beurteilt wird. Ein anschliessender und ausgiebiger Acceptance Test mit der finalen Konfiguration ist zwingend notwendig und auch hier nicht wegzudenken. So wie das letzte Mal, kommen einige Empfehlungen aus der Security Community und den SIX-Weisungen. Andere wurden für den SCION-Router spezifisch entwickelt. Aufgrund der gegebenen SIG-Funktion konnten manche Empfehlungen nicht oder nur teilweise berücksichtigt werden. Im Testskript befinden sich jedoch unter den einzelnen Tests die finalen und gewünschten Endresultate als Empfehlungen. Damit kann die SCION-Appliance weiterhin den hohen Anforderungen gerecht werden und erfüllt so die bestmöglichen Sicherheitsvorteile bezüglich Cyber Security (Protection, Detection and Response). Als Grundvoraussetzung zu den besprochenen, zahlreichen und tiefgreifenden Sicherheitsüberprüfungen der SCION-Services gilt das OS-Hardening des SCION-Routers. Die SCION-Appliance führt mehrere Container mit den SCION-Kernservices aus, daher ist es äusserst wichtig, das Hostsystem auf dem neuesten Stand zu halten und gemäss Best Practices zu härten, um Fehlkonfigurationen und bekannte Sicherheitslücken in der Hostsicherheit zu vermeiden. Bei bestehenden Sicherheitsrisiken resultiert eine erhöhte Gefahr von möglichen Kompromittierungen des Systems und der SCION-Services. Diese Voraussetzungen werden mit unseren bereits getätigten Systemhärtungen vollumfänglich erfüllt. Einen direkten Internetzugang für alle IT-Systeme, sowie den SCION-Routern, ist aus dem SIX Corporate Network nicht gestattet. Derartige direkte Verbindungen zur Aussenwelt benötigen, zusätzliche und besondere Schutzmassnahmen inkl. einer SIX-internen Sonderbewilligung. Durch diese SIX-Weisung vermeiden oder limitieren wir bestmöglichst die Angriffsfläche aus dem unsicheren Internet. Wir in der SIX stellen für solche Anforderungen den bevorzugten SmartProxy von JFrog Artifactory oder den WebProxy von Bluecoat zur Verfügung. Da SCION in der SIX nach wie vor den Status „experimental“ genießt, muss der Punkt mit der geregelten und gehärteten Supply Chain nicht nur für das Ubuntu-Betriebssystem, sondern auch für die SCION-Container, zwischen Anapaya Systems AG und SIX noch vor dem produktiven Einsatz geklärt werden. Zudem fordert dies SIX grundsätzlich für alle IT-Systeme und Containern mit unterschiedlichem Entwicklungsstatus eine physisch

²⁹Im Container-Umfeld gibt es unterschiedliche Network-Security-Projekte (z. B. NeuVector, Calico, Weave Net oder Flannel), um die Container-Infrastruktur noch besser schützen zu können. Auf einem SIG erscheint aufgrund der einzelnen primären Funktion, den möglichen zusätzlichen Performance- und Stabilitäts-Einbussen und der erhöhten Komplexität nicht gerechtfertigt. Auf dem SIG wäre eine Container-Konsolidierung in manchen Belangen sinnvoller und gewinnbringender.

oder logisch getrennte Appliance (Preproduction and Production [PnP] Environment). Wenn immer möglich testet die SIX die Services, wie wir es auch für die SCION-Services umsetzen, sogar auf einer komplett getrennten und physisch voneinander isolierten Netzwerkinfrastruktur (Lab/Prod). Dieses Vorgehen erlaubt es, uns Performance- und Security-Tests wie z. B. Pentests ohne die Beeinflussung der produktiven Infrastruktur durchzuführen. Definiert wird PnP im SIX-Dokument „Layered Security Masterplan (LSM)[40]“. Ein weiterer Sicherheitsaspekt kommt hinzu, dass auf demselben Server nur mehrere Container zum Zweck derselben primären Funktion wie z. B. das SIG gleichzeitig vorhanden sein dürfen. Eine Mischung von unterschiedlichen Primärfunktionen oder von Funktionen mit unterschiedlichen Sicherheitsstufen ist verboten. Eine Verletzung des CIA Prinzips muss verhindert werden. Alle SCION-Binaries werden so minimal und schlank wie nur möglich entwickelt und gehalten. Damit weiterhin die Komplexität möglichst tief gehalten und den SCION-Versprechen weiterhin treu geblieben werden kann, darf keine Endpoint Security Software innerhalb der Container installiert werden. Wenn dann, sollte die Endpoint Security Lösung künftig nur auf dem SCION-Hostsystem eingesetzt werden.

Ergänzend zu diesem Schwerpunkt, möchten noch ein paar wichtige und unerwähnte Punkte mit Nachdruck auf den Weg zur erfolgreichen SCION-Integration bei SIX mitgegeben werden:

- * SCION Security Update and Patch Management (SIX CERT-Prozess³⁰)
- * SCION Supply Chain Management (SSCM)
- * SCION Security Module Optimization (AppArmor und Seccomp)
- * SCION Implementation of Hardening Measures
- * SCION Firewall Rule Logging Concept (Iptables)
- * SCION Confidentiality and Integrity (Real Time Auditing)³¹
- * SCION Release Acceptance Test (Integration- und Produktions-Umgebung)
- * SCION Hardened Services with Tripwire (Ubuntu und Red Hat)
- * SCION Use Cases für Security Operations Center (SOC)
- * SCION Application Logging³²

Die obere Liste ist keinesfalls als vollständig anzusehen, denn sie verfolgt das Ziel, die unbedingt umzusetzenden Themen nochmals anzudeuten oder weitere unbearbeitete Punkte auf den Tisch zu bringen. Es wird stets eine noch sichere und widerstandsfähigere SCION-Infrastruktur angestrebt. Abschliessend benötigt es noch einige Klärungen bezüglich der Vollständigkeit der gemachten Optimierungsvorschläge. Im Testskript gibt es einige Plausibilitätskontrollen, die eine grobe Prüfung durchführen aber den Inhalt

³⁰Es dürfen nur Sicherheitsupdates verwendet werden, die von Anapaya Systems AG bereitgestellt resp. freigegeben wurden. Sicherheitsupdates oder Sicherheitskonfigurationen, die von Ubuntu oder Anapaya als „kritisch“ eingestuft werden, MÜSSEN gemäss den Ergebnissen des SIX CERT-Prozesses installiert oder implementiert werden. Das Patchen von kritischen Vulnerabilities MUSS innerhalb eines Tages möglich sein. Da Container-Images auf einer Basis-Betriebssystemschiicht übertragen werden, ist ein schneller Patch-Mechanismus von grundlegender Bedeutung. Das Ubuntu-Image wird durch SIX aktualisiert und die SCION-Images werden von Anapaya Systems AG mit den Aktualisierungen neu erstellen und ausgeliefert.

³¹Auditd als Linux Auditing System ist ein mächtiges Werkzeug und kann auch zur Überwachung von Dateien und Verzeichnissen verwendet werden. Die Vermeidung von zusätzlichen Agents oder Programmen auf dem SCION-System ist sinnvoll. Künftig könnten z. B. sehr sensible Daten wie Firewall-Regeln, Zertifikate, TRCs etc. mit diesem Bordmittel überwacht werden. Jegliche Änderungen würden im SOC registriert und verifiziert werden.

³²Die zugrundeliegende SCION-Dokumentation lässt momentan keine Aussage über die Protokollierung der einzelnen SCION-Applikationen zu. In einer weiterführenden Arbeit empfiehlt sich, den Detaillierungsgrad der Logging-Informationen anzuschauen und gegebenenfalls zu erweitern. Das Hauptziel sollte sein, dass künftig mit akzeptablen Kompromissen das Cyber Security Monitoring und das Post Mortem von Cyberattacken optimiert werden kann.

nicht exakt überprüfen. Das heisst, es kann vorkommen, dass bei manchen Tests eine nachträgliche und manuelle Sichtung durch einen Experten immer noch notwendig ist. Dies wird entsprechend im Testinglog ausgewiesen und vermerkt. Als gutes Beispiel möchte zur Erklärung das Iptable-Regelwerk genannt werden. In dieser Kontrolle wird lediglich die Anzahl von Regeln pro Chain geprüft. Die Sinnhaftigkeit und Korrektheit kann momentan mit den zugrundeliegenden Informationen nicht geprüft werden und ausserdem sind sie sehr kundenspezifisch. Eine vollumfängliche Automatisierung inklusive einer Detailprüfung ist erst nach einem finalen Regelwerk möglich. Ein weiteres gutes Beispiel ist die BGP-Router-Konfiguration. Eine Prüfung vom BGP- oder Login-Passwort wird nicht geprüft. In diesem Fall verlassen wir uns vorerst auf das Appliance-Hardening (Triple-A-System) und die regelmässigen SCB-Checks seitens SIX Access Plattform. Ausserdem sind die Kontrollen nicht abschliessend zu betrachten und bei einigen gibt es noch immer Verbesserungspotenzial. Der Testumfang und Detaillierungsgrad darf künftig gerne erweitert und optimiert werden.

FORENSISCHE ANALYSE

Mit einem immer bedeutsam werdenden Themenbereich, beschäftigt sich das letzten Kapitel mit der Computerforensik. Im Vorfeld wurde in der funktionstüchtigen Trainingsumgebung bereits eine relativ tiefgreifende Anwendungsanalyse der wichtigsten SCION Services auf einem SIG durchgeführt und unter Abschnitt 1.1 und im Kapitel 6 detailliert beschrieben. Bei einem Sicherheitsvorfall muss sich der Forensiker an fast unzähligen und komplexen Fragen stellen und klären. Da ist ein grundlegendes Verständnis über die Systemfunktionalitäten, der zu untersuchenden Komponenten, ein grosser Vorteil und praktisch nicht wegzudenken. Mit den vorangegangenen Themenschwerpunkten wurde also eine solide Basis geschaffen, die Systemsicherheit auf ein höheres Niveau gehoben, die Erkennung von möglichen Sicherheitsvorfällen optimiert und die beiden forensischen Analysepraktiken Dead- und Live-Analyse merklich unterstützt. Das hier verfolgte Hauptziel der forensischen Untersuchungen ist, möglichst alle verbleibenden Spuren auf einer SCION Appliance nach der Ausführung von verschiedenen Inbetriebnahmeschritten aufzuzeigen und zu beschreiben. Die Annahme geht von einem sauberen nicht kompromittierten SCION System aus und somit sind die zu analysierenden Daten mit deren Inhalten weitestgehend bekannt. Die hier durchgeführten Spurenanalysen finden im begrenzten Umfang an persistenten Speichern, an sogenannten „toten“ Datenträgern, statt. Die erwähnte Anwendungsanalyse erfolgte damals bewusst ohne Spurensicherung an laufenden Komponenten und dient dem reinen funktionellen SCION Verständnis. Anknüpfende forensische Live-Analysen von flüchtigen Spuren im laufenden Betrieb z. B. von Prozessorregistern, Cache, Arbeitsspeicher, Netzwerkdaten, offene Dateien, aktive Prozesse und benutzte Bibliotheken dürfen sehr gerne in einer weiterführenden Arbeit wiederaufgenommen werden.

7.1. Implementierung

Dieses Kapitel dient der abschliessenden detaillierten Beschreibung und Darstellung der erwähnten Laborumgebung, mit Erläuterungen der verwendeten zusätzlichen Applikationen und deren Aktionen sowie der Darstellung welche Untersuchungsmethoden in welchem Fall angewendet wurden. Damit wird das Vorgehen weiter verdeutlicht und begründet. Zugleich dient es der Nachvollziehbarkeit der vorliegenden Arbeit. Anschliessend folgt das forensische Hauptkapitel der Dokumentation, in dem die Spuren anhand der geschilderten Methoden extrahiert, analysiert, bewertet und beschrieben werden. Alle nachfolgenden Erläuterungen und Ausführungen innerhalb den forensischen Unterkapiteln basieren auf dem erlangten Wissen aus den Studienbriefen[12][55][21][56][20] und deren Modul-Projektarbeiten.

Dem Thema entsprechend und hinsichtlich der Bedeutsamkeit sowie zu Vollständigkeitszwecken möchte hier zu Beginn die gemachte Annahme als Grundvoraussetzung nochmals klargestellt werden. Bei den durchgeführten Untersuchungen resp. im IT-Sicherheitsumfeld sind die Begriffe „Integrität“ und „Authentizität“ der digitalen Spuren besonders wichtig und von Interesse. Daher wird in dieser SCION Laboraufgabe davon ausgegangen, dass die Vorgaben für die Verwahrungskette (Chain of Custody), bis zum Zeitpunkt nach

der Einlieferung der genannten Abbilder im Cloudstore¹, seitens Anapaya Systems AG eingehalten wurde. Bei der Generierung, Sicherung und Analyse digitaler Spuren muss eine allgemein akzeptierte und erprobte Vorgehensweise angewandt werden, damit diese Spuren in möglichst überzeugender Form als Beweismittel vor Gericht verwendet werden können. Unsere digitalen Ermittlungen erfolgten nicht als Teil einer Strafverfolgung und daher ist die nachfolgende Dokumentation nicht als forensischer Bericht zu verstehen. Wie schon mehrfach betont, wird hier eine solide Basis der IT-Forensik rund um das Thema „SCION IP Gateway“ gelegt. Die Spurenerstellung gehört in unserem forensischen Prozess zur sogenannten Generate Evidence-Phase (GE). Das ist sozusagen der zweite Prozessschritt vor der Spurengewinnung und Untersuchung. Zuvor folgt immer die Preparation Phase (P) und sie versucht:

- das Grundrauschen der zu untersuchenden Maschine so weit möglich zu minimieren,
- für die Automation hinderlichen Sicherheitsmechanismen zu justieren,
- für die Untersuchungen notwendigen Tools vorzuinstallieren und zu konfigurieren,
- sowie das Hintergrundrauschen zu ermitteln.

Wie vermutlich bemerkt, stellt uns das bewährte forensische Vorgehensmodell schon zu Beginn vor zusätzliche Herausforderungen und einem ungewünschten oder besser gesagt zu einem komplexen Sachverhalt. Die Gewinnung von digitalen Spuren fordert also ein striktes und exaktes Vorgehen. Jegliche Abweichungen im Prozess haben unweigerlich und unwiderrufliche Auswirkung auf die digitalen Spurenbilder. In den Analysen stellt die Feststellung von Assoziationen und damit die Rekonstruktionen von Ereignissen den Kern der Untersuchung dar. Die Rekonstruktionen oder daraus resultierten Hypothesen könnten berechtigterweise in Frage gestellt werden, da sie dadurch verfälscht oder verunmöglicht werden. Die eingelieferten Images wurden weitestgehend von Technikern und Entwicklern der Firma Anapaya Systems AG vorbereitet. Sie sind keine ausgebildeten IT-Forensiker und haben nach bestem Wissen und Gewissen, anhand grundlegender Unterweisungen seitens Autors in das Vorgehensmodell, die Images vorbereitet und zur weiteren Bearbeitung eingeliefert. Des weiteren besteht die Tatsache, dass einige weitere vorbereitenden Anpassungen, für die automatisierte Analyse nach der GE-Phase vorgenommen werden mussten. Mit anderen Worten widerfuhren den Images nachträglich nochmals einige Änderungen, die eigentlich in der P-Phase hätten erledigt werden müssen. Die genannten unvermeidbaren Konstellationen sollen nicht an den geplanten forensischen Untersuchungen hindern. Die gegebenen besonderen Umstände müssen bekannt sein und auf mögliche Spurenabweichungen bei weiteren unabhängigen mit identischen Untersuchungen hinweisen. Je nach Leserschaft könnten die Spurenbilder und daraus resultierenden Hypothesen kritisiert oder sogar als unbrauchbar betitelt werden. Der Autor kann diese Diskussionspunkte absolut nachvollziehen und verstehen. Jedoch ist er auch der Ansicht, dass die daraus resultierenden Resultate eher der Realität aus einer produktiven Umgebung entsprechen. In einem produktivem Umfeld vernehmen wir praktisch nie dieselben Aspekte.

7.1.1. Untersuchungsumgebung

Über die Umsetzung, wie und unter welchen Bedingungen, sowie in welcher Umgebung die forensischen Analysen durchgeführt werden, wurde schon einleitend und unter dem Abschnitt 1.3 und Abschnitt 4.2 ausgiebig diskutiert und dokumentiert. Aufgrund von unterschiedlichen einleuchtenden Argumenten konnten die folgenden Analysen leider nicht an laufenden und funktionierenden Systemen gemacht werden. Wie

¹https://anapaya-my.sharepoint.com/:f:/r/personal/bischofberger_anapaya_net/Documents/SIX%20Andreas%20Maure%20r?csf=1&web=1&e=G8NR1u

dargelegt, war damals die in der Cloud betriebene Trainingsumgebung mit einem älteren Softwarestand versehen und entsprach nicht der definierten Installation und Konfiguration. Die SSFN Integrationsinfrastruktur befand sich noch mitten im Endaufbau und in der Testphase zusammen mit den strategischen Endkunden. Einen Nachbau einer funktionierenden SSFN Infrastruktur wäre nicht verhältnismässig gewesen. Nichtsdestotrotz konnten die Untersuchungen unter best möglichen, optimalen Bedingungen, effizient und effektiv lokal auf der Forensik-Workstation in virtueller Form durchgeführt werden.

Die Umstände wurden transparent klargelegt. Nun möchten noch auf die unerlässlichen und vorbereitenden Massnahmen, der erweiterten P-Phase, eingegangen werden. Diese waren wie erfahren vor der GE-Phase notwendig. Die einleitenden Massnahmen haben leider zwei Kehrseiten und daher ist es unerlässlich die Systemveränderungen im Voraus zu deklarieren und transparent auszuweisen. Jegliche Veränderungen hinterlassen unerwünschte Artefakte². Die erhaltenen Images wurden weitgehend automatisiert aufgesetzt und gleichen produktionsnahen Abbildern aus der SIX SSFN Infrastruktur nachgebaut. Es besteht nun mal die Tatsache, dass wir uns hier in einer nachgebildeten produktiven Testumgebung befinden und produktive Daten analysieren möchten. Die SCION Hardening-Konfigurationen sehen z. B. keinen SSH-Remotezugriff mittels Benutzernamen und Passwort vor. Jegliche Fernzugriffe sind nur mittels einem gültigen SSH-Key zur Authentifizierung zugelassen. Die dafür notwendigen SSH-Keys sind vertraulich und daher nicht vorliegend. Für den Security Audit benötigt es einen sicheren und einfachen Datenaustausch mittels SCP und einen Fernzugriff mittels SSH. Um diese Anforderungen zu bewerkstelligen, waren die folgenden Systemveränderungen resp. Vorbereitungen notwendig:

Funktion/Tool	Beschreibung
Passwortänderung	Mit dem Boardmittel „passwd“ wurde für den Benutzer „anapaya“ das kryptische Passwort geändert und auf „test123“ gesetzt.
SSH Konfiguration	Mit dem Boardmittel „vi“ wurde die SSHD-Konfiguration „/etc/ssh/sshd_config“ so abgeändert, dass eine Authentifizierung mittels Passwort möglich ist. Der Parameter PasswordAuthentication wurde auf „yes“ gesetzt.
Snapshot	Nach der Sicherstellung des ordnungsgemässen Betriebs wird zu Wiederherstellungszwecken eine Momentaufnahme (Snapshot) der VM erstellt. Bei zukünftigen Problemen, kann wenn immer notwendig, wieder auf den Ausgangspunkt zurückgesprungen werden.
Hintergrundrauschen	In den folgenden Untersuchungen wird in unterschiedlichen Abständen immer wieder die VM gestartet und eingefroren. Innerhalb diesem kurzen Zeitraum werden die zu untersuchenden Aktionen ausgeführt und es liegt in der „Natur“ des Betriebssystems, dass auch im Ruhezustand ohne Benutzerinteraktionen gewisse System- und Anwendungsservices ihre Hintergrundaktionen ausführen. Es ist demnach absolut notwendig, das Hintergrundrauschen herauszufiltern und zu vermeiden. Für eine spätere Herausfilterung wird einerseits ein Ursprungsabbild und ein Abbild mit dem Hintergrundrauschen erstellt.

Tabelle 7.1.: Vorbereitungen der SCION-Images (Untersuchungsobjekte)

Der Vollständigkeit halber folgen die durchgeführten Massnahmen an der Admin- und Forensik-Workstation. Beide Workstations haben ohne Interaktionen mit den SCION-Images und den zu eruiierenden Spurenbil-

²Artefakte [[https://de.wikipedia.org/wiki/Artefakt_\(Diagnostik\)](https://de.wikipedia.org/wiki/Artefakt_(Diagnostik))] sind durch menschliche oder technische Einwirkung entstandene Produkte oder Phänomene. Sie sind wissenschaftlich wertlos, weil sie nichts über den eigentlichen Untersuchungsgegenstand aussagen, sondern lediglich eine diagnostische Fehlerquelle darstellen.

den keinen Zusammenhang. Aus dem jungfräulichen Anapaya-Base-Image wurde die Admin-Workstation gebildet. Grundsätzlich sollte jedes Linux-System unabhängig vom Release und der Konfiguration dafür verwendet werden können. Die einzigen bestehenden Systemvorgaben sind die Einhaltung der Unternehmenskonformität und den schadstofffreien Betrieb im Netzwerk. Zur Erfüllung unserer hier gestellten Aufgabe waren die folgenden Systemveränderungen notwendig:

Funktion/Tool	Beschreibung
Passwortänderung	Mit dem Boardmittel „passwd“ wurde für den Benutzer „anapaya“ das kryptische Passwort geändert und auf „test123“ gesetzt.
SSH Konfiguration	Mit dem Boardmittel „vi“ wurde die SSHD-Konfiguration „/etc/ssh/sshd_config“ so abgeändert, dass eine Authentifizierung mittels Passwort möglich ist. Der Parameter PasswordAuthentication wurde auf „yes“ gesetzt.
Lynis Installation	Mit dem Boardmittel „scp“ wurden die Lynis-Konfiguration „\$HOME/lynis“, „\$HOME/lynis-sdk“ und das Helper-Skript „\$HOME/j2lynis.sh“ auf das System kopiert. Die Remote-Zugriffe und -Audits werden anschliessend nur noch über SSH angesteuert und mittels Benutzernamen „anapaya“ und dem Passwort „test123“ authentifiziert.
Snapshot	Nach der Sicherstellung des ordnungsgemässen Betriebs wird zu Wiederherstellungszwecken eine Momentaufnahme (Snapshot) der VM erstellt. Bei zukünftigen Problemen, kann wenn immer notwendig, wieder auf den Ausgangspunkt zurückgesprungen werden.

Tabelle 7.2.: Vorbereitungen der Admin-Workstation

Die letzten zu erwähnenswerte Images sind die Forensik-Workstations. Sie werden vor allem von IT-Forensikern oder gegebenenfalls von einem SOC Mitarbeiter bei einem Security Incident eingesetzt. Diese Workstation befindet sich normalerweise in einer Laborumgebung und daher sollte die korrekte und schadstofffreie Funktion vollkommen ausreichen. Dem von der Universität³ bereitgestelltem DFXML-Image und dem Windows-Rechner widerfahren zur Erfüllung unserer hier gestellten Aufgabe lediglich noch folgende Systemveränderungen:

³Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU)

Funktion/Tool	Beschreibung
OS Updates	Für einen reibungsloseren und sicheren Betrieb wurde die Ubuntu- und Windows-Software entsprechend auf den neusten aktuellsten Stand gehoben.
Software Installation	Für die forensischen Analysen sind auf dem Windows-Rechner die erwähnten Tools notwendig. Daher wurden die Anwendungen TestDisk, FTK Imager, Autopsy und The Sleuth Kit heruntergeladen und ordnungsgemäss vorinstalliert.
Shared Directory	Um den Datenaustausch zwischen dem Host- und den Gast-Systemen zu gewährleisten wurde ein gemeinsames Verzeichnis eingerichtet.
Überprüfung/Tests	Die VirtualBox bietet für die VM-Steuerung eine API-Schnittstelle an. Um die Analysen weitgehend zu automatisieren, wird über die CLI mittels Befehl „VBoxManage“ die VMs gesteuert und fordert daher im Voraus einen Funktionstest.
Snapshot	Nach der Sicherstellung des ordnungsgemässen Betriebs wird zu Wiederherstellungszwecken eine Momentanaufnahme (Snapshot) der VM erstellt. Bei zukünftigen Problemen, kann wenn immer notwendig, wieder auf den Ausgangspunkt zurückgesprungen werden.

Tabelle 7.3.: Vorbereitungen der Forensik-Workstations

7.1.2. Angewendete Methode

Zu den essenziellen Analysemethoden gehört in der IT-Forensik die Dateisystemanalyse. In direkter Abhängigkeit zum Sicherheitsvorfall, dem Anwendungsfall oder der Hardware- und Software-Spezifikationen kann eine Datenträgeranalyse weniger oder umfangreicher ausfallen. Je nachdem wie der Forensiker den Sachverhalt deutet, variiert das Vorgehen bei der Spurengewinnung und Spurenanalysen. Die im Vordergrund stehenden forensischen Fragestellungen, wurden bereits unter Abschnitt 1.3 auf Seite 14 festgehalten. Wie es in Projekten üblich ist, können gewisse Sachverhalte den Projektverlauf und/oder Projektumfang direkt beeinflussen. Aus den bekannten Gründen erfolgen daher etwas reduzierte forensische Untersuchungen. Die für die Spurenanalysen in Frage kommenden Aktionen, werden jeweils in den dafür vorgesehenen Unterkapiteln erläutert.

Die Spurengewinnungen und Auswertungen erfolgen situationsgerecht manuell oder automatisiert. Nicht alle zu untersuchenden Spuren der ausgeführten Aktionen, Konfigurationen und SCION-Installationen erfolgten komplett automatisiert über ein API oder das CLI/SSH. Wo möglich und zur Vereinfachung wurden unterstützende Anwendungen erstellt. Mehr dazu im nächsten Unterkapitel. Wie die konkreten Abläufe für die Spurengenerierungen und Spurensicherungen der zu untersuchenden Aktionsbilder im Detail umgesetzt wurden, können der Datei „README_FORENSICS“ auf der beigelegten CD-ROM entnommen werden. Bei forensischen Analysen von Anwendungen kommen zwei Methoden, die Ereignis- und Zustandsmethode in Frage. Da die Techniken ihre eigenen spezifischen Vor- und Nachteile haben, werden für die Untersuchungen normalerweise immer beide angewendet. Bei der Ereignismethode analysiert man bekanntlich das laufende System und speichert lediglich die Ereignisse von einem bestimmten Programm, die zu einer Zustandsänderung führten. Das dramatische Wachstum von Speicherkapazität und Netzwerkbandbreite macht forensische Untersuchungen immer schwieriger. Auch zu berichten, was auf einem bestimmten Datenträger vorhanden ist und was sich in einem gewissen Zeitraum verändert hat. Im SCION-Umfeld sind die Speicherplatzanforderungen nicht gross. Andererseits sind die hier zu untersuchenden Abbilder mit 64 GiByte

schon sehr zeitraubend und ressourcenintensiv. Stattdessen konzentrieren sich die Analysten darauf, welche Eigenschaften des Mediums (Laufwerke) sich zwischen zwei Schnappschüssen in der Zeit verändert haben. Der bekannte Computer Wissenschaftler Simson Garfinkel beschäftigte sich stark mit verschiedenen Algorithmen, um eine differenzielle Analyse[23] von Computemedien zu implementieren. Das bekannte DFXML Toolset (2012) basiert auf dem allgemeinen Algorithmus von Garfinkel[23]. In diesem Vorgehen der Zustandsmethode vergleicht man vor und nach der Ausführung einer Aktion die Zustände (MAC⁴ times) der Dateisystemdaten. Zu den altbekannten MAC-Zeiten kommt noch eine weitere wichtige Zeitanzeige hinzu, die auch innerhalb der Inode-Metadaten⁵ aufzufinden ist, und zwar der Löschezitpunkt „mtime“ einer Datei. Die Firma QuoScient GmbH⁶ hat über die Zeitstempel einen sehr interessanten Artikel verfasst. Er verfügt sogar über mehrere Matrices, die anhand von verschiedenen Systemmodifikationen die MAC(B)-Auswirkungen aufzeigen. Eine weitere sehr beliebte und effektive Vorgehensart resp. sehr nützlicher und entscheidender Schritt in der Zustandsmethode ist die Erstellung einer Super-Timeline. Das Ziel ist es, von verschiedenen Logdateien und forensischen Artefakten der Datenträger, eine Analyse zu machen, um eine einzige korrelierte Zeitleiste zu erhalten. Diese Zeitleiste kann dann die forensischen Ermittlungen massiv erleichtern und beschleunigen, indem die riesige Menge an Informationen, die auf einem durchschnittlichen Computersystem gefunden wurden, korreliert werden. Plaso ist beispielsweise ein Framework, das initial von Kristinn Gudjonsson⁷ entwickelt wurde, und für die Erstellung von Super-Timelines angedacht ist. Bei beiden Analysemethoden besteht die Schwierigkeit, dass immer alle Änderungen von allen laufenden Prozessen auf dem Rechner protokolliert werden. Die Herausforderung besteht nun darin, alle Nebenläufigkeiten (Hintergrundrauschen) herauszufiltern, damit möglichst nur noch die relevanten Anwendungsspuren übrigbleiben. Das Hauptproblem ist bei der Ereignismethode genau umgekehrt, dort liegt die Schwierigkeit bei der Sicherstellung alle Ereignisse zu erfassen, die „nur“ zu einer bestimmten Aktion gehören. Bei einer Aufzeichnung mit einem ungeeigneten Filter gehen wichtige Spuren verloren oder indirekt verursachte Änderungen (Wiederverwendung von Funktionen anderer Programme) werden übersehen. Um diese Unschärfe möglichst gering zu halten, empfiehlt es sich in der Anwendungsforensik zur gegenseitigen Bestätigung der Resultate, beide Methoden einzusetzen. Hier haben wir andere Anwendungsfälle (Use Cases) resp. verfolgen andere Hauptziele. Damit eine forensische wirkungsvolle und gerecht werdende sowie aussagekräftige Untersuchung, basierend auf der Ereignismethode, durchgeführt werden könnte, fehlt die dafür notwendige Infrastruktur. Mit dieser realitätsentsprechenden Ausgangslage liegt das Hauptaugenmerk bei der effektiven Zustandsmethode. Bei möglichen Sicherheitsvorfällen liefert das betroffene Unternehmen zu Analyse Zwecken dem Forensiker oftmals auch nur die Festplattenabbilder aus. Jedoch ist dann unbedingt zu beachten, dass diese Zeitstempel verhältnismässig einfach verändert werden können. Es empfiehlt sich in Einzelfällen diese Zeitstempel als verlässliche Quelle für Zeitinformationen z. B. durch Abgleich

⁴Der Begriff MAC-Times bezieht sich auf die Zeitstempel der letzten Änderung mtime, der letzten geschriebenen Zugriffszeit atime oder der Änderung ctime einer bestimmten Datei. Typischerweise werden diese drei Zeitstempel auf den aktuellen Zeitpunkt gesetzt. POSIX-Systeme behalten die historische Interpretation von ctime als den Zeitpunkt, als bestimmte Dateimetadaten (letzte Änderung am Inode) wie z. B. Berechtigungen oder der Eigentümer, zuletzt geändert wurde. Seit der Einführung des Dateisystems Ext4 gibt es einen weiteren Zeitstempel crtime. Die crtime ist die „Geburt“ des Inodes im aktuellen Dateisystem und nicht der Datei. Demzufolge kann auch mittels Befehl `copy -p` beim Kopieren auf ein neues Dateisystem (Partition) nur atime und mtime auf den neu angelegten Inode übertragen. Weiter ist wichtig zu wissen, dass leider die Creation Time von verschiedenen Programmen, insbesondere von Editoren, unterschiedlich respektiert wird. Einige Editoren wie Geany oder Vim schreiben geänderte Dateien komplett neu, so dass die crtime gleichbedeutend mit mtime wird.

⁵Ein Inode (Index Node) [<https://de.wikipedia.org/wiki/Inode>] ist die grundlegende Datenstruktur zur Verwaltung von Dateisystemen mit Unix-artigen Betriebssystemen. Inodes sind das Äquivalent der MFT-Eintragsnummern in der Windows-Welt. Alles ist bekanntlich eine Datei und demnach wird jeder Datei eine eindeutige Inode-ID zugewiesen. Der Inode enthält alle notwendigen Metadaten über die Datei, einschliesslich ihres Typs und ihrer Berechtigungen sowie ihrer Grösse. Inodes enthalten keine Dateinamen, nur andere Dateimetadaten. Verzeichnisse sind Listen von Zuordnungsstrukturen, die jeweils einen Dateinamen und eine Inode-Nummer enthalten. Der Inode enthält auch Platz für 15 Zeiger, die die Position und Länge von Datenblöcken oder Extents im Dateiteil der Zylindergruppe beschreiben.

⁶MAC(B) Timestamps across POSIX implementations (Linux, OpenBSD, FreeBSD) [<https://medium.com/@quoscient/mac-b-timestamps-across-posix-implementations-linux-openbsd-freebsd-1e2d5893e4f1>]

⁷Cyber Security Interview von Kristinn Gudjonsson [<https://cybersecurityinterviews.com/episodes/045-kristinn-gudjonsson-dont-want-analysts-spending-time-extracting-data>]

mit Logdateien oder ähnlichen Dateien auf dem Datenträger selbst oder anderen Systemen gegen zu prüfen. Mit anderen Systemen verstehen wir verbundene und/oder voneinander abhängige Umsysteme aus der Applikations-Architektur. Damit möglichst alle Ereignisse erfasst werden und sie sich gegeneinander bestätigen, sind für alle Aktionen, wenn immer möglich und durchführbar, drei Untersuchungsdurchläufe geplant.

Initial nach der Fertigstellung des Betriebssystems (anapaya-base), über das bereits in den vorangegangenen Themenschwerpunkten und unter Abschnitt 4.1 detailliert gesprochen wurde, wird ein Abbild (init.raw) vom zu untersuchenden Dateisystem erzeugt. Dieses Abbild ist der Basisausgangspunkt, auf dem jeweils die geschilderten Aktionen nacheinander ausgeführt und untersucht werden. Die im Unterabschnitt 4.2.3 erwähnten Images sind folglich Snapshots der besprochenen Installations-, Konfigurations- und Härtungs-Massnahmen bis zum endgültigen SIX SCION Router-Image. Ein zweites sehr wichtiges Abbild wird für die Ermittlung des Hintergrundrauschens benötigt. Nach einem 15-minütigen Leerlaufbetrieb vom initialen Betriebssystem wird das System eingefroren und ein Speicherabbild (noise.raw) generiert. Ein Vergleich der beiden Abbildern bringt die Nebengeräusche „NOISE = noise.raw \ init.raw“ zum Vorschein. Die Nebengeräusche kommen jeweils im Nachgang der Gewinnung der Zustände nach der Aktionsausführung zum Abzug. Wir befinden uns nun wie unter Abschnitt 7.1 und im Unterabschnitt 7.1.1 angesprochen in der P-Phase. Für das bessere Verständnis, der geschilderten und noch folgenden Zusammenhänge zwischen den erhaltenen SCION-Images, den Aktionsmengen und Spurenabbildern, konsultieren sie bitte die Abbildung 7.1. Bei näherer Betrachtung fällt schon in unserem relativ kleinen Umfeld die zu analysierende grosse Datenmenge auf.

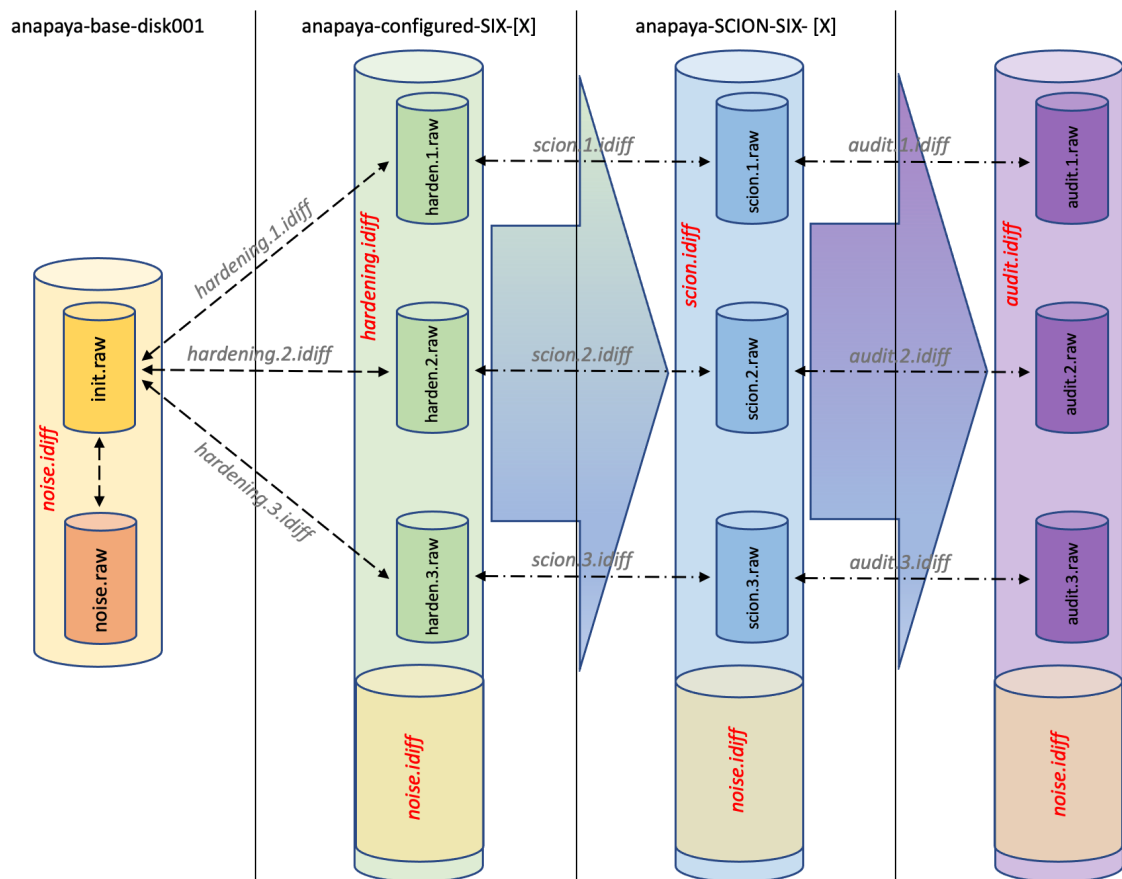


Abbildung 7.1.: Berechnung der Spurenmenge verknüpft zu den SCION-Images

Um verlässliche Endergebnisse zu erhalten, benötigt es bereits 11 Spurenabbilder. Je nach Anwendungsfall oder Sichtweise kommen die gewonnenen Spurenbilder zum Abzug. Ein strukturiertes Vorgehen schon in der Vorbereitungsphase, ist der erste Schritt zur erfolgreichen und integren Spurengewinnung. Für uns interessant sind vor allem die charakteristischen Spuren (CE). Die CE-Spuren können mathematisch mit der Formel „ $CE = (aktion.x.raw \setminus init.raw) \setminus noise.raw$ “ aufgezeigt werden. Schlussendlich ist die Assoziation der charakteristischen Spuren der zentrale Aspekt. Durch die Identifizierung, Klassifizierung und Individualisierung der digitalen Objekte wird versucht plausibel, die Assoziation herzustellen und eine Hypothese über unsere Ereignisse aufzustellen. In unserem Vorgehensmodell sollen gemeinsame charakteristische Spuren zwischen den geplanten Ereignissen und Kontraspuren allgemein nicht ausgewiesen und beschrieben werden. Das Ausweisen von Kontraspuren⁸ könnte bei der Rekonstruktion von unseren Ereignissen zwar von Relevanz sein, aber aufgrund der eher minderen Aussagekraft und kaum findenden Praxisrelevanz wird auf die Gewinnung von dieser Art von Spuren verzichtet. Der Sachverhalt sieht jedoch bei den gemeinsamen charakteristischen Spuren etwas anders aus. Bei Bedarf können und dürfen die charakteristischen und gemeinsamen charakteristischen Spuren grundsätzlich zusammengefasst werden, um eine Gesamtsicht über das Spurenbild einer bestimmten Aktion zu erhalten. Auch nach den durchgeführten Security Audits, möchten nur die CE-Spuren ausgewiesen werden. Nur so können wir sie kondensiert, hinsichtlich des SCION Installationszustandes und den erweiterten Sicherheitsauditest, ausweisen. Die dafür vorgesehene und angewendete Formel „ $CE = (aktion.x.raw \setminus [ZUSTAND_X].raw) \setminus noise.raw$ “ bleibt wie bei der CE-Formel faktisch bestehen. Der auffallende Unterschied liegt bei den „initialen“ Abbildern von „`init.raw`“ und „`[ZUSTAND_X].raw`“. Im „neuen“ Init sind z. B. die getätigten Aktionen wie das Hardening bereits inkludiert, da die einzelnen Konfigurations- oder Installationsspuren bei den Implementationsschritten nicht mehr erwünscht sind. Das heisst, dass wir bei unseren CE-Spurenberechnungen besonders acht geben müssen. Ansonsten könnte es passieren, dass die eigenen CE-Spuren wieder abgezogen oder fremde Spurenbilder nicht berücksichtigt werden. Sind erstmals in der GE-Phase die Spuren gewonnen, so geht es im darauffolgenden Schritt der sogenannten Prepare Evidence Phase (PE) darum, dass Spuren extrahiert und zur weiteren Verarbeitung formatiert werden. Auch hier wieder entsteht, pro Aktion und Durchlauf x jeweils eine Datei „`aktion.x.pe`“. Vor der letzten Phase folgt noch die Merge Evidence Phase (ME). Wie der Name es verrät, dient sie zur Vereinigung der Spuren pro Ereignis. Die in drei Durchläufen gesammelt Spuren, werden nun bereinigt und die Auftretungshäufigkeit gezählt. Für jedes Ereignis, sowie für das Hintergrundrauschen, besteht letztendlich eine gemeinsame Datei „`aktion.me`“ und „`noise.me`“. In der abschliessenden Characteristic Evidence Phase (CE) erfolgen, durch entfernen der Hintergrundgeräusche und gegebenenfalls der Spuren von anderen Aktionen, die Ermittlungen der gewünschten CE-Spuren. Es entstehen wieder pro Aktion eine Datei „`aktion.ce/se`“. Aus den 5-Phasen, resultiert das gewünschte Endresultat, mit den übriggebliebenen CE-Spuren pro Aktion.

Die geschilderte CE-Spurengewinnung stellt den Forensiker je nach angetroffener Konstellation immer wieder vor Herausforderungen. Diese aufwändigen und komplexen Spuren-Extraktionen erfolgten daher mittels bewährter forensischer Werkzeuge und mittels selbst entwickelten Python-Tools. Ohne unterstützende Massnahmen wären solche Analysen fast nicht durchführbar. Die Nachvollziehbarkeit der Resultate könnten nicht durchgängig gewährleistet werden, und geschweige denn, die Glaubwürdigkeit der darauf basierenden Herleitungen und Hypothesen. Unter dem nachfolgenden Unterabschnitt 7.1.4 werden daher noch auf die angetroffenen erschwerten Umstände und verwendeten Werkzeuge detailliert eingegangen.

⁸Die Kontraspuren erlauben im Wesentlichen die Ausführung bestimmter Aktionen auszuschliessen.

7.1.3. Berücksichtigte Spurenbilder

Anfangs dieser Arbeit, hauptsächlich während der Einarbeitungsphase, fanden einige Projektumfangsdiskussionen im Projektteam und mit den SCION Spezialisten statt. In der IT-Forensik können oftmals auch Spuren nach der Entfernung z. B. durch Löschen oder Deinstallieren einer Applikation von grossem Interesse sein. Bei Verdacht auf illegale Machenschaften mittels Hacker Tools, Malicious Code oder andere unterstützende Programme, möchte ein Forensiker immer gerne herausfinden, mit welchen Werkzeugen eine mögliche Tat erfolgte. Genau an diesem Punkt möchte zusätzlich angeknüpft und die Eruiierung des Spurenbildes nach einer SCION Deinstallation gleichzeitig ausgeklammert werden. Einerseits wurde dieses System bewusst für den SCION Betrieb ausgewählt und andererseits kennen wir anschliessend an die nachfolgenden forensischen Untersuchungen die SCION verursachten Spuren. Ein mir zugewiesener SCION Spezialisten teilte mir damals per E-Mail wie folgt mit: *Grundsätzlich vertreiben wir SCION als Produkt in einer Appliance, d.h. wir liefern das ganze Package: Hardware, OS und Software. Da macht es keinen Sinn danach die Software wieder zu entfernen, da niemand anderes auf dieser Hardware/OS Konfiguration etwas machen wird. Die OS Konfiguration an sich ist ja auch sehr spezifisch auf die SCION Software, welche darauf installiert wird, vorbereitet.* (Lukas Bischofberger, 3. Nov. 2020 um 17:50). Auch in Anbetracht eines potenziellen Rogue SCION Routers sähen wir diesbezüglich keinen relevanten Mehrwert. Durch die bereits verkörpernden und standardmässigen Sicherheitsfunktionalitäten von SCION selbst, zusammen mit dem Betrieb, in einer durchgängig gehärteten und überwachten SCION Infrastruktur, ist es praktisch ausgeschlossen einen böartigen oder ungewünschten SCION Router unbemerkt zu integrieren.

Auf einem System gibt es mehrere Bereiche, die Spuren zu vorherigen Systemaktivitäten oder versteckte Daten enthalten könnten. Das SCION System wurde seitens Anapaya direkt mittels einer Ubuntu-Image-Datei vorinstalliert und mittels einer SIX Konfigurationsvorlage (Ansible Script) konfiguriert. Der durchaus lauffähige und funktionierende SCION Router stand bisher noch nicht im Netzwerkbetrieb. Er transportierte daher noch keine produktive oder synthetische Daten über das Netzwerk. Somit war er auch noch nie lückenlos im SCION Kommunikationsprozess involviert. Bevor normalerweise mit einer Dateisystemanalyse begonnen werden kann, müsste eine detaillierte Datenträgeranalyse vorgängig stattfinden. Die Datenträgeranalyse gibt vor allem wichtige Informationen über bestehende, gelöschte oder versteckte Partitionen respektive Datenbereiche preis. Jegliche Inbetriebnahmevergänge erfolgten direkt in einer virtuellen Umgebung als VM. Wie schon einleitend erwähnt, konzentrieren wir uns hier, vor allem auf eine Post Mortem Analyse von Datenträgern und führen eine tiefgreifende Dateisystemanalyse durch. In unserem nachgestellten Fall handelt es sich nicht um einen Sicherheitsvorfall und wir dürfen uns darauf verlassen, dass sich beispielsweise keine versteckten oder verschlüsselten Partitionen auf dem Datenträger mit für uns relevanten Daten befinden. Partitionsänderungen fanden auch nicht statt und daher sind keine nicht-zugeordnete Speicherplätze (Unallocated Space) wie freier Laufwerks- oder Partitionslückenspeicher vorhanden. Der sogenannte Schlupfspeicher (File Slack Space) von ungenutztem Speicher in der allozierten Dateneinheit auf den Datenträgern könnten z. B. durch eine einfache String-Analyse untersucht werden. Des Weiteren wäre nach einem Sicherheitsvorfall unter anderem sinnvoll, in einem sehr aufwändigen Verfahren die nicht-allozierten und leeren Journalblöcke auf interessante Daten zu untersuchen. Grundsätzlich wird auch keine Wiederherstellung von Daten oder Inhaltsanalysen dieser angestrebt. Werden jedoch unerwartete Spurenbilder mit vertieftem Erklärungsbedarf aufgedeckt, so steht ihnen eine vertiefte Untersuchung zu. Mit unserer Konfiguration und unter den gegebenen Umständen, erscheinen die Aufwände gegenüber den potentiellen Analyseergebnissen, auf dem neu aufgesetzten SCION System, nicht gerechtfertigt zu sein. Selbstverständlich gäbe es auch noch weitere Verstecke⁹, die von forensischer Relevanz sein könnten, aber in unserer

⁹OSForensics™[<https://www.osforensics.com/hidden-areas-hpa-dco.html>] can discover and expose the Host Protected Area (HPA) and Device Configuration Overlay (DCO) hidden areas of a hard disk, which can be used for malicious intent including hiding illegal data.

Situation haben sie keine Bedeutung. Aus diesen Gründen werden die erwähnten Bereiche nicht ermittelt und gegebenenfalls untersucht.

7.1.4. Angewendete Werkzeuge mit ihren Eigenheiten

Wir haben in den vorangegangenen Kapiteln ausgiebig über die gewünschten Spurenbilder gesprochen. Hier wird gezielt auf die angewendeten Werkzeuge mit ihren besonderen Eigenheiten während der Spurengewinnung und den Analysen eingegangen. Damit soll das Vorgehen abschliessend verdeutlicht und begründet werden. Wie es in der IT-Forensik üblich ist, läuft nicht immer alles optimal und nach dem Lehrbuch. Es muss oftmals auf die besonderen Umstände mit angepassten Methoden und Vorgehensweisen gekontert werden. Somit dient es zusätzlich der vollständigen Nachvollziehbarkeit dieser Arbeit und den daraus resultierenden Hypothesen.

Als erstes werden für die forensischen Analysen nach der Spurenerzeugung in den unterschiedlichen Statis jeweils die Speicherabbilder benötigt. Diese Abbilder können in RAW-Format ganz einfach dank der virtuellen Infrastruktur mit der Funktion „clonemedium“ von VBoxManage gewonnen werden. Beim darauf folgenden Schritt, musste festgestellt werden, dass der direkte Dateisystemzugriff nicht ohne Weiteres gelangt. Scheinbar wurde der Dateisystemtyp nicht erkannt. Weitere Untersuchungen mit TSK MMLS, Test-Disk und FTK Imager ergaben etwas mehr Klarheit über die Sachlage. Wie in der Abbildung 7.2 ersichtlich sind mehrere nicht zugewiesene Bereiche und Partitionen vorhanden.

```

dfxml@dfxml: /media/sf_host_ssd_share/iddiff
File Edit View Search Terminal Help
dfxml@dfxml:/media/sf_host_ssd_share/iddiff$ mmls init.raw
DOS Partition Table
Offset Sector: 0
Units are in 512-byte sectors

   Slot   Start      End      Length    Description
000: Meta   0000000000  0000000000  0000000001  Primary Table (#0)
001: ----- 0000000000  0000002047  0000002048  Unallocated
002: 000:000 0000002048  0000999423  0000997376  Linux (0x83)
003: ----- 0000999424  0001001471  0000002048  Unallocated
004: Meta   0001001470  0134215679  0133214210  DOS Extended (0x05)
005: Meta   0001001470  0001001470  0000000001  Extended Table (#1)
006: 001:000 0001001472  0001003519  0000002048  Linux (0x83)
007: Meta   0001003520  0134215679  0133212160  DOS Extended (0x05)
008: Meta   0001003520  0001003520  0000000001  Extended Table (#2)
009: ----- 0001003520  0001005567  0000002048  Unallocated
010: 002:000 0001005568  0134215679  0133210112  Linux Logical Volume Manager (0x8e)
011: ----- 0134215680  0134217727  0000002048  Unallocated
dfxml@dfxml:/media/sf_host_ssd_share/iddiff$ fsstat -o 1001470 init.raw
Cannot determine file system type
dfxml@dfxml:/media/sf_host_ssd_share/iddiff$ fsstat -f ext4 -o 1001470 init.raw
Invalid magic value (not an EXT4FS file system (magic))
dfxml@dfxml:/media/sf_host_ssd_share/iddiff$

```

Abbildung 7.2.: TSK mmls - Layout der Festplatten Partitionen

Eine andere und vermeintlich genauere oder verlässlicherer Sicht auf das Abbild liefert das Partitionierungsprogramm „fdisk“. In der Abbildung 7.3 sind die Partitionsinformationen veranschaulicht. Zudem scheint ein Logical Volume Manager (LVM) installiert zu sein, der die forensischen Analysen vorerst verhindert. Der LVM führt eine höhere Abstraktionsschicht ein und ermöglicht eine flexible und einfachere Verwaltung von Datenspeichern eines Computersystems. Die physischen Volumes werden zu logischen Volume-Gruppen zusammengefasst, die ihrerseits in logische Volumes unterteilt werden können, die Einhängpunkte und einen Dateisystemtyp wie z. B. Ext4 haben. Diese administrative Vereinfachung von mehreren Festplatten führte zu einer ersten forensischen Hürde.

```
dfxnl@dfxnl:/media/sf_host_ssd_share$ file scion.1.raw
scion.1.raw: DOS/MBR boot sector
dfxnl@dfxnl:/media/sf_host_ssd_share$ fdisk -l scion.1.raw
Disk scion.1.raw: 64 GiB, 68719476736 bytes, 134217728 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xd4c5f80b

Device      Boot  Start      End  Sectors  Size Id Type
scion.1.raw1 *    2048    999423   997376  487M 83 Linux
scion.1.raw2          1001470 134215679 133214210  63,5G  5 Extended
scion.1.raw5          1001472 1003519    2048    1M 83 Linux
scion.1.raw6          1005568 134215679 133210112  63,5G 8e Linux LVM
dfxnl@dfxnl:/media/sf_host_ssd_share$
```

Abbildung 7.3.: fdisk - Layout der Festplatten Partitionen

Zusätzliche und erschwerende sowie zeitraubende forensische Eingriffe mussten erfolgen. Es gibt mehrere Vorgehensvarianten in solchen Fällen. Auch hier muss Situationsgerecht entschieden werden. Eine Lösung wäre, die Zuweisungen aus der LVM-Partitionstabelle zu erstellen und im Read-Only-Mode an Loopback-Geräten zuzuordnen, so dass sie die Dateisystemstruktur für die Festplatten bilden. Kpartx (siehe Abbildung 7.4) übernimmt in unserem Fall die automatische Zuordnungen der Partitionsgeräte ohne die Partitions-Offsets angeben zu müssen.

```
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo kpartx -rav scion.1.raw
add map loop17p1 (253:0): 0 997376 linear 7:17 2048
add map loop17p2 (253:1): 0 2 linear 7:17 1001470
add map loop17p5 (253:2): 0 2048 linear 7:17 1001472
add map loop17p6 (253:3): 0 133210112 linear 7:17 1005568
dfxnl@dfxnl:/media/sf_host_ssd_share$
```

Abbildung 7.4.: Kpartx - Loopback-Geräten-Zuordnung der Partitionen

Abschliessend werden sie wie in den Abbildung 7.5 gezeigt, mit den dafür vorgesehenen LVM-Tools, schreibgeschützt für den Dateizugriff und die forensische Analyse eingebunden.

```
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo pv
PV          VG      Attr PSize  PFree
/dev/mapper/loop17p6 anapaya-vg lvm2 a-- <63,52g 3,91g
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo vgscan
Reading volume groups from cache.
Found volume group "anapaya-vg" using metadata type lvm2
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo vgchange -a y anapaya-vg
2 logical volume(s) in volume group "anapaya-vg" now active
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo ls /dev/anapaya-vg/
root swap 1
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo file -sl /dev/anapaya-vg/root
/dev/anapaya-vg/root: Linux rev 1.0 ext4 filesystem data, UUID=34de4266-1c2d-47ce-8ec9-2e26c24a0474 (extents) (64bit) (large files) (huge files)
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo mkdir /mnt/scion_1_root
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo mount -o ro /dev/anapaya-vg/root /mnt/scion_1_root
mount: /mnt/scion_1_root: /dev/mapper/anapaya-vg-root already mounted on /mnt/scion_1_root.
dfxnl@dfxnl:/media/sf_host_ssd_share$ ls /mnt/scion_1_root/
bin boot dev etc home initrd.img initrd.img.old lib lib64 lost+found media mnt opt proc root run/sbin srv sys usr var vmlinuz vmlinuz.old
dfxnl@dfxnl:/media/sf_host_ssd_share$
```

Abbildung 7.5.: LVM2 - Einbindung der Partitionen

Ein anderer Weg ist das Herauslösen der einzelnen EXT4-Datenpartition. Dieser Weg wurde hier bewusst zusätzlich eingeschlagen, da wir im Vorfeld einige Abgrenzungen getroffen haben, es forensisch verantworten können und die meisten forensischen Tools (Encase, FTK, TSK usw.) die Daten nicht aus einem LVM-Raw-Image herauslesen können. Sie können zwar den Dateityp korrekt als LVM (technisch gesehen „LVM2“ oder „Typ 8e“) identifizieren, aber sie können die verschiedenen Dateien nicht wieder zu einem einzigen Volume zusammenfügen. Das Mounten eines intakten Dateisystems oder als ein ganzes forensisches Image zu erstellen, ist leider noch nicht möglich. In unserem Fall nicht weiter tragisch oder problematisch. Der Nachteil, an diesem Vorgehen ist ganz klar, dass wir hier die SWAP-Partition „anapaya-vg-swap“ nicht einbinden und analysieren können. Würden noch weitere Datenpartitionen bestehen, so müssten auch diese separat herausgelöst werden. Wie sie sich aus den vorangehenden Themenschwerpunkten dem Security Hardening bestimmt erinnern, ist in manchen Bereichen eine Separierung auf unterschiedlichen Festplatten oder logischen Partitionen wie z. B. für die Log-Dateien und Containers empfehlenswert und sinnvoll.

Unter diesen Umständen, kommt uns dies entgegen und erleichtert etwas die Vorbereitungen. Die forensischen Programme wie „fiwalk“ und „idifference2“¹⁰ sind für die geschilderte automatisierte Auswertung (Vergleich von zwei Festplattenabbildern) geeignet und sollen bei Möglichkeit für die anstehenden Analysen eingesetzt werden. Wie erwünscht, vergleicht es zwei Dateisystemabbildern und gibt eine Datei „.idiff“ mit den Veränderungen aus. Pro Aktion und Durchlauf x entsteht jeweils eine Datei „aktion.x.idiff“. Dieses Tool ist wie bereits erwähnt auf der Forensik-Workstation „DFXML“ vorinstalliert. Während der Studienzeit konnten einige gute Erfahrungen damit gemacht werden und dürfte unseren Anforderungen gerecht werden.

Insbesondere im Bereich der Postmortem-Forensik von Dateisystemen, spielt die Rekonstruktion von verlorenen oder gelöschten Dateien eine grosse Rolle. Uns interessiert nicht den Inhalt, da uns dieser in den Images bereits vorliegt. Die Information über Dateien und Verzeichnisse, welche nicht mehr vorhanden sind, reichen vollkommen aus. Die Techniken, die zu diesem Zweck eingesetzt werden können, hängen stark von den Besonderheiten des jeweiligen Dateisystems ab. SCION benutzt wie bekannt das aktuellste Dateisystem Ext4, das seit dem Linux 2.6.28 Kernel im Oktober 2008 offiziell als stabil deklariert wurde und auf den aktuellen Ubuntu-Versionen standardmässig läuft. Für die gut erforschten Vorgänger Dateisysteme Ext2/3 gibt es eine Vielzahl von verlässlichen und bewährten Tools, um forensische oder informative Dateisystemanalysen zu fahren. Doch gibt es immer noch Tools, die das Ext4-Dateisystem nicht verlässlich unterstützen. Das Programm „debugfs“¹¹ ist ein interaktiver Dateisystem-Debugger. Obwohl es offiziell den Zustand eines Ext2-, Ext3- oder Ext4-Dateisystems untersuchen kann, unterstützt es z. B. den Befehl „sudo debugfs -R 'lsdel' /dev/anapaya-vg/root“ nicht. Dieser Befehl war nützlich für die Anzeige und Wiederherstellung von gelöschten Dateien bei Ext2-Dateisystemen. Leider ist es für diesen Zweck nicht mehr nützlich, wenn die Dateien mit Ext3 oder Ext4 gelöscht wurden, da die Datenblöcke der Inodes seither nicht mehr zur Verfügung stehen, nachdem der Inode freigegeben wurde. In forensischen Untersuchungen können auch solche Informationen sehr hilfreich sein und interessante Anhaltspunkte liefern. Wie die Beispielsauswertung in der Abbildung 7.6 zeigt, fanden die Modifikationen resp. SCION-Einrichtungen mit hoher Wahrscheinlichkeit nur morgens und nachmittags am 29. Okt. 2020 zwischen 10:00 und 16:00 Uhr statt. Dieses Indiz wird in den weiteren Analysen mitberücksichtigt.

Im Falle eines Ext-Dateisystems ist die Interpretation des sogenannten Superblocks essenziell, um die Daten zu interpretieren. Wie seine Vorgänger speichert Ext4 die Metadaten im sogenannten Superblock oder in der Group Descriptor Table. Ohne diese Metadatenstrukturen ist es schwierig, das Dateisystem richtig zu interpretieren und die Daten zu rekonstruieren. Das Ext4-Dateisystem kann hauptsächlich mit den Werkzeugen und Techniken analysiert werden, die für seinen Vorgänger Ext3 entwickelt wurden, da die meisten Prinzipien und internen Strukturen unverändert geblieben sind. Wir können und dürfen hier einen intakten Superblock und eine Group Descriptor Table annehmen. Als Randbemerkung möchte erwähnt werden, dass einige Neuerungen bei Ext4¹² implementiert wurden, die bei der Wiederherstellung von Dateien berücksichtigt werden müssen. Vor einigen Jahren entwickelte Andreas Dewald[13] im Hinblick auf die forensische Dateiwiederherstellung einen neuartigen Ansatz, um Dateien in einem Ext4-Dateisystem auch dann zu identifizieren, wenn der Superblock beschädigt oder überschrieben ist. Der Ansatz wendet heuristische Suchmuster zur Nutzung von Methoden des File Carving an und kombiniert diese mit der Analyse von Metadaten. Im berühmten Sleuthkit (TSK) Framework wurde er bereits integriert. Weitere Informationen können gerne dem referenzierten Artikel entnommen werden.

¹⁰Digital Forensics XML Project [<https://github.com/simsong/dfxml>]

¹¹The debugfs [<https://man7.org/linux/man-pages/man8/debugfs.8.html>] program is an interactive file system debugger. It can be used to examine and change the state of an ext2, ext3, or ext4 file system.

¹²Vorteile im Vergleich zu Ext3 [https://www.thomas-krenn.com/de/wiki/Ext4_Dateisystem]

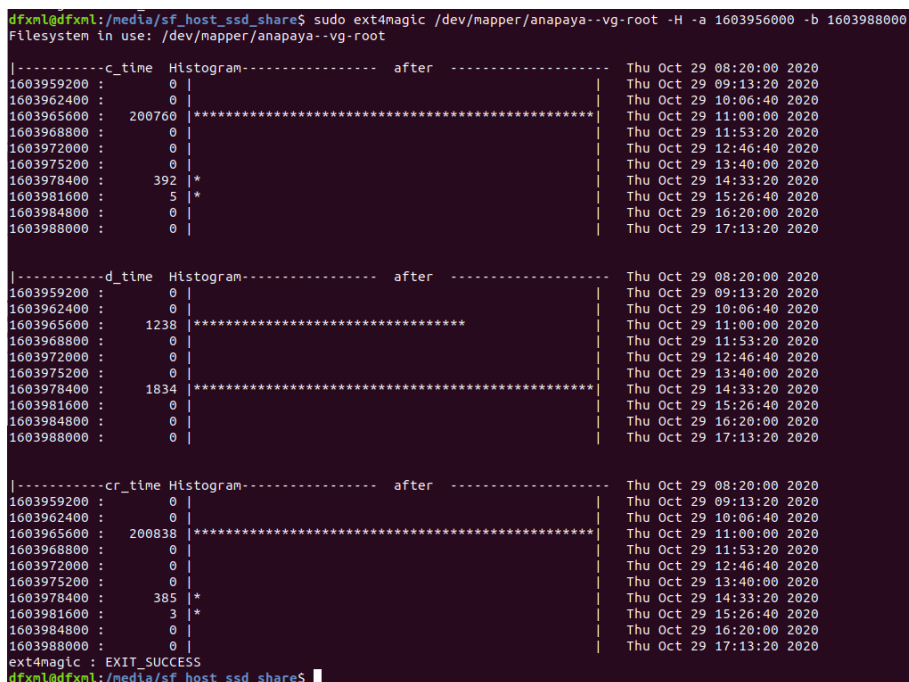


Abbildung 7.6.: Ext4magic - Histogramm von gelöschten Dateien

Eine weitere sehr wichtige Eigenheit von Ext4 ist das Metadaten-Journaling¹³. Alle Änderungen werden vor dem eigentlichen Schreiben in einem dafür reservierten Speicherbereich dem sogenannten Journal protokolliert. Der daraus resultierende Performancenachteil ist durch die erreichten Vorteile zu vernachlässigen. Gerade bei Systemabstürzen sollte es einen Vorteil bieten, denn zu jedem Zeitpunkt sollte es möglich sein, trotz Unterbrechung von Schreibvorgängen, einen konsistenten Datenzustand zu rekonstruieren. Während der GE-Phase musste festgestellt werden, dass durch den geschilderten Prozess mittels Clonemedium die Speicherabbildergewinnung teilweise nicht erfolgreich gelang. Wie die Abbildung 7.7 veranschaulicht, kam uns hier das Journaling in die Quere und verunmöglichte das Einbinden der logischen Volume-Gruppen.

```
dfxnl@dfxnl:/media/sf_host_ssd_share$ file audit.1.raw
audit.1.raw: DOS/MBR Boot sector
dfxnl@dfxnl:/media/sf_host_ssd_share$ fdisk -l audit.1.raw
Disk audit.1.raw: 64 GiB, 68719476736 bytes, 134217728 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0xd4c5f80b

Device      Boot  Start    End  Sectors  Size Id Type
audit.1.raw1 *    2048    999423   997376   487M 83 Linux
audit.1.raw2          1001470 134215079 133214210 63.5G 5 Extended
audit.1.raw5          1001472   1003519    2048    1M 83 Linux
audit.1.raw6          1005568 134215079 133210112 63.5G 8e Linux LVM
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo kpartx -rav audit.1.raw
add map loop17p1 (253:0): 0 997376 linear 7:17 2048
add map loop17p2 (253:1): 0 2 linear 7:17 1001470
add map loop17p5 (253:2): 0 2048 linear 7:17 1001472
add map loop17p6 (253:3): 0 133210112 linear 7:17 1005568
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo pvs
pvs
pvs scan
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo pvs
PV          VG          Fmt Attr PSize  PFree
/dev/mapper/loop17p6 anapaya-vg lvm2 a-- <63.52g 3,91g
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo vgs
vgs
vgs scan  vgsplit
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo vgscan
Reading volume groups from cache.
Found volume group "anapaya-vg" using metadata type lvm2
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo vgchange -a y anapaya-vg
2 logical volume(s) in volume group "anapaya-vg" now active
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo ls /dev/anapaya-vg/
root swap_1
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo file -sL /dev/anapaya-vg/root
/dev/anapaya-vg/root: linux rev 1.0 ext4 filesystem data, UUID=34de4266-1c2d-47ce-86c8-2a26c24a0474 (needs journal recovery) (extents) (64bit) (large files) (huge files)
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo mount -o ro /dev/anapaya-vg/root /mnt/audit_1_root
mount: /mnt/audit_1_root: Can't read superblock on /dev/mapper/anapaya--vg-root.
dfxnl@dfxnl:/media/sf_host_ssd_share$
```

Abbildung 7.7.: Volume Group Mounting - needs journal recovery

¹³Journaling-Dateisystem [https://de.wikipedia.org/wiki/Journaling-Dateisystem]

Die Meldung „needs journal recovery“ bedeutet, dass das Dateisystem nicht sauber ausgehängt wurde oder noch eingehängt zu sein scheint. Ein solches Verhalten kann auch bei einem Rechnerabsturz beim gerade Einhängen bedeuten. Falls erforderlich wird die Journalwiederherstellung automatisch, beim nächsten Systemneustart oder sobald das Dateisystem wieder eingehängt wird, durchgeführt. Ist ein Systemneustart oder eine Wiedereinhängung im ReadWrite-Modus nicht möglich oder erwünscht, dann könnte gegebenenfalls das uneingehängte Dateisystem mit dem Boardmittel bezüglich File System Check „e2fsck“ repariert werden. Bei jeder Aktion verändert sich grundsätzlich das Systembild und dadurch natürlich auch die Spurenbilder. Es muss immer versucht werden, keine Spuren zu verwischen oder auf dem kleinstmöglichen Schaden zu halten. Deshalb wurde zuerst versucht, die LVM-Partition zu reparieren. Wie in der Abbildung 7.8 ersichtlich jedoch leider ohne Erfolg. Daraufhin musste entschieden werden, den eingefrorenen, virtuellen SCION-Router aus seinem Tiefschlaf zu erwecken und herunterzufahren. Zum direkten Vergleich wurde zusätzlich der etwas optimalere und spurenschonendere Ansatz gewählt. In diesem Vorgehen wurde lediglich die herausgelöste Daten-Partition mit der dafür notwendigen Schreibberechtigung gemountet. Mit beiden Ansätzen konnte schliesslich das Betriebssystem das Journal sauber herschreiben und ein neues und funktionierendes Speicherabbild gewonnen werden. Diese Situation zeigt es wieder deutlich, wie schnell und manchmal unverhofft die Post-Mortem-Analysen erschwert oder teilweise sogar verunmöglich wird. Wenn immer möglich, folgt daher zusätzlich eine Untersuchung des Live-Systems. Sie fragen sich jetzt bestimmt, warum es so wichtig war, eine funktionierende logische Volume-Gruppe zu haben, da alle benötigten Datenpartitionen als Speicherabbilder aus der LVG herausgelöst wurden und zu Analysezwecken vorlagen. Das ist eine berechtigte und nachvollziehbare Frage. Die Analysen im aktuellen TSK Autopsy ergaben bei diesen Abbildern während der Generierung der Timeline einen Fehler. Auch Autopsy nutzt fremde Module und daher stammt der Fehler vom Plaso der IngestModules.


```

dfxnldfxnl:/media/sf_host_hdd_shares$ lsblk
NAME                                MAJ:MIN RM  SIZE RO TYPE MOUNTPOINT
loop0                              7:0      0   2,5M  1 loop /snap/gnome-calculator/884
loop1                              7:1      0 1008K  1 loop /snap/gnome-logs/61
loop2                              7:2      0 55,5M  1 loop /snap/core18/1988
loop3                              7:3      0    4M  1 loop /snap/gnome-calculator/406
loop4                              7:4      0 276K  1 loop /snap/gnome-characters/570
loop5                              7:5      0 276K  1 loop /snap/gnome-characters/708
loop6                              7:6      0 548K  1 loop /snap/gnome-logs/103
loop7                              7:7      0 149,9M 1 loop /snap/gnome-3-28-1804/67
loop8                              7:8      0 55,5M  1 loop /snap/core18/1997
loop9                              7:9      0 162,9M 1 loop /snap/gnome-3-28-1804/145
loop10                             7:10     0 88,5M  1 loop /snap/core/7270
loop11                             7:11     0  2,2M  1 loop /snap/gnome-system-monitor/157
loop12                             7:12     0 219M  1 loop /snap/gnome-3-34-1804/66
loop13                             7:13     0 42,8M  1 loop /snap/gtk-common-themes/1313
loop14                             7:14     0  3,7M  1 loop /snap/gnome-system-monitor/100
loop15                             7:15     0 64,8M  1 loop /snap/gtk-common-themes/1514
loop16                             7:16     0 99,2M  1 loop /snap/core/10958
loop17                             7:17     0   52G  0 loop
loop18                             7:18     0   64G  0 loop
  loop18p1                         253:0     0 487M  0 part
  loop18p2                         253:1     0    1K  0 part
  loop18p5                         253:2     0    1M  0 part
  loop18p6                         253:3     0 63,5G  0 part
    anapaya--vg-root               253:4     0   52G  0 lvm
    anapaya--vg-swap_1             253:5     0    7,6G  0 lvm
sda                                8:0      0   10G  0 disk
└─sda1                             8:1      0   10G  0 part /
sr0                                11:0     1 1024M  0 rom
dfxnldfxnl:/media/sf_host_hdd_shares$ sudo lvscan
ACTIVE          '/dev/anapaya-vg/root' [51,97 GiB] inherit
ACTIVE          '/dev/anapaya-vg/swap_1' [<7,63 GiB] inherit
dfxnldfxnl:/media/sf_host_hdd_shares$ sudo fsck.ext4 -fy /dev/anapaya-vg/root
e2fsck 1.44.1 (24-Mar-2018)
/dev/anapaya-vg/root: recovering journal
Superblock needs_recovery flag is clear, but journal has data.
Run journal anyway? yes

fsck.ext4: Unknown code ____ 251 while recovering journal of /dev/anapaya-vg/root
fsck.ext4: unable to set superblock flags on /dev/anapaya-vg/root

/dev/anapaya-vg/root: ***** WARNING: Filesystem still has errors *****
dfxnldfxnl:/media/sf_host_hdd_shares$ sudo e2fsck -fy /dev/anapaya-vg/root
e2fsck 1.44.1 (24-Mar-2018)
/dev/anapaya-vg/root: recovering journal
Superblock needs_recovery flag is clear, but journal has data.
Run journal anyway? yes

e2fsck: Unknown code ____ 251 while recovering journal of /dev/anapaya-vg/root
e2fsck: unable to set superblock flags on /dev/anapaya-vg/root

/dev/anapaya-vg/root: ***** WARNING: Filesystem still has errors *****
dfxnldfxnl:/media/sf_host_hdd_shares$ sudo tune2fs -l /dev/anapaya-vg/root | egrep -i "mount count|Check interval|Last|Next"
Last mounted on: /
Last mount time: Mon Mar 29 19:03:49 2021
Last write time: Mon Mar 29 19:03:49 2021
Mount count: 7
Maximum mount count: -1
Last checked: Thu Oct 29 10:08:36 2020
Check interval: 0 (<none>)
dfxnldfxnl:/media/sf_host_hdd_shares$ sudo dumpe2fs /dev/anapaya-vg/root | grep -i backup
dumpe2fs 1.44.1 (24-Mar-2018)
Journal backup: inode blocks
Backup superblock at 32768, Group descriptors at 32769-32775
Backup superblock at 98304, Group descriptors at 98305-98311
Backup superblock at 163840, Group descriptors at 163841-163847
Backup superblock at 229376, Group descriptors at 229377-229383
Backup superblock at 294912, Group descriptors at 294913-294919
Backup superblock at 819200, Group descriptors at 819201-819207
Backup superblock at 884736, Group descriptors at 884737-884743
Backup superblock at 1605632, Group descriptors at 1605633-1605639
Backup superblock at 2654208, Group descriptors at 2654209-2654215
Backup superblock at 4096000, Group descriptors at 4096001-4096007
Backup superblock at 7962624, Group descriptors at 7962625-7962631
Backup superblock at 11239424, Group descriptors at 11239425-11239431
dfxnldfxnl:/media/sf_host_hdd_shares$ sudo e2fsck -b 32768 /dev/anapaya-vg/root
e2fsck 1.44.1 (24-Mar-2018)
Superblock needs_recovery flag is clear, but journal has data.
Recovery flag not set in backup superblock, so running journal anyway.
/dev/anapaya-vg/root: recovering journal
Superblock needs_recovery flag is clear, but journal has data.
Recovery flag not set in backup superblock, so running journal anyway.
e2fsck: Unknown code ____ 251 while recovering journal of /dev/anapaya-vg/root
Superblock needs_recovery flag is clear, but journal has data.
Recovery flag not set in backup superblock, so running journal anyway.
e2fsck: unable to set superblock flags on /dev/anapaya-vg/root

/dev/anapaya-vg/root: ***** FILE SYSTEM WAS MODIFIED *****
/dev/anapaya-vg/root: ***** WARNING: Filesystem still has errors *****

```

Abbildung 7.8.: File System Check - Dateisystem-Reparatur

Plaso bereitet seine Daten in einer SQLite v3 Datenbank auf und verarbeitet sie mit der Anwendung „psort“ weiter. Psort wird hauptsächlich für die richtige Timeline-Sortierung der Daten benötigt. Da der Fehler für Autopsy nicht eruiert und behoben werden konnte, wurde aus Konsistenzgründen entschieden, die wichtigen Timelines mittels der damals brandaktuellen Plaso-Suite¹⁴ auf der Ubuntu-Forensik-Workstation zu erstellen und auszuwerten. Diese Auswertungen liefen dank der zusätzlich gewählten Methode ohne jegliche Fehlermeldungen erfolgreich durch. Die Timeline benötigen wir also zur Bestätigung resp. Festigung der aufgefundenen Spurenbilder aus den Festplattenanalysen. Das kommt uns später direkt wieder zugute, da in der GE-Phase während den Aufbereitungen der Spurenbilder weitere Ungereimtheiten auftauchten. Fiwalk ist selbst Teil vom bekannten SleuthKit und mit Hilfe von TSK-Bibliotheken verarbeitet es die zu untersuchenden Speicherabbilder und gibt die Ergebnisse im gewünschten DFXML-Format (z. B. XML, ARFF oder TXT) aus. Fiwalk liest also alle Dateien und Inodes mit den forensisch relevanten Metadaten aus und bereitet einen Report für die weitere Verarbeitung auf. Im zweiten Verarbeitungsschritt wird dann versucht die Unterschiede zweier zeitversetzten Images auszuweisen. Das erwähnte Python-Skript „Idifference2“ besitzt diese Funktion und vergleicht zwei Fiwalk-Reporte oder direkt zwei zeitversetzte Speicherabbilder miteinander. Idifference2 ruft bei einem direkten Speichervergleich Fiwalk selbst auf. Der Unterschied präsentiert sich dann wie schon angedeutet pragmatisch in einer Textdatei mit der selbst gewählten Endung „.idiff“. Mit der aktuellen Version wird ein Vergleich von zwei Fiwalk-Reporte nicht mehr unterstützt, also musste auf die zweite Vorgehensvariante gewechselt werden. Anhand der Idifference2-Logging-Informationen konnten fast alle Speicherabbilder wie in der Abbildung 7.1 veranschaulicht gegeneinander ausgewertet werden. Jedoch schlugen alle Auswertungen zwischen den Speicherabbildern `hardening.x.raw` und `scion.x.raw` fehl.

```
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo python3.6 /home/dfxnl/tools/dfxnl/python/Idifference2.py hardening.1.001 scion.1.001 > /media/sf_host_hdd_share/scion.1.idiff
[sudo] password for dfxnl:
INFO:Idifference2.py: Reading hardening.1.001.
INFO:Idifference2.py: Reading scion.1.001.
WARNING:make_differential_dfxml.py:Multiple instances of the file path 'var/lib/docker/overlay2/1de9784217a10614eeff14d3c9b1429b4aad41b425c4483396c797e816637dc4-init/diff/
.dockerenv' were found in partition 1; this violates an assumption of this program, that paths are unique within partitions.
WARNING:make_differential_dfxml.py:Multiple instances of the file path 'var/lib/docker/overlay2/2a9060be0278d13b02d742eece005e475dfcc745537217dfa625eda10a3acc4/work/work'
were found in partition 1; this violates an assumption of this program, that paths are unique within partitions.
WARNING:make_differential_dfxml.py:Multiple instances of the file path 'var/lib/docker/overlay2/f1e48c9de91eb9358050669da5873baf91d968b16e8dd22e70153eef676e027e/work/work'
were found in partition 1; this violates an assumption of this program, that paths are unique within partitions.
Traceback (most recent call last):
  File "/home/dfxnl/tools/dfxnl/python/Idifference2.py", line 112, in <module>
    timesten=args.timestenp
  File "/home/dfxnl/tools/dfxnl/python/summarize_differential_dfxml.py", line 206, in report
    deleted_files.sorted = sorted(deleted_files, key=sorkey_single())
TypeError: '<' not supported between instances of 'NoneType' and 'str'
```

Abbildung 7.9.: Idifference2 - Fehlermeldung in „deleted_files_sorted“

Genauerer Fehleranalysen anhand der Fehlermeldung (siehe Abbildung 7.9) deuteten nicht nur auf Probleme in der Sortierfunktion im Bereich der gelöschten Dateien hin. Nur dieser Analysebereich und ausschliesslich in den Rohdaten der SCION-Images schienen auf den ersten Blick betroffen zu sein. Da nicht auf diese Art von Auswertung verzichtet werden konnte, erfolgten aufwändige manuelle Datenanalysen an eingehängten SCION-Speicherabbildern und an zusätzlich erstellten Fiwalk-Reporten. Die stichprobenartigen Checks widerlegten unter anderem, die befürchteten Herausforderungen mit der Fiwalk-Kompatibilität im Zusammenhang mit dem Ext4-Dateisystem¹⁵. Alle Inode-Metadaten werden korrekt und konsistent im Fiwalk-Report abgelegt. Die Herausforderungen liegen also devinitiv nicht bei den vorliegenden Rohdaten oder an der Fiwalk-Anwendung. Die fundamantalen Basisvoraussetzungen wurden bewiesen und sind gegeben. Alles deutet auf einen Programmfehler im renommierten Idifference2 oder in den abhängigen Funktionen/Bibliotheken hin. Eine Ablösung von Idifference2 durch ein selbst entwickeltes Tool erschien als nicht gerechtfertigt, da die Komplexität bei den Metadatenauswertungen als beträchtlich und fehleranfällig angesehen wird. Eine zielführende alternative Softwarelösung scheint es nicht zu geben. Bei Überlegungen und gründlicher Abwägung wie integer und authentisch die aufbereiteten Daten bei der Implementierung eines Workarounds in Idifference2 noch sein mögen, erschienen als handhabbar und vertret-

¹⁴Plaso-20210412 GitHub [https://github.com/log2timeline/plaso/releases]

¹⁵Ext4 Disk Layout [https://ext4.wiki.kernel.org/index.php/Ext4_Disk_Layout]

bar. Solange die Ursache der Missinterpretationen plausibel aufgezeigt und erklärt werden können, sowie die Integrität der Spuren gewährleistet wird, steht diesem weiteren Vorgehen nichts im Wege. Im Image-Vergleich sind die Zeiten noch nicht von Interesse und Relevanz, darum wurde bewusst auf die Sortierung im Bereich „Deleted Files“ verzichtet und in der Hilfsfunktion „summarize_differential_dfxml.py“ ausgeklammert. Die Abbildung 7.10 zeigt einen Teilausschnitt der Hilfsfunktion mit dem implementierten und pragmatischen Workaround.

```
idifference.h2("Deleted files:")
# deleted_files_sorted = sorted(deleted_files, key=_sortkey_singlefi())
deleted_files_sorted = deleted_files
res = [
    obj.original_fileobject.mtime,
    obj.original_fileobject.filename or "",
    obj.original_fileobject.filesize
] for obj in deleted_files_sorted
idifference.table(res)

def _sortkey_renames():
    def _key_by_path(fi):
        return (
            fi.original_fileobject.filename or "",
            fi.filename or "",
            str(fi.mtime) or "",
            str(fi.original_fileobject.mtime) or ""
        )
    def _key_by_times(fi):
        return (
            str(fi.mtime) or "n/a",
            str(fi.ctime) or "n/a",
            str(fi.atime) or "n/a",
            str(fi.dtime) or "n/a",
            str(fi.crttime) or "n/a",
```

Abbildung 7.10.: Summarize Differential - Abschaltung der Sortierfunktion

Zuvor wurde das Analyseproblem mit „vermeintlich“ umschrieben. Das hatte der Grund, weil weitere Dateisystemanalysen zum Beweis der Spurenintegrität resp. Darlegung der Ursache weitere Fragen aufgeworfen haben. Die ausgewiesenen Dateisystem-Differenzen auch im Bereich „New Files“ schienen das Phänomen der zeitstempellosen Spuren aufzuweisen. Jedoch wird, wie die Abbildung 7.11 zeigt, als Zeitstempel ein „n/a“ für not available vermerkt.

```
dfxml@dfxml:/media/sf_host_ssd_share$ sed -n '/New files/, $p' ./idiff/original/scion.1.idiff | grep '^n/a'
n/a var/lib/dpkg/info/process-exporter.prerm
n/a var/lib/dpkg/info/python.md5sums
n/a var/lib/dpkg/info/python3-distupgrade.md5sums
```

Abbildung 7.11.: Idifference2 - Ausschnitt „New files“ der fehlenden Zeitangaben

Diese Funktion scheint bei den gelöschten Dateien nicht richtig zu funktionieren, da bei diesem Platzhalter (siehe Abbildung 7.12) nichts hinzugefügt und eine Sortierung verständlicherweise verunmöglicht wird. Das ist auch der Hauptgrund, weshalb das Idifference2 mit einer Fehlermeldung abbricht. Nachfolgend einige Bildausschnitte mit den geschilderten Widersprüchen und Erklärungen. Sie treten meistens dann auf, wenn kein Zeitstempel ausgelesen werden konnte.

```

dfxnl@dfxnl:/media/sf_host_ssd_share$ sed -n '/Deleted files/, $p' ./idiff/original/scion.1.idiff | grep $'^\t'
var/lib/dpkg/info/amd64-microcode.postrm
var/lib/dpkg/info/fuse.conf.files
var/lib/dpkg/info/perl.postinst
var/lib/dpkg/info/unattended-upgrades.md5sums
var/lib/dpkg/info/fuse.md5sums
var/lib/dpkg/info/popularity-contest.config
var/lib/dpkg/info/taskel.list
var/lib/dpkg/info/dmidecode.list
var/lib/dpkg/info/libaccounts-service0:amd64.triggers

```

Abbildung 7.12.: Idifference2 - Ausschnitt „Deleted files“ der fehlenden Zeitangaben

In der ersten Abbildung 7.13 sehen sie einen Ausschnitt aus einem Fiwalk-Hardening-Report. Er zeigt eine rapportierte Datei „/var/lib/dpkg/info/process-exporter.prerm“, die im Endergebnis des Idiff-Berichts „scion.1.idiff“ als neue Datei ausgewiesen wird. Hier und in den nachfolgenden Abbildungen sind von besonderem Interesse die Metadateneinträge Parent-Inode-ID „2883811“, File-Inode-ID „2890603“, MAC(B)-Time-Stamps sowie Dateiprüfsummen.

```

73756 <fileobject>
73757 <parent_object>
73758 <inode-2883811</inode>
73759 </parent_object>
73760 <filename>var/lib/dpkg/info/process-exporter.prerm</filename>
73761 <partition>1</partition>
73762 <id>2778</id>
73763 <name_type>r</name_type>
73764 <filesize>83</filesize>
73765 <alloc>1</alloc>
73766 <used>1</used>
73767 <inode>2890603</inode>
73768 <meta_type>1</meta_type>
73769 <mode>493</mode>
73770 <nlink>1</nlink>
73771 <uid>0</uid>
73772 <gid>0</gid>
73773 <mtime>2020-01-01T15:56:32Z</mtime>
73774 <ctime>2020-10-29T09:15:44Z</ctime>
73775 <atime>2020-10-29T09:15:44Z</atime>
73776 <ctime>2020-10-29T09:15:44Z</ctime>
73777 <byte_runs>
73778 <byte_run file_offset='0' fs_offset='41025937408' img_offset='41025937408' len='83' />
73779 </byte_runs>
73780 <hashdigest type='md5'>f0698ddf85fa206fab597e3ccb596db1</hashdigest>
73781 <hashdigest type='sha1'>0d96fd2d42186eca967fb893ce2e18f1ac8a88c7</hashdigest>
73782 </fileobject>

```

Abbildung 7.13.: Fiwalk Hardening Report - Ausschnitt der Datei „process-exporter.prerm“

Ein Vergleich der beiden Speicherbilder sollte bekanntlich lediglich die Unterschiede hervorbringen und entsprechend aufbereitet präsentieren. Unverständlicherweise verzeichnen wir im Idiff-Report teilweise keine Zeitstempel und fälschlicherweise eine unpassende Dateizuordnung. Die untere Abbildung 7.14 zeigt einen weiteren Ausschnitt aus dem Fiwalk-SCION-Report, der die gleichen Werte wie schon vorhin ausweist. Der einzige auffallende Unterschied ist die File-Object-ID und sie hat eine reine interne Bedeutung und kommt in den Auswertungen nicht zu tragen. Keine Veränderungen im Dateisystem dürften daher ausgewiesen werden. Kommen wir nun dem Grund auf die Spur. Im selben Fiwalk-SCION-Report stossen wir bei weiteren Analysen zu einem identischen Dateinamen in derselben Verzeichnisstruktur.

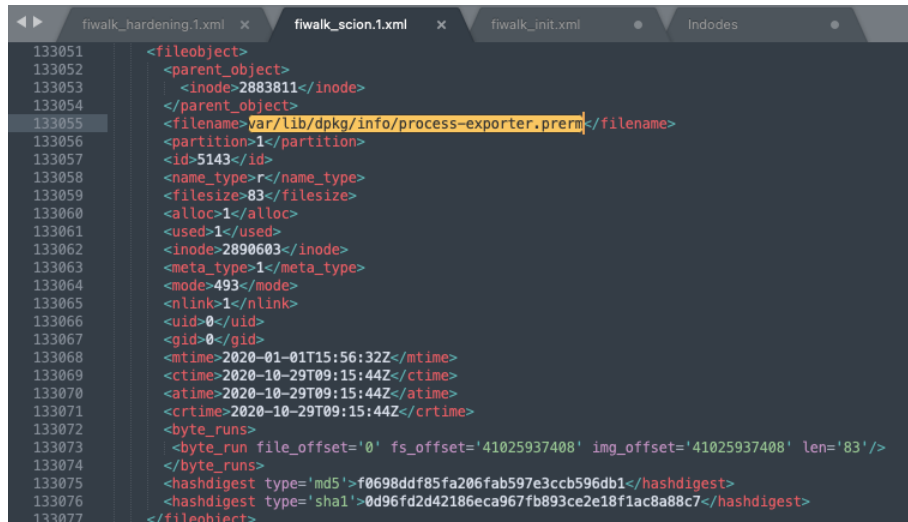


Abbildung 7.14.: Fiwalk SCION Report - Ausschnitt der Datei „process-exporter.prerm“

Die untere Abbildung 7.15 veranschaulicht die angeblich gleiche Datei „var/lib/dpkg/info/process-exporter.prerm“, aber in einem nicht zugewiesenen Dateisystemzustand. Der Eintrag verrät, dass sich die Datei im Verzeichnis mit der Inode-ID „2883811“ befunden haben muss und aufgrund der fehlenden File-Inode-ID gelöscht wurde.

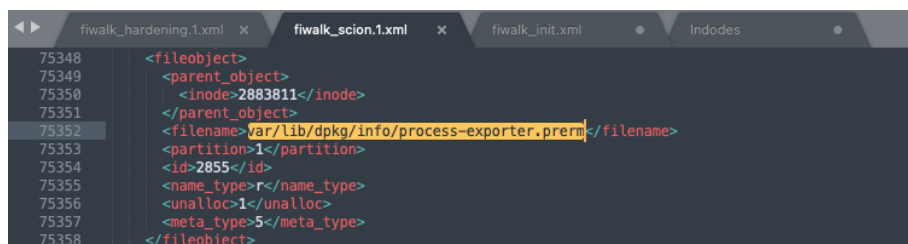


Abbildung 7.15.: Fiwalk SCION Report - Ausschnitt einer nicht zugewiesenen Datei

Gehen wir direkt auf das Speicherabbild mit dem entsprechenden TSK-Werkzeug nachschauen, können wir dank der Abbildung 7.16 nun definitiv einige wichtige Tatsachen bestätigen und aufklären. Beginnen wir mit den Erläuterungen von links nach rechts. Das erste „r“ identifiziert den Dateityp des Verzeichniseintrages und das zweite „r“ gibt den Typ im Inode an. Es handelt sich hier also um eine reguläre Datei. Wichtig zu wissen ist, dass bei gelöschten Dateien die Angaben der Dateitypen nicht immer übereinstimmen, da sie nicht mehr korrekt erkannt werden. In diesem Fall, wird überhaupt kein Dateityp mehr erkannt. Das sehen wir am Zeichen „-“, aber im Normalfall stimmen beide Angaben überein. Direkt nachfolgend vernehmen wir einen Stern „*“ und der besagt, dass die Datei gelöscht wurde. Bei gelöschten Dateien ist es möglich die alte Inode-ID noch zu erfahren. Hier hat die Datei leider einen gelöschten Inode-Zeiger. Die File-Inode-ID wurde also auf „0“ gesetzt.

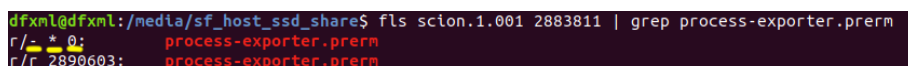


Abbildung 7.16.: TSK fls - Auflistung des Verzeichnisses „var/lib/dpkg/info“

Aufgrund der zuvor beschriebenen Dateisystemanalysen und den daraus herauskristallisierten Tatsachen ist bei den weiteren Spurenanalysen resp. weiteren Spurenverarbeitungen ein gewisses Mass an Vorsicht geboten. Idifference2 scheint also mit noch vorhandenen Inodes von gelöschten Dateien in direkter Ab-

hängigkeit der Sortierung innerhalb des Fiwalk-Reportes gewisse Komplikationen aufzuweisen. Bevor die Spuren definitiv in die Dokumentation aufgenommen und beschrieben werden können, müssen alle Spuren ohne Zeitangaben aus dem Idiff-Report nochmalig manuell überprüft oder mindestens anhand der Timelines gegengeprüft und bestätigt werden. Grundsätzlich kann bis auf diese Ausnahme, den Idiff-Resultaten vertraut werden. Lediglich bei den zeitstempellosen Einträgen muss demnach die Glaubwürdigkeit vollumfänglich überprüft werden. Trotz dem Einsatz von wissenschaftlich anerkannten Methoden und deren Werkzeugen muss hier demzufolge besonders auf die Glaubhaftigkeit der Spuren geachtet werden. Daher wurden die detaillierten Klärungen als angebracht erachtet und zudem sollten sie die bevorstehenden Herausforderungen transparent offenlegen.

Mit den etwas modifizierten und optimierten Python-Skripten, die in diesem Studiengang entwickelt wurden, können schliesslich die zuvor beschriebenen CE-Spuren gewonnen und ausgewertet werden. Eine automatisierte Spurensuche und Spurenanalyse ist für die Bewältigung dieser Arbeit sehr hilfreich. Bei weiteren zukünftigen Analysen verhilft es, zu einer verbesserten Konsistenz und erspart somit viel Zeit. Die Erstellung solcher Tools liegt bei Ermittlungen nicht immer im Vordergrund und sind nicht unbedingt von Nöten. Die Wiederholbarkeit durch Dritte kann und ist selbstverständlich mittels den beigelegten Python-Skripte sowie der Readme-Datei auf der beigelegten CD-ROM gewährleistet. Das README_FORENSICS liefert eine detaillierte Beschreibung der 5 durchlaufenen Phasen zur Gewinnung der Evidenzen.

```
dfxm@dxfml:/media/sf_host_hdd_share$ python3 ce.py
Skript ce.py aktiv, Andreas Maurer #87508
InputFile /media/sf_host_hdd_share/me/noise.me vorhanden.
InputFile /media/sf_host_hdd_share/me/hardening.me vorhanden.
InputFile /media/sf_host_hdd_share/me/scion.me vorhanden.
InputFile /media/sf_host_hdd_share/me/audit.me vorhanden.
InputFile /media/sf_host_hdd_share/me/hardening_2_scion.me vorhanden.
InputFile /media/sf_host_hdd_share/me/scion_2_audit.me vorhanden.
6 Datei(en) werden bearbeitet.

('noise', 'hardening', 'scion', 'audit') als Input-Datei(en) werden verarbeitet...
Die ('hardening', 'scion', 'audit') Output-Datei(en) werden dafür erstellt.

'hardening' als Dictionary-Key (CurrentElementOut) wird gerade verarbeitet...
'noise' wird gerade abgezogen...
'scion' wird gerade abgezogen...
'audit' wird gerade abgezogen...

'scion' als Dictionary-Key (CurrentElementOut) wird gerade verarbeitet...
'noise' wird gerade abgezogen...
'hardening' wird gerade abgezogen...
'audit' wird gerade abgezogen...

'audit' als Dictionary-Key (CurrentElementOut) wird gerade verarbeitet...
'noise' wird gerade abgezogen...
'hardening' wird gerade abgezogen...
'scion' wird gerade abgezogen...

Altes OutputFile /media/sf_host_hdd_share/ce/hardening.ce wurde zuvor gelöscht.
Aktuelles OutputFile /media/sf_host_hdd_share/ce/hardening.ce erstellt.
Altes OutputFile /media/sf_host_hdd_share/ce/scion.ce wurde zuvor gelöscht.
Aktuelles OutputFile /media/sf_host_hdd_share/ce/scion.ce erstellt.
Altes OutputFile /media/sf_host_hdd_share/ce/audit.ce wurde zuvor gelöscht.
Aktuelles OutputFile /media/sf_host_hdd_share/ce/audit.ce erstellt.
3 Datei(en) wurden erstellt.
```



```

('noise', 'hardening') als Input-Datei(en) werden verarbeitet...
Die ['hardening'] Output-Datei(en) werden dafür erstellt.

'hardening' als Dictionary-Key (CurrentElementOut) wird gerade verarbeitet...
'noise' wird gerade abgezogen...

Altes OutputFile /media/sf_host_hdd_share/ce/se/hardening.se wurde zuvor gelöscht.
Aktuelles OutputFile /media/sf_host_hdd_share/ce/se/hardening.se erstellt.
1 Datei(en) wurden erstellt.

('noise', 'hardening_2_scion') als Input-Datei(en) werden verarbeitet...
Die ['hardening_2_scion'] Output-Datei(en) werden dafür erstellt.

'hardening_2_scion' als Dictionary-Key (CurrentElementOut) wird gerade verarbeitet...
'noise' wird gerade abgezogen...

Altes OutputFile /media/sf_host_hdd_share/ce/se/hardening_2_scion.se wurde zuvor gelöscht.
Aktuelles OutputFile /media/sf_host_hdd_share/ce/se/hardening_2_scion.se erstellt.
1 Datei(en) wurden erstellt.

('noise', 'scion_2_audit') als Input-Datei(en) werden verarbeitet...
Die ['scion_2_audit'] Output-Datei(en) werden dafür erstellt.

'scion_2_audit' als Dictionary-Key (CurrentElementOut) wird gerade verarbeitet...
'noise' wird gerade abgezogen...

Altes OutputFile /media/sf_host_hdd_share/ce/se/scion_2_audit.se wurde zuvor gelöscht.
Aktuelles OutputFile /media/sf_host_hdd_share/ce/se/scion_2_audit.se erstellt.
1 Datei(en) wurden erstellt.
Skript ce.py beendet, Andreas Maurer #87508

```

Abbildung 7.17.: Forensik Python Skript - Ermittlung der charakteristischen Spuren

Die gezeigte Abbildung 7.17 führt die letzte Phase der Spurengewinnung durch. Hier werden aus den vereinigten Spurenmengen (ME-Phase) die charakteristischen Spuren für jede Aktion ermittelt. Die Basis dafür sind die mittels Idifference2 ermittelten Spuren pro Durchlauf, die jeweils mit den entwickelten Python-Skripten verarbeitet werden. Auch diese sind freilich aus Gründen der Nachvollziehbarkeit beigelegt. Wir sind nun erfolgreich am Ende der Spurengewinnung angelangt. Alle gewünschten Spurenbilder liegen als Rohdaten in einzelnen Dateien vor und warten im abschliessenden Kapitel auf die Auswertungen.

7.2. Spurenauswertung

Die Anforderungen an eine erfolgreiche forensische Untersuchung sind verständlicherweise sehr gross. Daher ist es essenziell wichtig die fünf Schlüsselpunkte wie die Akzeptanz, Glaubwürdigkeit, Wiederholbarkeit und Integrität zur Anerkennung der Umstände und Tatsachen immer vor Auge zu haben und bestmöglichst zu bewahren. Das solide Fundament konnte also geschaffen und mittels der bisherigen Ausführungen belegt werden. Bevor wir zu den Erläuterungen der wichtigsten charakteristischen Spuren und Ausprägungen kommen, benötigt es noch einige Klärungen bezüglich Warnmeldungen und merkwürdigen Erscheinungen während den differenzierten Analysen. Die Analyseresultate sollen in künftigen Untersuchungen von realen Cybervorfällen unterstützen und den Aufwand deutlich senken. Daher wird weiterhin mit gleichen oder ähnlichen Gegebenheiten gerechnet. Sie werden meist durch das betreffende Design verursacht.

Ähnlich wie die berichteten Herausforderungen mit Idifference2, wegen den Inodes ohne MAC-Angaben in Metadaten, benötigt es weiteren Klärungsbedarf hinsichtlich mehrfachen und identischer Dateisystemeinträgen (siehe Warnhinweise Listing 7.1) mit unterschiedlichen Inode-IDs.

```

1 $ sudo python3.6 /home/dfxml/tools/dfxml/python/iddifference2.py init.001 audit.1.001 > /media/sf_host_hdd_share/audit.1.idiff
2 INFO:iddifference2.py:>>> Reading init.001.
3 INFO:iddifference2.py:>>> Reading audit.1.001.
4 WARNING:make_differential_dfxml.py:Multiple instances of the file path \
5 'etc/shadow.lock' were found in partition 1; this violates an assumption of this program, that paths are unique within partitions.
6 WARNING:make_differential_dfxml.py:Multiple instances of the file path \

```

```

7      'var/lib/docker/overlay2/1de9784217a10614eeff14d3c9b1429b4aad41b425c4483396c797e816637dc4-init/diff/.dockerenv' were found in \
8      partition 1; this violates an assumption of this program, that paths are unique within partitions.
9  WARNING:make_differential_dfxml.py:Multiple instances of the file path \
10     'var/lib/docker/overlay2/24906be6278d13b82d742eecec005e475dfcc745537217dffa625eada10a3acc4/work/work' were found in partition 1; \
11     this violates an assumption of this program, that paths are unique within partitions.
12  WARNING:make_differential_dfxml.py:Multiple instances of the file path \
13     'var/lib/docker/overlay2/1fe48c9de91eb9358050069da5873baf91d968b16e8dd22e70153eef676e027e/work/work' were found in partition 1; \
14     this violates an assumption of this program, that paths are unique within partitions.

```

Listing 7.1: Idifference2 Warnings - Multiple instances of the file path

Die vertieften Ext4-Dateisystemanalysen führten wieder zu entfernten Daten und dieses Phänomen tritt dann auf, wenn sich der Dateiname in einem nicht zugewiesenen Zustand und die Metadatenstruktur in einem zugewiesenen Zustand befindet. Dies kann nur bei Dateisystemen auftreten, die den Dateinamen von den Metadaten trennen. Wie zuvor schon angedeutet gibt es in Ext4 keine feste Zuordnung zwischen Dateinamen und Datei. Bei der Erstellung einer neuen Datei wird zunächst eine Inode-ID als Referenz gebildet und als nächstes einen Verzeichniseintrag mit dem Dateinamen mit einem Verweis auf den Inode erzeugt. Genau in diesem Zwischenzustand vermerkt TSK fls bei einer Verzeichnisabfrage den Zusatz „realloc“. Zur Unterdrückung doppelter Dateinamen ist im Allgemeinen dieser Hinweis vermerkt, dass die Metadatenstruktur einer neuen Datei neu zugewiesen wurde und daher wahrscheinlich nicht die Metadaten oder der Dateinhalt sind, die ursprünglich diesem Dateinamen entsprechen. In der Abbildung 7.18 sehen sie im selben Verzeichnis mit Inode-ID „921728“ zwei identische Dateinamen „.dockerenv“ mit unterschiedlichen Inode-IDs „921755“ und „921759“. Die weiteren Darlegungen basieren auf dieser Beispieldatei und entsprechen der zweiten Idiff-Warnung.

```

<fileobject>
  <parent_object>
    <inode-921728</inode>
  </parent_object>
  <filename>var/lib/docker/overlay2/1de9784217a10614eeff14d3c9b1429b4aad41b425c4483396c797e816637dc4-init/diff/.dockerenv</filename>
  <partition-1</partition>
  <id-105463</id>
  <name_type>f</name_type>
  <filesize-0</filesize>
  <alloc-1</alloc>
  <used-1</used>
  <inode-921755</inode>
  <meta_type-1</meta_type>
  <mode-493</mode>
  <nlink-1</nlink>
  <uid-0</uid>
  <gid-0</gid>
  <mtime-2020-10-29T16:51:42Z</mtime>
  <ctime-2020-10-29T16:51:42Z</ctime>
  <atime-2020-10-29T16:51:42Z</atime>
  <crtime-2020-10-29T16:51:42Z</crtime>
</fileobject>
<fileobject>
  <parent_object>
    <inode-921728</inode>
  </parent_object>
  <filename>var/lib/docker/overlay2/1de9784217a10614eeff14d3c9b1429b4aad41b425c4483396c797e816637dc4-init/diff/.dockerenv</filename>
  <partition-1</partition>
  <id-105464</id>
  <name_type>f</name_type>
  <filesize-4096</filesize>
  <alloc-1</alloc>
  <used-1</used>
  <inode-921759</inode>
  <meta_type-2</meta_type>
  <mode-493</mode>
  <nlink-2</nlink>
  <uid-0</uid>
  <gid-0</gid>
  <mtime-2020-10-29T16:51:42Z</mtime>
  <ctime-2020-10-29T16:51:42Z</ctime>
  <atime-2021-03-29T17:12:00Z</atime>
  <crtime-2020-10-29T16:51:42Z</crtime>
  <byte_runs>
    <byte_run file_offset='0' fs_offset='15071789056' img_offset='15071789056' len='4096' />
  </byte_runs>
  <hashdigest type='md5'>07d3799c7bcd3b0c20e06b19968ea4c</hashdigest>
  <hashdigest type='sha1'>0786a28770b183e5c8cd5a4fab34ad2353278ce9</hashdigest>
</fileobject>

```

Abbildung 7.18.: Fiwalk Report - Multiple instances of the file

Das sehr übersichtliche und verständliche Beispiel veranschaulicht anhand der Abbildung 7.19 sehr klar den gelöschten Eintrag „r/d * 921759(realloc): .dockerenv“. Als Randbemerkung möchte zusätzlich darauf hingewiesen werden, dass hier der Verzeichniseintrag (r - Regular File) noch den richtigen und die Inode-Information (d - Directory) schon nicht mehr den richtigen Dateityp anzeigt. Als zusätzliche Bestätigung ziehen wir den unteren Verzeichnisauszug hinzu und vernehmen die momentan aktuell und gültige Datei mit der Inode-ID „921755“ in unserem Dateisystem.

```
dfxnl@dfxnl:/media/sf_host_hdd_share$ sudo fls /dev/loop18 921759
dfxnl@dfxnl:/media/sf_host_hdd_share$ sudo fls /dev/loop18 921755
dfxnl@dfxnl:/media/sf_host_hdd_share$ sudo fls /dev/loop18 921728
d/d 921749: dev
d/d 921752: etc
r/r 921755: .dockerenv
r/d * 921759(realloc): .dockerenv
dfxnl@dfxnl:/media/sf_host_hdd_share$ sudo ls -liaF /mnt/audit.1.001/var/lib/docker/overlay2/1de9784217a10614eeff14d3c9b1429b4aad41b425c4483396c797e816637dc4-lnit/diff/
total 16
921728 drwxr-xr-x 4 root root 4096 Okt 29 2020 ./
921435 drwx----- 4 root root 4096 Okt 29 2020 ../
921749 drwxr-xr-x 4 root root 4096 Okt 29 2020 dev/
921755 -rwxr-xr-x 1 root root 0 Okt 29 2020 .dockerenv* * Indicates a executable file ($ is -F)
921752 drwxr-xr-x 2 root root 4096 Okt 29 2020 etc/
```

Abbildung 7.19.: Directory and File Listing - Verification of multiple file instances

Alle anderen Idiff-Warnhinweise waren gemäss den Analyseresultaten auf dasselbe Verhalten (Works as designed!) zurückzuführen. Den aufmerksamen Lesern und Interessierten wird bei der Durchsicht der Fiwalk- und Idiff-Reporten vermutlich aufgefallen sein, dass es etliche Einträge von Datei- und Verzeichnisnamen mit Sonderzeichen gibt. Ein gutes Beispiel zeigt das Verzeichnis „/var/lib/dpkg/info“ mit der Inode-ID „2883811“ aus dem Audit.1.001-Abbild. Unter diesem Verzeichnis gibt es wiederum eine Inode „-/- * 119: ^“ das mit hoher Wahrscheinlichkeit ein Überbleibsel einer gelöschten Datei oder einem Verzeichnis sein muss und die Sonderzeichen kommen von bereits überschriebenen Metadaten. Bei den Spuren-Auswertungen besteht also die Möglichkeit von solchen Vorkommnissen, die daher nicht nennenswert sind oder abschliessend konkretisiert werden können.

Die beschriebenen Idiff- und Fiwalk-Probleme sind alle auf gelöschte Dateien zurückzuführen. Auch in den drei folgenden CE-Spurenermittlungen wird dieses Thema dauernd ein Begleiter sein. Bei näherer Betrachtung, der ausgewerteten und zusammengeführten Idiff-Spurenansammlungen (z. B. audit.me), erkennt die aufmerksame Leserschaft bei manchen Spurenerscheinungen einen ungewöhnlich hohen Zähler an Spurenvorkommnisse. Eigentlich dürfte dieser Zähler, hinsichtlich der Anzahl von gleichen Spurenbildern (z. B. audit.{1, 2, 3}.pe), nicht höher als Drei (3) sein. In der genannten Beispieldatei „audit.me“ vernehmen wir bei manchen Spuren wie z. B. unter den Einträgen „usr/share/mime/application/x-troff-man-compressed.xml“ einen Zähler von jeweils Sechs (6). Schon wieder dreht sich die Sachlage, so wie die Abbildung 7.20 belegt, um gelöschte Dateien. Bei der Auslegung der CE-Spuren gehört diesem Erscheinungsbild erneut eine besondere Aufmerksamkeit.

```
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo ls -liaF /mnt/audit.1.001/usr/share/mime/application/ | grep x-troff-man-compressed.xml
2625724 -rw-r--r-- 1 root root 3760 Okt 29 2020 x-troff-man-compressed.xml
dfxnl@dfxnl:/media/sf_host_ssd_share$ sudo fls /dev/loop17 2625687 | grep x-troff-man-compressed.xml
r/r * 2625725(realloc): x-troff-man-compressed.xml
r/r 2625724: x-troff-man-compressed.xml
```

Abbildung 7.20.: Merged Evidences - Zu hohe Anzahl an Spurenerscheinungen

Gemäss Carrier[5] kann ein verwaister Inode (Orphaned Inode/File) eine gelöschte Datei sein, die keinen Verzeichniseintrag mehr hat, aber noch in irgendeinem Prozess geöffnet ist. Die Daten sind dann noch auf der Festplatte vorhanden. Erst wenn der letzte Prozess, der diese Datei geöffnet hat, sie schliesst oder das System herunterfährt, wird die Datei vollständig gelöscht und der verwaiste Inode verschwindet. Der Superblock führt eine Liste, um diesen Prozess zu ermöglichen. Eine andere Erklärung könnte sein, wenn ein Verzeichnis gelöscht wird und sein Eintrag neu zugewiesen wird. In diesem Fall gibt es keinen Zeiger (Adresse) mehr auf die Dateien und Verzeichnisse im gelöschten Verzeichnis. Die nicht zugewiesenen Verzeichniseinträge existieren noch, aber wir können sie nicht finden und zugreifen, indem wir einfach

dem Verzeichnisbaum folgen, und wenn wir sie finden, haben wir keine Adresse für sie. Im TSK werden verwaiste Dateien im virtuellen Verzeichnis „\$OrphanFiles“ aufgelistet. Dieses Verzeichnis existiert nicht auf der Disk und daher auch nicht im Abbild. Es ist lediglich ein virtueller Weg für TSK, um dem Forensiker den Zugriff auf die vorhandenen Metadaten zu ermöglichen. Da wir bekanntlich nicht weiter auf diese Orphan Files eingehen oder analysieren, genügt eine einfache Auflistung in der entsprechenden CE-Spurensammlung `aktion.ce/se`.

Wie erklärt, interessiert in unserem Fall auch im beschränkten Masse der zeitliche Aspekt. Plaso speichert seine gesammelten Daten mittels seinem Linux-Parser¹⁶ und den Plugins in einem Plaso-Speicherabbild (SQLite v3 Datenbank). Es enthält zusätzliche Hinweise über die Ausführung selbst und andere nützliche Informationen, wie z. B. solche die während der Vorverarbeitung gesammelt wurden oder Warnungen von nicht geparsen Daten. Der untere Ausschnitt über die Plaso-Log-Informationen zeigt lediglich 5 Warnungen. Diese sind nach einer gründlichen Prüfung lediglich als Hinweise zu verstehen und können in den weiteren Untersuchungen ignoriert werden.

```
***** Warnings generated per parser *****
Parser (plugin) name : Number of warnings
-----
      utmp : 2
      syslog : 1
      pls_recall : 1
      <no parser> : 1
-----
***** Path specifications with most warnings *****
Number of warnings : PathsSpec
-----
      2 : type: OS, location:
          /mnt/audit_rep.1.001/lib/firmware/915/skl_guc_ver1.bin
      1 : type: OS, location:
          /mnt/audit_rep.1.001/var/log/installer/syslog
      1 : type: OS, location:
          /mnt/audit_rep.1.001/var/lib/docker/overlay2/3071d81587aeca53cdde9250fb57ceab8a5280ab5afdd62bf7210b491df28ac/dlff/usr/share/python/pyversions.py
      1 : type: OS, location:
          /mnt/audit_rep.1.001/var/lib/docker/overlay2/e389347ab08f5df3ef6f12271ef20fcb732590998808f60826c23fa13ebcf64/dlff/usr/local/go/src/compress/bzip2/testdata/fail-issue5747.bz2
      1 : type: COMPRESSED_STREAM, compression_method: bzip2
-----
```

Abbildung 7.21.: Plaso Storage Information (Extract) - Warnings generated per parser

Die Utmp- und Syslog-Warnungen sind mit hoher Wahrscheinlichkeit auf die Ereignisse der automatisierten SCION-Installationen zurückzuführen. In diesem Zeitraum wurden während den SCION-Installationen und Konfigurationen etliche Fehlermeldungen generiert. Eine zusätzliche Inspektion mit den Tools¹⁷ „last“ oder „utmpdump“ der relevanten Dateien wie „/var/log/wtmp“, „/var/run/utmp“ und „/var/log/btmp“ führten nicht zu weiteren erklärenden Erkenntnissen. Die dritte Meldung verweist auf das Python-Skript „pyversions.py“ innerhalb eines nicht benötigten Docker Images. Es besitzt eine besondere Funktionalität und kann in der aktuellen Sitzung von importierten Modulen die Versionen herauslesen. Dafür verwendet es das Python-Inspect-Modul¹⁸, um den globalen Namespace des Aufrufers zu erhalten. Das nicht bemängelte Original liegt unter einem typischen Python-Verzeichnis „/usr/share/python/pyversions.py“. Weshalb innerhalb eines Docker Containers dieses Skript benötigt wird, möchte hier nicht weiter geklärt oder hinterfragt werden. Die vierte und letzte Andeutung besagt, dass die Datei aufgrund der Komprimierung nicht analysiert werden konnte. Bei möglichen Sicherheitsvorfällen oder auch bei allgemeinen Untersuchungen sind solche Angaben immer sehr interessant und können auch mögliche Probleme aufdecken.

Nach den Klärungen aller offenen Punkte, gehen wir nun mit einem gutem Gewissen abschliessend und konkret auf die einzelnen charakteristischen resp. spezifischen Spurenbilder, der einzelnen Installationsschritten und dem Security Auditing ein. Wie bereits geschildert, wird normalerweise bei der differenzierten forensischen Analyse ein etwas anderes Vorgehen gewählt, so dass die Spurenerzeugung grundsätzlich immer vom selben initialen Ausgangspunkt startet. Aufgrund der realen Nachbildung einer SCION-Installation (siehe dafür Abbildung 7.1) müssen wir hier die Spuren Mengen ausnahmsweise etwas anders voneinander abziehen. Das Endresultat ist aber schlussendlich dasselbe. Die entsprechenden Unterkapitel geben eine Aufklärung der verwendeten Formeln und schildern die wichtigsten, charakteristischen Spuren.

¹⁶<https://github.com/log2timeline/plaso/blob/main/docs/sources/user/Parsers-and-plugins.md>

¹⁷<https://www.thegeekdiary.com/what-is-the-purpose-of-utmp-wtmp-and-btmp-files-in-linux/>

¹⁸Das Python Inspect Module [<https://docs.python.org/3/library/inspect.html>] kurz erklärt.

7.2.1. Charakterische Spuren des SCION Hardening - OS Konfiguration

Nach der Erzeugung des Anapaya-Basis-Images erfolgten die ersten kundenspezifischen Systemmodifikationen. Anhand der im Vorfeld geklärten SCION-Designfragen und den notwendigen Implementierungsspezifikationen, konnten die weiteren Kundenkonfigurationen in einem Ansible-Playbook abgebildet und ausgerollt werden. In diesem Paket sind bereits gewisse Hardening-Massnahmen, die seitens Integrators und aufgrund von Kundenwünschen kommen, bereits berücksichtigt. Die Beantwortung der Frage, welche unverkennbaren Spuren die ersten SCION-Installationsschritte nach Abzug aller fremdverursachten Spurenbilder hinterliessen, steht hier im Vordergrund. Diese Fragestellung wird mit der nachfolgenden Formel beantwortet:

$$\underline{\text{CE_H}} = \text{hardening.me} - \text{hardening_2_scion.me} - \text{scion_2_audit.me} - \text{noise.me}$$

Das gesamte Endresultat „CE_H“, befindet sich als Datei auf der beigelegten CD-ROM mit dem Namen `hardening.se`¹⁹. Anschliessend werden die wichtigsten Spuren aufgelistet und falls vorhanden die Abweichungen zu den uns bekannten Hintergrundinformationen aufgezeigt. Unter Unterabschnitt 4.2.4 wurden die Systemveränderungen stichwortartig kurz aufgezählt und hier mit Teilausschnitten aus den eruierten CE_H-Spuren entsprechend nachgewiesen.

Das Listing 7.2 zeigt, dass vermutlich ein Admin von Anapaya Systems AG namens Lukas mit dem Benutzer „root“ die SCION-Konfigurationen durchgeführt hatte. Da die weiteren Systemkonfigurationen auch mit Ansible gemacht wurden, sehen wir hier nur die für das Hardening typischen Spuren. Zudem belgt der Ausschnitt auch gewisse Modifikationen an den besprochenen Firewall-Regeln (Iptables).

```

1  ...
2  home/anapaya/~lukas/.ansible/tmp/ansible-tmp-1603963188.7988334-177992759180548 a
3  home/anapaya/~lukas/.ansible/tmp/ansible-tmp-1603963188.7988334-177992759180548 cr
4  etc/iptables/rules.v4.ansible a
5  etc/iptables/rules.v4.ansible c
6  etc/iptables/rules.v4.ansible cr
7  etc/iptables/rules.v4.ansible m
8  root/.ansible a
9  root/.ansible c
10 root/.ansible cr
11 root/.ansible m
12 root/.ansible/tmp cr
13 usr/local/sbin/ansible-iptables-apply a
14 usr/local/sbin/ansible-iptables-apply c
15 usr/local/sbin/ansible-iptables-apply cr
16 usr/local/sbin/ansible-iptables-apply m
17 ...

```

Listing 7.2: CE_H-Spuren - Ansible Playbook

¹⁹Die Dateierdung `.se` kommt daher, weil das ursprüngliche Python-Skript für den Abzug anderer Spurenbilder angedacht ist. Wie zuvor erläutert, geht die differenzielle Forensische-Analyse meistens von Spurenmengen mit Ursprung des initialen Abbildes aus. Das justierte Skript legt unsere CE-Spuren immer mit dieser Dateierdung und im Unterverzeichnis `„./ce/se“` ab.

Mit dem nachfolgenden Listing 7.3 belegen wir die SCION-Benutzerkonten, Superuser- und User-Name-space²⁰-Konfigurationen und die Einrichtung des SSH-Zugangs mittels dem autorisierten öffentlichen Schlüssel. Die Hardening-Checks haben dieses Verhalten zuvor bestätigt. Wenn also der Client eine Verbindung zur SCION-Appliance herstellt, authentifiziert das System den Client, indem er seinen gespeicherten signierten öffentlichen Schlüssel überprüft.

```
1  ...
2  etc/shadow- a
3  etc/shadow- c
4  etc/shadow- m
5  etc/shadow.12099 d
6  etc/shadow.lock a
7  etc/shadow.lock c
8  etc/shadow.lock cr
9  etc/shadow.lock m
10 etc/ssh/sshd_config a
11 etc/ssh/sshd_config c
12 etc/ssh/sshd_config cr
13 etc/ssh/sshd_config m
14 etc/subgid a
15 etc/subgid c
16 etc/subgid cr
17 etc/subgid m
18 etc/subgid- a
19 etc/subgid- c
20 etc/subgid- m
21 etc/subgid.lock a
22 etc/subgid.lock c
23 etc/subgid.lock cr
24 etc/subgid.lock m
25 etc/subuid a
26 etc/subuid c
27 etc/subuid cr
28 etc/subuid m
29 etc/subuid- a
30 etc/subuid- c
31 etc/subuid- m
32 etc/subuid.lock a
33 etc/subuid.lock c
34 etc/subuid.lock cr
35 etc/subuid.lock m
36 etc/sudoers.d a
37 etc/sudoers.d c
38 etc/sudoers.d m
39 etc/sudoers.d/README.dpkg-new d
40 etc/sudoers.d/scion a
41 etc/sudoers.d/scion c
42 etc/sudoers.d/scion cr
43 etc/sudoers.d/scion m
44 ...
45 home/scion a
46 home/scion cr
47 home/scion/.bash_logout a
48 home/scion/.bash_logout c
49 home/scion/.bash_logout cr
50 home/scion/.bash_logout m
51 home/scion/.bashrc a
52 home/scion/.bashrc c
53 home/scion/.bashrc cr
54 home/scion/.bashrc m
55 home/scion/.profile a
56 home/scion/.profile c
57 home/scion/.profile cr
58 home/scion/.profile m
```

²⁰Container durch User Namespace isolieren [<https://docs.docker.com/engine/security/usersns-remap/>]

```

59 home/scion/.ssh a
60 home/scion/.ssh c
61 home/scion/.ssh cr
62 home/scion/.ssh m
63 home/scion/.ssh/authorized_keys a
64 home/scion/.ssh/authorized_keys c
65 home/scion/.ssh/authorized_keys cr
66 home/scion/.ssh/authorized_keys m
67 ...

```

Listing 7.3: CE_H-Spuren - SCION Benutzer mit SSH Konfiguration

Im Listing 7.4 sehen wir einen Ausschnitt der Host- und Netzwerk-Konfigurationen. Das SIG verfügt bekanntlich über mehrere Netzwerkschnittstellen und hier nochmals andeutungsweise mit den Zeilen 25 bis 40 bestätigt. Zuoberst und zuunterst vernehmen wir, die wichtigen und unerlässlichen Netzwerkinfrastrukturservicekonfigurationen wie NTP und DNS.

```

1 ...
2 etc/chrony c
3 etc/chrony m
4 etc/chrony/chrony.conf a
5 etc/chrony/chrony.conf c
6 etc/chrony/chrony.conf cr
7 etc/chrony/chrony.conf m
8 etc/hostname a
9 etc/hostname c
10 etc/hostname cr
11 etc/hostname m
12 etc/network c
13 etc/network m
14 etc/network/interfaces a
15 etc/network/interfaces c
16 etc/network/interfaces cr
17 etc/network/interfaces m
18 etc/network/interfaces.d a
19 etc/network/interfaces.d c
20 etc/network/interfaces.d m
21 etc/network/interfaces.d.dpkg-new a
22 etc/network/interfaces.d.dpkg-new c
23 etc/network/interfaces.d.dpkg-new m
24 etc/network/interfaces.d/ens1f0 a
25 etc/network/interfaces.d/ens1f0 c
26 etc/network/interfaces.d/ens1f0 cr
27 etc/network/interfaces.d/ens1f0 m
28 etc/network/interfaces.d/ens1f1 a
29 etc/network/interfaces.d/ens1f1 c
30 etc/network/interfaces.d/ens1f1 cr
31 etc/network/interfaces.d/ens1f1 m
32 etc/network/interfaces.d/ens2f0 a
33 etc/network/interfaces.d/ens2f0 c
34 etc/network/interfaces.d/ens2f0 cr
35 etc/network/interfaces.d/ens2f0 m
36 etc/network/interfaces.d/lo a
37 etc/network/interfaces.d/lo c
38 etc/network/interfaces.d/lo cr
39 etc/network/interfaces.d/lo m
40 etc/resolv.conf a
41 etc/resolv.conf c
42 etc/resolv.conf cr
43 etc/resolv.conf m
44 ...

```

Listing 7.4: CE_H-Spuren - Hostnamen-, Netzwerk- und DNS/NTP-Konfigurationen

Zusätzlich zu den bekanntgegebenen Systemänderungen registrierten die Analysen auch gewisse Anpassungen an den Kernelparametern (siehe Listing 7.5). Diese Parameter wurden bereits zuvor im Bereich Auditing und Hardening thematisiert und steuern wichtige Kernel-Eigenschaften, Treiberoptionen und die Ansteuerung von Hardwarekomponenten. Einige Parameter waren schon optimal gesetzt und dies ist vermutlich auf diese Änderungsregistrierung zurückzuführen.

```

1  ...
2  etc/sysctl.d a
3  etc/sysctl.d c
4  etc/sysctl.d m
5  etc/sysctl.d/10-console-messages.conf.dpkg-new d
6  etc/sysctl.d/10-ipv6-privacy.conf.dpkg-new d
7  etc/sysctl.d/10-kernel-hardening.conf.dpkg-new d
8  etc/sysctl.d/10-link-restrictions.conf.dpkg-new d
9  etc/sysctl.d/10-magic-sysrq.conf.dpkg-new d
10 etc/sysctl.d/10-pttrace.conf.dpkg-new d
11 etc/sysctl.d/60-buffers.conf a
12 etc/sysctl.d/60-buffers.conf c
13 etc/sysctl.d/60-buffers.conf cr
14 etc/sysctl.d/60-buffers.conf m
15 etc/sysctl.d/60-coredumps.conf a
16 etc/sysctl.d/60-coredumps.conf c
17 etc/sysctl.d/60-coredumps.conf cr
18 etc/sysctl.d/60-coredumps.conf m
19 etc/sysctl.d/60-forwarding.conf a
20 etc/sysctl.d/60-forwarding.conf c
21 etc/sysctl.d/60-forwarding.conf cr
22 etc/sysctl.d/60-forwarding.conf m
23 etc/sysctl.d/60-kernel_panic_timeout.conf a
24 etc/sysctl.d/60-kernel_panic_timeout.conf c
25 etc/sysctl.d/60-kernel_panic_timeout.conf cr
26 etc/sysctl.d/60-kernel_panic_timeout.conf m
27 etc/sysctl.d/60-rp_filter.conf a
28 etc/sysctl.d/60-rp_filter.conf c
29 etc/sysctl.d/60-rp_filter.conf cr
30 etc/sysctl.d/60-rp_filter.conf m
31 etc/sysctl.d/60-syncookies.conf a
32 etc/sysctl.d/60-syncookies.conf c
33 etc/sysctl.d/60-syncookies.conf cr
34 etc/sysctl.d/60-syncookies.conf m
35 ...

```

Listing 7.5: CE_H-Spuren - Kernelparameter-Änderungen

Nachfolgend erkennen wir abschliessend im Listing 7.6, wie die installierten Container bezüglich Monitoring- und IP-Routing-Services konfiguriert und sie mit hoher Wahrscheinlichkeit über Docker Compose gesteuert werden. Ausserdem registrieren wir im unteren Bereich gewisse Änderungen bezüglich Logging (Journal).

```

1  ...
2  etc/docker-compose/blackbox-exporter a
3  etc/docker-compose/blackbox-exporter c
4  etc/docker-compose/blackbox-exporter cr
5  etc/docker-compose/blackbox-exporter m
6  etc/docker-compose/blackbox-exporter-sigonly a
7  etc/docker-compose/blackbox-exporter-sigonly c
8  etc/docker-compose/blackbox-exporter-sigonly cr
9  etc/docker-compose/blackbox-exporter-sigonly m
10 etc/docker-compose/blackbox-exporter-sigonly/docker-compose.yml a
11 etc/docker-compose/blackbox-exporter-sigonly/docker-compose.yml c
12 etc/docker-compose/blackbox-exporter-sigonly/docker-compose.yml cr
13 etc/docker-compose/blackbox-exporter-sigonly/docker-compose.yml m

```

```

14  etc/docker-compose/blackbox-exporter/docker-compose.yml a
15  etc/docker-compose/blackbox-exporter/docker-compose.yml c
16  etc/docker-compose/blackbox-exporter/docker-compose.yml cr
17  etc/docker-compose/blackbox-exporter/docker-compose.yml m
18  etc/docker-compose/node-exporter a
19  etc/docker-compose/node-exporter c
20  etc/docker-compose/node-exporter cr
21  etc/docker-compose/node-exporter m
22  etc/docker-compose/node-exporter/docker-compose.yml a
23  etc/docker-compose/node-exporter/docker-compose.yml c
24  etc/docker-compose/node-exporter/docker-compose.yml cr
25  etc/docker-compose/node-exporter/docker-compose.yml m
26  etc/docker-compose/quagga a
27  etc/docker-compose/quagga c
28  etc/docker-compose/quagga cr
29  etc/docker-compose/quagga m
30  etc/docker-compose/quagga/docker-compose.yml a
31  etc/docker-compose/quagga/docker-compose.yml c
32  etc/docker-compose/quagga/docker-compose.yml cr
33  etc/docker-compose/quagga/docker-compose.yml m
34  ...
35  etc/process-exporter c
36  etc/process-exporter m
37  etc/process-exporter/all.yml a
38  etc/process-exporter/all.yml c
39  etc/process-exporter/all.yml cr
40  etc/process-exporter/all.yml m
41  etc/process-exporter/all.yml.dpkg-new a
42  etc/process-exporter/all.yml.dpkg-new c
43  etc/process-exporter/all.yml.dpkg-new cr
44  etc/process-exporter/all.yml.dpkg-new m
45  etc/prometheus a
46  etc/prometheus c
47  etc/prometheus cr
48  etc/prometheus m
49  etc/prometheus/blackbox.yml a
50  etc/prometheus/blackbox.yml c
51  etc/prometheus/blackbox.yml cr
52  etc/prometheus/blackbox.yml m
53  etc/quagga a
54  etc/quagga c
55  etc/quagga cr
56  etc/quagga m
57  etc/quagga/bgpd.conf a
58  etc/quagga/bgpd.conf c
59  etc/quagga/bgpd.conf cr
60  etc/quagga/bgpd.conf m
61  etc/quagga/zebra.conf a
62  etc/quagga/zebra.conf c
63  etc/quagga/zebra.conf cr
64  etc/quagga/zebra.conf m
65  ...
66  etc/systemd/journald.conf a
67  etc/systemd/journald.conf c
68  etc/systemd/journald.conf cr
69  etc/systemd/journald.conf m
70  ...

```

Listing 7.6: CE_H-Spuren - Konfigurationen der IP-Router- und Monitoring-Container/Services

Zu den Auswertungen ist jedoch anzumerken, dass wir mit dieser Art von Report (min. dreimaliges Vorkommen eines Artefaktes) mit sehr hoher Wahrscheinlichkeit sagen können, dass gewisse Docker Container Images heruntergeladen und installiert wurden. Um welche Images es sich genau handelt, mit ihrem jeweiligen Namen oder ihrer ID benannt, ist eher sehr schwierig oder praktisch unmöglich zu sagen. Docker

ändert die Container-IDs nach jeder Installation. Mit diesem Vorgehen verhindert Docker Duplikate auf demselben Host. Mit dieser forensischen Auswertung können wir aber trotzdem mehr als zufrieden sein, denn alle aufgefundenen charakterlichen Spuren bezüglich Hardening konnten erfolgreich belegt und bewiesen werden. Weitere Erläuterungen dürften hier nicht mehr notwendig sein, denn sie erscheinen für sich als selbstsprechend.

7.2.2. Charakterische Spuren der SCION Services - SCION Konfiguration

Nach dem ersten Installationsabschnitt, mit dem die Basis-OS-Konfiguration und ersten Hardening-Massnahmen erfolgreich umgesetzt wurden, folgt nun der zweite und letzte Schritt für eine gelungene SCION-Inbetriebnahme. In Anlehnung an das SCION-Integrationskonzept und den weiterführenden Implementierungsspezifikationen findet hier die finale SCION-Konfiguration statt. Wie gewohnt, ermöglicht uns auch hier wieder das Ansible-Playbook, eine vereinfachte und deckungsgleiche Ausrollung. Eine erste grobe Sichtung und in Anbetracht der grosse Spurenmenge, deutet dies auf erhebliche Anwendungsinstallationen hin. Scheinbar wurden noch andere Pakete, nicht nur für SCION selbst, installiert. Sollte sich diese Behauptung bewahrheiten, dann werden nicht die zahllosen Spuren aufgeführt, sondern lediglich die Anwendungen bestmöglich benannt und aufgelistet. Für die Beantwortung der Frage, welche unverkennbaren Spuren die abschliessende SCION-Installation mit sich brachte, wird nach Abzug aller Spuren von den uns bekannten fremden Aktionen mit der nachfolgenden Formel beantwortet:

$$\underline{\text{CE_S}} = \text{scion.me} - \text{hardening.me} - \text{scion_2_audit.me} - \text{noise.me}$$

Das gesamte Endresultat „CE_S“ befindet sich auch als Datei auf der beigelegten CD-ROM mit dem Namen `scion.se`. Es werden nun die wichtigsten Spuren aufgelistet und falls vorhanden, die Abweichungen zu den uns bekannten Hintergrundinformationen aufgezeigt. Unter Unterabschnitt 4.2.4 wurden die Systemveränderungen stichwortartig kurz aufgezählt und hier mit Teilausschnitten aus den eruierten CE_S-Spuren entsprechend nachgewiesen.

Wie vermutet, finden wir in dieser CE-Spurenmenge keine Anzeichen auf die automatisierte Installation mittels Ansible. Würden wir bei den Merged Evidences „`hardening_2_scion.me`“ nachschauen gehen, dann würden wir die entsprechenden Spuren verursacht von Ansible sehen. Dies ist sehr gut möglich und sehr einfach zu erklären, denn es wurden dieselben Skripte dafür verwendet und Ansible arbeitet oft mit temporären Dateien und zufälligen Dateinamen. Die Dateien resp. Spuren mit kleiner (<) 3 Vorkommnissen werden bekanntlich nicht gelistet und als charakteristisch angesehen. Das ähnliche Verhalten haben wir schon bei den Docker Container IDs gesehen und daher ist ein besonderes Augenmerk auch auf solche einmaligen und wichtigen Spuren geboten.

Anhand der Spuren und dem Ansible-Playbook „`./roles/packages/vars/main.yml`“ wurden mit hoher Wahrscheinlichkeit schon etliche APT Packages vor dem Status „Anapaya-Base-Image“ vorinstalliert. Lediglich anhand der Bibliotheken ist es nicht möglich zuzusagen, um welche Anwendungen es sich genau handelt. Anhand der Datei- und Verzeichnisnamen können jedoch ziemlich genaue Annahmen getroffen werden. In den vorliegenden Spuren können wir mit hoher Sicherheit heraussehen, dass gewisse Pakete wie z. B. Wireshark (tshark) oder SCION-Apps z. B. `scion scion-pki` oder `bwtester` aktualisiert oder neu installiert wurden. Das nachfolgende Listing 7.7 zeigt einen Ausschnitt der angeblich installierten SCION Dienstprogrammen und Plugins.

```

1  ...
2  usr/lib/x86_64-linux-gnu/wireshark/plugins/scion.lua  a
3  usr/lib/x86_64-linux-gnu/wireshark/plugins/scion.lua  c
4  usr/lib/x86_64-linux-gnu/wireshark/plugins/scion.lua  cr

```



```

5  usr/lib/x86_64-linux-gnu/wireshark/plugins/scion.lua  m
6  usr/lib/x86_64-linux-gnu/wireshark/plugins/scion.lua.dpkg-new  a
7  usr/lib/x86_64-linux-gnu/wireshark/plugins/scion.lua.dpkg-new  c
8  usr/lib/x86_64-linux-gnu/wireshark/plugins/scion.lua.dpkg-new  cr
9  usr/lib/x86_64-linux-gnu/wireshark/plugins/scion.lua.dpkg-new  m
10 ...
11 var/lib/dpkg/info/anascion-utils.list  a
12 var/lib/dpkg/info/anascion-utils.list  c
13 var/lib/dpkg/info/anascion-utils.list  cr
14 var/lib/dpkg/info/anascion-utils.list  m
15 var/lib/dpkg/info/anascion-utils.list-new  a
16 var/lib/dpkg/info/anascion-utils.list-new  c
17 var/lib/dpkg/info/anascion-utils.list-new  cr
18 var/lib/dpkg/info/anascion-utils.list-new  m
19 ...

```

Listing 7.7: CE_S-Spuren - SCION Dienstprogramme und Plugins

In den typischen Anwendungsverzeichnis wie „/usr/bin/*“, „/usr/lib/x86_64-linux-gnu/*“, „/usr/share/*“, „/var/lib/dpkg/*“ und „/var/cache/*“ vernehmen wir die grössten Aktivitäten. Einen Blick in die APT-Paketmanagement-System-Logs (siehe Listing 7.8) würde das vermeintliche Geheimnis vermutlich grösstenteils lüften.

```

1  ...
2  var/log/apt/history.log  c
3  var/log/apt/history.log  m
4  var/log/apt/term.log  c
5  var/log/apt/term.log  m
6  var/log/dpkg.log  c
7  var/log/dpkg.log  m
8  ...

```

Listing 7.8: CE_S-Spuren - APT-Paketmanagement-System-Log-Dateien

Mit unserem Hintergrundwissen ergibt es wenig Sinn, sich weiter auf diese Spuren zu konzentrieren und wir setzen den Fokus wieder auf die SCION relevanten Spuren. Wäre die SCION-Appliance kompromittiert, dann würde die Sachlage natürlich etwas anders aussehen.

Bereits zu Beginn der Analysen tauchten vier (4) nicht gelistete Container auf. Wie im Listing 7.9 gezeigt, handelt es sich hier um die Anwendungen „Patroni“ und „Consul“. Patroni²¹ ist ein High-Availability-Cluster-Manager, der zur Anpassung und Automatisierung der Bereitstellung und Wartung von PostgreSQL-HA-Clustern verwendet wird. Dafür ist er auf verteilte Konfigurationsspeicher z. B. mit Hilfe von Consul für die maximale Erreichbarkeit angewiesen. Diese Funktionalität wurde bei SIX für den SCION-Bereich der Certificate Authority eingesetzt und wird nächstens aus den SCION-Services ausgelöst und separat ausgeführt. Wie die Monitoring-Fähigkeiten, stand diese Funktion daher auch nicht im Fokus. Die SIG-Services beziehen also künftig den CA-Service von ausserhalb. Das war der Hauptgrund weshalb sie nicht aktiv sind und bei den Security Benchmarks nicht mitberücksichtigt wurden.

```

1  ...
2  etc/consul  a
3  etc/consul  c
4  etc/consul  cr
5  etc/consul  m
6  etc/consul/consul.json  a
7  etc/consul/consul.json  c

```

²¹<https://www.cybertec-postgresql.com/en/patroni-setting-up-a-highly-available-postgresql-cluster/>

```
8  etc/consul/consul.json  cr
9  etc/consul/consul.json  m
10 etc/docker-compose/consul a
11 etc/docker-compose/consul c
12 etc/docker-compose/consul cr
13 etc/docker-compose/consul m
14 etc/docker-compose/consul/docker-compose.yml a
15 etc/docker-compose/consul/docker-compose.yml c
16 etc/docker-compose/consul/docker-compose.yml cr
17 etc/docker-compose/consul/docker-compose.yml m
18 etc/docker-compose/patroni a
19 etc/docker-compose/patroni c
20 etc/docker-compose/patroni cr
21 etc/docker-compose/patroni m
22 etc/docker-compose/patroni/docker-compose.yml a
23 etc/docker-compose/patroni/docker-compose.yml c
24 etc/docker-compose/patroni/docker-compose.yml cr
25 etc/docker-compose/patroni/docker-compose.yml m
26 etc/patroni a
27 etc/patroni c
28 etc/patroni cr
29 etc/patroni m
30 etc/patroni/iniql a
31 etc/patroni/iniql c
32 etc/patroni/iniql cr
33 etc/patroni/iniql m
34 etc/patroni/iniql/init.sql a
35 etc/patroni/iniql/init.sql c
36 etc/patroni/iniql/init.sql cr
37 etc/patroni/iniql/init.sql m
38 etc/patroni/metrics.pwd a
39 etc/patroni/metrics.pwd c
40 etc/patroni/metrics.pwd cr
41 etc/patroni/metrics.pwd m
42 etc/patroni/patroni.yml a
43 etc/patroni/patroni.yml c
44 etc/patroni/patroni.yml cr
45 etc/patroni/patroni.yml m
46 etc/patroni/setup_db a
47 etc/patroni/setup_db c
48 etc/patroni/setup_db cr
49 etc/patroni/setup_db m
50 var/lib/consul a
51 var/lib/consul c
52 var/lib/consul cr
53 var/lib/consul m
54 var/lib/patroni a
55 var/lib/patroni c
56 var/lib/patroni cr
57 var/lib/patroni m
58 var/lib/postgresql a
59 var/lib/postgresql c
60 var/lib/postgresql cr
61 var/lib/postgresql m
62 var/lib/postgresql/data a
63 var/lib/postgresql/data c
64 var/lib/postgresql/data cr
65 var/lib/postgresql/data m
66 ...
```

Listing 7.9: CE_S-Spuren - Patroni PostgreSQL HA-Cluster-Konfigurationen

Auch nicht gelistet sind die nennenswerten Einrichtungen für die wichtigen und unterstützenden SCION-Infrastruktur-Aufgaben. Die im Listing 7.10 aufgeführten Python-Skripts „as_cert_renewal“ und „showpaths_prom“ werden einerseits für das Monitoring (Pfadüberwachung) und die Erneuerung des AS-Zertifikates

verwendet. Wie es scheint, werden die Skripts mit hoher Wahrscheinlichkeit automatisiert über die Linux-Funktionalität „cron“ kontinuierlich angestossen.

```

1  ...
2  etc/cron.d/as_cert_renewal_ISD70 a
3  etc/cron.d/as_cert_renewal_ISD70 c
4  etc/cron.d/as_cert_renewal_ISD70 cr
5  etc/cron.d/as_cert_renewal_ISD70 m
6  etc/cron.d/showpaths_export a
7  etc/cron.d/showpaths_export c
8  etc/cron.d/showpaths_export cr
9  etc/cron.d/showpaths_export m
10 usr/local/bin/as_cert_renewal a
11 usr/local/bin/as_cert_renewal c
12 usr/local/bin/as_cert_renewal cr
13 usr/local/bin/as_cert_renewal m
14 usr/local/sbin/showpaths_prom a
15 usr/local/sbin/showpaths_prom c
16 usr/local/sbin/showpaths_prom cr
17 usr/local/sbin/showpaths_prom m
18 ...

```

Listing 7.10: CE_S-Spuren - Einrichtung der automatisierten Skript-Ausführung

Analog zu den Monitoring- und IP-Routing-Services starten sich die SCION- und SIG-Services gemeinsam über Docker Compose (siehe Listing 7.11) als Gruppe gemäss den Definitionen in der jeweiligen Konfigurationsdatei „docker-compose.yml“. Hier nochmals kurz als Erinnerung, die SCION-Gruppe beinhaltet anapaya-dispatcher, anapaya-sd70-9025, anapaya-cs70-9025-2 und anapaya-br70-9025-2 und die SIG-Gruppe anapaya-posix-gateway und anapaya-confagent als containerisierte Anwendungen.

```

1  ...
2  etc/docker-compose/scion a
3  etc/docker-compose/scion c
4  etc/docker-compose/scion cr
5  etc/docker-compose/scion m
6  etc/docker-compose/scion/docker-compose.yml a
7  etc/docker-compose/scion/docker-compose.yml c
8  etc/docker-compose/scion/docker-compose.yml cr
9  etc/docker-compose/scion/docker-compose.yml m
10 etc/docker-compose/sig a
11 etc/docker-compose/sig c
12 etc/docker-compose/sig cr
13 etc/docker-compose/sig m
14 etc/docker-compose/sig/docker-compose.yml a
15 etc/docker-compose/sig/docker-compose.yml c
16 etc/docker-compose/sig/docker-compose.yml cr
17 etc/docker-compose/sig/docker-compose.yml m
18 ...

```

Listing 7.11: CE_S-Spuren - Konfigurationen der SCION- und SIG-Container

Bestätigt durch das Listing 7.12 befinden sich im selben Verzeichnis „/etc“ parallel zu den Monitoring- und IP-Routing-Services auch die Konfigurationsdateien von SCION und SIG. Wie schon diskutiert nehmen wir in den Unterverzeichnissen von „/etc/scion/*“ die einzelnen Service-Konfigurationen und die Schlüsselmaterialien. Über den möglichen Inhalt der Dateien wurde bereits früher gesprochen.

```
1  ...
2  etc/scion a
3  etc/scion c
4  etc/scion cr
5  etc/scion m
6  etc/scion/br70-9025-2 a
7  etc/scion/br70-9025-2 c
8  etc/scion/br70-9025-2 cr
9  etc/scion/br70-9025-2 m
10 etc/scion/br70-9025-2/br.toml a
11 etc/scion/br70-9025-2/br.toml c
12 etc/scion/br70-9025-2/br.toml cr
13 etc/scion/br70-9025-2/br.toml m
14 etc/scion/common70-9025 a
15 etc/scion/common70-9025 c
16 etc/scion/common70-9025 cr
17 etc/scion/common70-9025 m
18 etc/scion/common70-9025/certs a
19 etc/scion/common70-9025/certs c
20 etc/scion/common70-9025/certs cr
21 etc/scion/common70-9025/certs m
22 etc/scion/common70-9025/certs/ISD70-B1-S1.trc a
23 etc/scion/common70-9025/certs/ISD70-B1-S1.trc c
24 etc/scion/common70-9025/certs/ISD70-B1-S1.trc cr
25 etc/scion/common70-9025/certs/ISD70-B1-S1.trc m
26 etc/scion/common70-9025/crypto a
27 etc/scion/common70-9025/crypto c
28 etc/scion/common70-9025/crypto cr
29 etc/scion/common70-9025/crypto m
30 etc/scion/common70-9025/crypto/as a
31 etc/scion/common70-9025/crypto/as c
32 etc/scion/common70-9025/crypto/as cr
33 etc/scion/common70-9025/crypto/as m
34 etc/scion/common70-9025/crypto/as/cp-as.key a
35 etc/scion/common70-9025/crypto/as/cp-as.key c
36 etc/scion/common70-9025/crypto/as/cp-as.key cr
37 etc/scion/common70-9025/crypto/as/cp-as.key m
38 etc/scion/common70-9025/crypto/as/cp-as.pem a
39 etc/scion/common70-9025/crypto/as/cp-as.pem c
40 etc/scion/common70-9025/crypto/as/cp-as.pem cr
41 etc/scion/common70-9025/crypto/as/cp-as.pem m
42 etc/scion/common70-9025/keys a
43 etc/scion/common70-9025/keys c
44 etc/scion/common70-9025/keys cr
45 etc/scion/common70-9025/keys m
46 etc/scion/common70-9025/keys/master0.key a
47 etc/scion/common70-9025/keys/master0.key c
48 etc/scion/common70-9025/keys/master0.key cr
49 etc/scion/common70-9025/keys/master0.key m
50 etc/scion/common70-9025/keys/master1.key a
51 etc/scion/common70-9025/keys/master1.key c
52 etc/scion/common70-9025/keys/master1.key cr
53 etc/scion/common70-9025/keys/master1.key m
54 etc/scion/common70-9025/topology.json a
55 etc/scion/common70-9025/topology.json c
56 etc/scion/common70-9025/topology.json cr
57 etc/scion/common70-9025/topology.json m
58 etc/scion/confagent a
59 etc/scion/confagent c
60 etc/scion/confagent cr
61 etc/scion/confagent m
62 etc/scion/confagent/confagent.toml a
63 etc/scion/confagent/confagent.toml c
64 etc/scion/confagent/confagent.toml cr
65 etc/scion/confagent/confagent.toml m
66 etc/scion/cs70-9025-2 a
67 etc/scion/cs70-9025-2 c
68 etc/scion/cs70-9025-2 cr
```

```

69  etc/scion/cs70-9025-2 m
70  etc/scion/cs70-9025-2/cs.toml a
71  etc/scion/cs70-9025-2/cs.toml c
72  etc/scion/cs70-9025-2/cs.toml cr
73  etc/scion/cs70-9025-2/cs.toml m
74  etc/scion/dispatcher a
75  etc/scion/dispatcher c
76  etc/scion/dispatcher cr
77  etc/scion/dispatcher m
78  etc/scion/dispatcher/dispatcher.toml a
79  etc/scion/dispatcher/dispatcher.toml c
80  etc/scion/dispatcher/dispatcher.toml cr
81  etc/scion/dispatcher/dispatcher.toml m
82  etc/scion/quic a
83  etc/scion/quic c
84  etc/scion/quic cr
85  etc/scion/quic m
86  etc/scion/quic/tls.csr a
87  etc/scion/quic/tls.csr c
88  etc/scion/quic/tls.csr cr
89  etc/scion/quic/tls.csr m
90  etc/scion/quic/tls.key a
91  etc/scion/quic/tls.key c
92  etc/scion/quic/tls.key cr
93  etc/scion/quic/tls.key m
94  etc/scion/quic/tls.pem a
95  etc/scion/quic/tls.pem c
96  etc/scion/quic/tls.pem cr
97  etc/scion/quic/tls.pem m
98  etc/scion/sd70-9025 a
99  etc/scion/sd70-9025 c
100 etc/scion/sd70-9025 cr
101 etc/scion/sd70-9025 m
102 etc/scion/sd70-9025/sd.toml a
103 etc/scion/sd70-9025/sd.toml c
104 etc/scion/sd70-9025/sd.toml cr
105 etc/scion/sd70-9025/sd.toml m
106 etc/scion/showpaths_mon.yml a
107 etc/scion/showpaths_mon.yml c
108 etc/scion/showpaths_mon.yml cr
109 etc/scion/showpaths_mon.yml m
110 etc/scion/sig a
111 etc/scion/sig c
112 etc/scion/sig cr
113 etc/scion/sig m
114 etc/scion/sig/sig.default.json a
115 etc/scion/sig/sig.default.json c
116 etc/scion/sig/sig.default.json cr
117 etc/scion/sig/sig.default.json m
118 etc/scion/sig/sig.json a
119 etc/scion/sig/sig.json c
120 etc/scion/sig/sig.json cr
121 etc/scion/sig/sig.json m
122 etc/scion/sig/sig.toml a
123 etc/scion/sig/sig.toml c
124 etc/scion/sig/sig.toml cr
125 etc/scion/sig/sig.toml m
126 ...

```

Listing 7.12: CE_S-Spuren - Konfigurationen der SCION- und SIG-Services

Abschliessend stellten wir nebst den zuvor erkannten Netzwerkschnittstellen-Konfigurationen z. B. anhand den Dateien „/etc/network/interfaces.d/ens1f0“, „etc/network/interfaces.d/ens1f1“ und „etc/network/interfaces.d/lo“ zusätzliche an Bedingungen geknüpfte Netzwerkeinstellungen. Grundsätzlich gibt es zwei Methoden für solche Konfigurationen. So wie das Ubuntu-Wiki empfehlen wir, bei Servern und

Routern meist nicht den NetworkManager. Wir legen z. B. beim SIG grossen Wert auf eine präzise Kontrolle aller Netzwerk-Eigenschaften, daher registrieren wir wie im Listing 7.13 veranschaulicht, eine Konfigurationserweiterung über den sogenannten ifupdown-Mechanismus. Anhand dem Dateinamen „/etc/network/if-up.d/sig“ sind wohl einige Bedingungen oder Erweiterungen an das SIG-Netzwerkinterface geknüpft.

```

1  ...
2  etc/network/if-up.d a
3  etc/network/if-up.d c
4  etc/network/if-up.d m
5  etc/network/if-up.d/sig a
6  etc/network/if-up.d/sig c
7  etc/network/if-up.d/sig cr
8  etc/network/if-up.d/sig m
9  ...

```

Listing 7.13: CE_S-Spuren - Konfiguration der SIG-Netzwerkschnittstelle

Angeichts der beschriebenen Unschönheiten, wurde bei dieser differenzierten Analyse, ergänzend eine manuelle allgemeine Sichtung²² durchgeführt. Das Ziel war, die Aufdeckung von übersehenen wichtigen SCION-Installationsspuren. Die gemachte Aussage ist nun bestätigt. Da während dem Aufsetzen sehr viele temporäre Dateien erzeugt werden, sind sie wie angenommen, nicht in den charakteristischen Spuren zu finden. Dem Anschein nach kann in unserem Fall darüber hinweggeschaut werden, weil alle relevanten CE-Spuren erfasst und richtig gedeutet wurden. Wir bleiben also bei der Ansicht, dass eine Konsultierung der ME-Spuren oder der Abbilder selbst, bei notwendig werdenden zusätzlichen und detaillierteren Informationen z. B. seitens Container-ID unumgänglich ist. Dies gilt ähnlich auch im zweiten Punkt bezüglich der zu hohen Anzahl von vereinzeltten Spuren. Gemäss Beurteilung, konnten auch dort, alle Aktionen richtig gedeutet werden, doch müssten diese Spuren bei Bedarf nochmals genauer ausgewertet und gegebenenfalls zu den einzelnen CE-Spuren addiert werden.

7.2.3. Charakterische Spuren des SCION Auditing - Lynis Audit Tool

Die meisten Systemmodifikationen, wie wir es in den letzten zwei Schritten gesehen haben, hinterlassen unverkennbare und eindeutige Spuren. Die spannende Frage, die wir uns hier stellen ist, wie sieht es nun bei einem vollautomatisierten Security Audit aus, der vorgeblich nur lesende Abfragen durchführt und seine temporär angelegten Dateien und Reporte wieder vorbildlich hinterher entfernt. Rein theoretisch gesehen, dürften wir keine auffälligen Artefakte mehr vorfinden. Die nachfolgende Formel wird nach Abzug aller uns bekannten fremden Spurenbilder das Geheimnis offenbaren:

$$\underline{\text{CE_A}} = \text{audit.me} - \text{scion.me} - \text{noise.me}$$

Auch hier befindet sich das gesamte Endresultat „CE_A“ als Datei auf der beigelegten CD-ROM mit dem Namen `audit.se`. Es werden nun die wichtigsten Spuren aufgelistet und falls vorhanden die Abweichungen zu den uns bekannten Hintergrundinformationen aufgezeigt. Diesmal finden sie im Unterabschnitt 4.2.4 keine stichwortartige Aufzählung, da die Liste, wie sie sich bestimmt vorstellen können, sehr umfangreich ausfallen würde. Wie gewohnt, folgt mit Teilausschnitten aus den eruierten CE_A-Spuren angemessen die wichtigsten Spuren kurz erläutert.

Wie korrekt angenommen, funktioniert das Lynis Auditing Tool so wie angedacht und entworfen. Das Spurenbild (siehe Listing 7.14) zeigt lediglich wenige Zugriffe auf das Konfigurationsverzeichnis „/etc“

²²Die manuelle Sichtung gilt ganzheitlich aller CE-Spurenbilder (*.se) und wurde hier lediglich einmalig zur Vollständigkeit dokumentarisch festgehalten.

und gewisse Unterverzeichnisse in denen sich von Lynis abgefragte Konfigurationsdateien befinden. Der oberste Eintrag lässt vermuten, dass gewisse Verzeichnisse auf einen Mount-Point überprüft wurden. Diese Vermutung erhärtet sich dank unserem Hintergrundwissen. Aber leider belegen diese Hinweise noch lange keinen durchgeführten Security Audit. Allein schon Administratoren, bei ihrer täglichen Arbeit, könnten diese Spuren hinterlassen haben.

```

1  ...
2  .ismount-test-file  a
3  .ismount-test-file  c
4  .ismount-test-file  cr
5  .ismount-test-file  m
6  ...
7  etc/chrony  a
8  etc/default  a
9  etc/docker-compose  a
10 etc/iproute2  a
11 etc/iptables  a
12 etc/modules-load.d  a
13 etc/network  a
14 etc/process-exporter  a
15 etc/rcS.d  a
16 etc/systemd  a
17 ...

```

Listing 7.14: CE_A-Spuren - Lynis überprüfte System-Konfigurationen

Andere hier nicht aufgeführte und sehr umfangreich ausfallende Spuren, deuten auf Abfragen bezüglich Docker Container und Paketmanagement-System hin. Sie lassen nur dank unseren Kenntnissen gewisse Mutmassungen zu, aber liefern für konkrete Aussagen zu wenig Informationen. Auch diese könnten im täglichen Betrieb auftreten. Jedoch die im Listing 7.15 gezeigten Spuren gestatten, dank der eindeutigen Benennung, eine verlässliche Hypothese. Selbstverständlich können Namen gefälscht oder manipuliert werden und so fehlinterpretiert werden. Das sieht glücklicherweise bei unserer Sache etwas anders aus. Diese eindeutigen und einzigen Spuren belegen den Lynis Audit und zeigen die temporär angelegten Dateien. Nach dem Audit wurden sie allerdings wieder gelöscht.

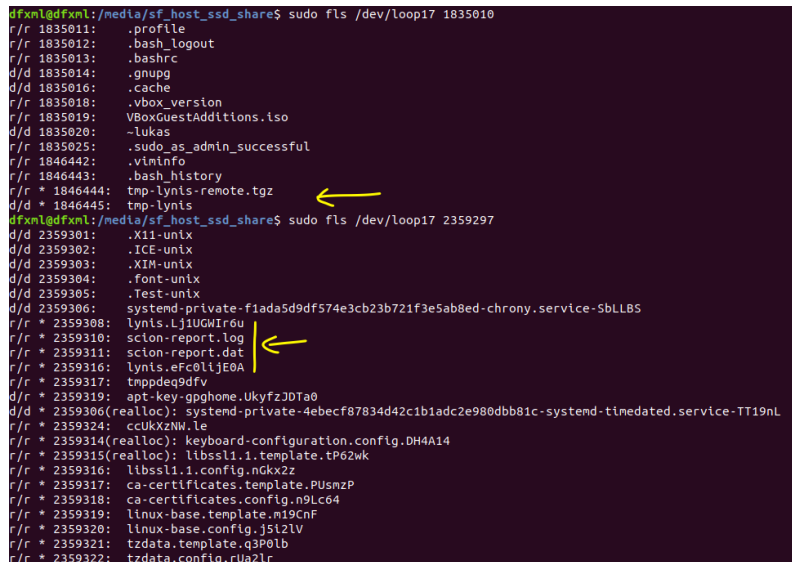
```

1  ...
2  home  a
3  home/anapaya/tmp-lynis  a
4  home/anapaya/tmp-lynis  c
5  home/anapaya/tmp-lynis  cr
6  home/anapaya/tmp-lynis  m
7  home/anapaya/tmp-lynis-remote.tgz  a
8  home/anapaya/tmp-lynis-remote.tgz  c
9  home/anapaya/tmp-lynis-remote.tgz  cr
10 home/anapaya/tmp-lynis-remote.tgz  m
11 ...
12 tmp  a
13 tmp/scion-report.dat  a
14 tmp/scion-report.dat  c
15 tmp/scion-report.dat  cr
16 tmp/scion-report.dat  m
17 tmp/scion-report.log  a
18 tmp/scion-report.log  c
19 tmp/scion-report.log  cr
20 tmp/scion-report.log  m
21 ...

```

Listing 7.15: CE_A-Spuren - Lynis angelegte temporäre Dateien

An dieser Stelle möchte nochmals wegen der Tragweite erwähnt sein, dass viele Spuren bei forensischen Arbeiten nach einem Systemneustart verloren gehen könnten. Erneut veranschaulicht die Abbildung 7.22 die im Nachgang an einen Security Audit entfernten Lynis-Dateien. Sie sind mit hoher Wahrscheinlichkeit nach einem Neustart nicht mehr nachzuweisen und als forensische Spuren verloren. Somit würden die forensischen Analysen deutlich beeinträchtigt und verkompliziert.



```
d/fxmldfxm1:/media/sf_host_ssd_share$ sudo ls /dev/loop17 1835010
r/r 1835011: .profile
r/r 1835012: .bash_logout
r/r 1835013: .bashrc
d/d 1835014: .gnupg
d/d 1835016: .cache
r/r 1835018: .vbox_version
r/r 1835019: VBoxGuestAdditions.iso
d/d 1835020: -lukas
r/r 1835025: .sudo_as_admin_successful
r/r 1846442: .viminfo
r/r 1846443: .bash_history
r/r * 1846444: tmp-lynis-remote.tgz
r/r * 1846445: tmp-lynis
d/fxmldfxm1:/media/sf_host_ssd_share$ sudo ls /dev/loop17 2359297
d/d 2359301: .X11-unix
d/d 2359302: .ICE-unix
d/d 2359303: .XIM-unix
d/d 2359304: .font-unix
d/d 2359305: .Test-unix
d/d 2359306: systemd-private-fiada5d9df574e3cb23b721f3e5ab8ed-chrony.service-SbLLB5
r/r * 2359308: lynis.Lj1UGWIr6u
r/r * 2359310: scion-report.log
r/r * 2359311: scion-report.dat
r/r * 2359316: lynis.eFc0ljE0A
r/r * 2359317: tmpdeq9dfv
d/r * 2359319: apt-key-gpgphone.UkyfzJDta0
d/d * 2359306(realloc): systemd-private-4ebecf87834d42c1b1adc2e980dbb81c-systemd-timedated.service-TT19nL
r/r * 2359324: ccUkXZNW.le
r/r * 2359314(realloc): keyboard-configuration.config.DH4A14
r/r * 2359315(realloc): libssl1.1.template.tP62wk
r/r * 2359316: libssl1.1.config.ncKx2z
r/r * 2359317: ca-certificates.template.PUsnzP
r/r * 2359318: ca-certificates.config.n9Lc64
r/r * 2359319: linux-base.template.n19CnF
r/r * 2359320: linux-base.config.j5t2LV
r/r * 2359321: tzdata.template.q3P0lb
r/r * 2359322: tzdata.config.rUa2Lr
```

Abbildung 7.22.: Lynis Auditing - Temporäre und gelöschte Dateien

7.2.4. Allgemeine (Super)Timeline Analyse

Hinsichtlich der doch eher kargen Spurenausbeute, sowie einiger geklärten Fragestellungen werden wir nun doch noch einen Blick auf die bedeutsamen und interessanten Timelines wagen. Eine eher grosse Datenansammlung ist zu erwarten und eine exakte und geduldige Arbeitsweise ist geboten, da ansonsten elementare Spuren übersehen werden. Beide Timelines haben ihre Vor- und Nachteile. Die Standard-Timeline generiert zusammen mit Mactime einen weniger detaillierteren Bericht. Dank seiner besseren Übersichtlichkeit verhilft er schneller und einfacher zu ersten Anhaltspunkten und Eindrücken. Die Super-Timeline von Plaso ist sehr gehaltvoll und stellt seinen Bericht sehr detailreich aus umfangreichen Quellen nämlich den bekanntesten Logdateien wie Kernel, Syslog, Journal, WTMP, dpkg, APT etc. und den Dateistatus zusammen. Alle wichtigen Informationen sind zentral und sortiert beisammen, aber dabei kann die Übersicht sehr schnell darunter leiden. Es folgt keine detaillierte (Super)Timeline-Untersuchung, da sie zu Redundanzen der bereits gemachten Arbeiten führt und den Rahmen dieser Arbeit sprengen würde. Die Idee dahinter ist eine grobe Verifikation der Spurenbilder und eine Bestätigung der gemachten Annahmen zu erhalten. Die Dateisystemanalyse ist eine komplexe Thematik und daher ist es sehr hilfreich einen Anhaltspunkt zu haben, damit die Analysen sich auf einem gewissen Zeitraum konzentrieren können. Anapaya Systems AG begann am 2. Okt. 2020 sich Gedanken zu machen, wie sie die Abbilder vereinfacht und effizient für die forensischen Analysen aufbereiten möchten. Die Arbeiten fanden während Randzeiten statt und forderten einige Modifikationen und Optimierungen bis zur Auslieferung. Wie wir wissen, konnten schliesslich am 29. Okt. 2020 die SCION-Images fertiggestellt und zur Verfügung gestellt werden.

Während Systeminstallationen dürfen wir wegen fehlendem oder ungenauem Zeitpunkt nicht von verlässlichen Zeitstempeln ausgehen und daher interessiert uns den Installationszeitpunkt sehr, da dieser der erste verlässliche Anhaltspunkt ist. Die nachfolgenden (Super)Timeline-Analysen basieren auf dem reparierten Abbild „audit.1.001“. Der einfache File System Check, mit dem Befehl „stat“, verrät den ungefähren Installationszeitpunkt²³ „2020-10-29 09:08:36“ anhand dem Verzeichnis „/lost+found“, das in der Regel bei der Installation von Linux und beim Einrichten des Laufwerks erstellt wird. Die Timeline-Analysen haben für uns grundsätzlich fünf (5) wichtige Zeitbereiche ergeben, die für die Untersuchungen eine besondere Bedeutung haben. In jedem Bereich fanden demnach gewisse Aktionen statt, die alle ausser die Basisinstallation via Remote-Zugriffe ausgeführt wurden. In den ersten rund 10 Minuten fanden die abschliessenden OS-Installationen und Konfigurationen zum Anapaya Base Image statt. Die abschliessenden Grundkonfigurationen fanden um 09:14:06 Uhr via SSH-Verbindung und bereits mit dem Benutzer „anapaya“ statt. Über Ansibel und Python-Skripts wurden sie und alle darauffolgenden Anpassungen dann auf das System appliziert. Dieser initiale Bereich war zwar nicht Teil der forensischen Untersuchungen, aber trotzdem genug bedeutungsvoll ihn im Bericht festzuhalten. Die grob umrissenen Spuren gaben für die nachfolgenden Timeline-Analysen wichtige Hinweise und Anhaltspunkte.

Base Image „anapaya-base-disk001“

Start: Thu Oct 29 2020 09:08:36

Ende: Thu Oct 29 2020 09:19:56

Im darauffolgenden Zeitbereich führte Anapaya Systems AG hauptsächlich die kundenspezifischen Konfigurationen durch. Wie sie sehen, reichen dank der eingerichteten Automation, rund zwei (2) Minuten aus. Sehr speditiv wurden damals also die bereits zuvor erwähnten Systemmodifikationen vorgenommen. Je nachdem, wie umfangreich die Konfigurationen bei Kunden künftig ausfallen, dürfen wir weiterhin bei Neuinstallationen von ähnlichen Aktionsmengen ausgehen.

SIX Hardened Image „anapaya-configured-SIX-[x]“

Start: Thu Oct 29 2020 12:53:38

Ende: Thu Oct 29 2020 12:55:01

Der letzte SCION-Installationsschritt nahm, wegen den SCION-Dienstprogrammen und zusätzlich installierten Anwendungen, etwas mehr Zeit in Anspruch. Trotzdem konnte sehr zügig die SCION-Installationen und Konfigurationen abgeschlossen werden. Nur mit den zuvor stattgefundenen Tasks kann ein lauffähiger SIG in Betrieb gehen, denn ohne Übergang „SCION \longleftrightarrow IP“ findet keine End-zu-Endkommunikation statt. Anhand der geführten Gespräche mit den SCION-Spezialisten wird sich vermutlich seitens SIG-Architektur noch einiges wandeln. Aufgrund der Kompaktheit werden sich vermutlich die forensischen Spuren in der Art und Weise nicht gravierend verändern.

SIX SCION Image „anapaya-SCION-SIX-[x]“

Start: Thu Oct 29 2020 16:49:36

Ende: Thu Oct 29 2020 16:52:03

Auch ein unbedingt festzuhaltendes Ereignis sind die Modifikationen in der Vorbereitungsphase (P-Phase). Diese vorbereitenden Änderungen resp. P-Aktionen könnten die CE-Spuren etwas verfälscht haben. Bei den differenziellen Dateisystemanalysen sind die SSHD-Konfigurationen verzeichnet und somit festgehalten. Die anderen Dateimodifikationen sind nicht relevant und können dank den Loginformationen vernachlässigt werden. Würden tiefergreifende Analysen anstehen und daraus Herleitungen entstehen, so müssten

²³ Anahnd von Syslog-Einträgen wie „...registered new interface driver usb-storage“ erfolgte die OS-Installation über ein USB-Speicher mittels dem Benutzer „root“. Das Vorgehen wurde auch so seitens Anapaya rückbestätigt.

z. B. das SSH-Login, Passwortänderung und SSHD-Konfigurationsänderungen in den Bericht aufgenommen und erklärt werden. In unserem Fall hatten die zusätzlichen P-Aktionen glücklicherweise keine negativen Seiteneffekte und werden mit hoher Wahrscheinlichkeit auch bei zukünftigen Untersuchungen keine Probleme darstellen.

Preparation Phase „N/A“

Start: Sun Mar 14 2021 16:56:48

Ende: Sun Mar 14 2021 17:02:34

Als zusätzliche Aktionsmenge wählten wir das SCION-Auditing. Vor allem hier war sehr spannend zu sehen, dass das SCION-Benchmarking praktisch keine offensichtlichen Spuren bezüglich den vier (4) Aspekten (New Files, Deleted Files, Modified Contents und Renamed Files) im Dateisystem hinterlässt. Die differenziellen forensischen Analysen sind allgemein sehr interessant und geben schnell gute und verlässliche Indizien auf mögliche ungewollte Dateimodifikationen. Die zuvor gemachte Aussage, kann also diesbezüglich durch die zusätzlichen (Super)Timeline-Analysen bestätigt werden. Jedoch ist in einem weiteren Schritt bei Sicherheitsverletzungen diese Art von forensischen Analysen nicht wegzudenken, denn die zusätzlichen Informationen können Aufschluss über den Spurenhergang geben. In unserem Fall benutzen wir lediglich Linux-Bordmittel. Das kann die Hypothesen bei ungenauen Loginformationen stark beeinträchtigen, da die hinterlassenen Lynis-Auditing-Spuren auch von täglichen Betriebsaufgaben herkommen könnten. Dank unseren Hintergrundkenntnissen würde sich noch immer nur eine vage Aussage gestatten. Da SCION laufend optimiert wird, dürfen wir zudem Verbesserungen bezüglich Logging und Auditing erwarten.

SIX Audited Image „audit.[x]“

Start: Mon Mar 29 2021 17:04:40

Ende: Mon Mar 29 2021 17:17:58

Abschliessend zu den forensischen Analysen, kann mit einem guten Gewissen, die Grundaussage gemacht und somit auch bestätigt werden, dass nur die erwarteten Aktionen ausgeführt und die Spuren korrekt und gesamthaft in den Evidenzen aufgezeichnet wurden. Die wesentlichsten Aspekte sind vermutlich die Beweislast der korrekten Spurensammlungen und die Glaubhaftigkeit der angewendeten Methoden. Die Eigenschaften eines Journal-Dateisystems, wie das verwendete Ext4, sind bekannt. Mit der Timeline-Analyse hat sich wieder gezeigt, dass ein Blickwinkel nur auf die Inode-Metadaten bei manchen Konstellationen zu fehlerbehafteter Interpretation führt. Die Herausforderungen hängen besonders mit gelöschten Daten (deleted/deleted-realloc) zusammen. Dateien mit dem Vermerk „deleted-realloc“ bedeutet eine gelöschte Datei und wiederverwendeter Inode-ID. Eine kontextlose Begutachtung ohne Gesamtsicht aller Zusammenhänge ist sehr schwierig oder praktisch unmöglich.

7.3. Erkenntnisse

Allgemein steigen aufgrund der Digitalisierung die Anforderungen an die IT-Sicherheit. Nicht nur die Systeme und die darauf laufenden Endanwendungen müssen noch sicher gestaltet werden, sondern auch das Transportmedium „Internet“ muss sich stetig weiterentwickeln. Schlussendlich laufen auf einem Netzwerkrouter auch nichts anderes als Anwendungen, aber mit anderen Anforderungen und komplett anderen Funktionalitäten. Mit SCION als das Next Generation Internet möchte SIX und SNB mit Hilfe der ETH Zürich²⁴ den Netzwerktransport für die SIC-Systeme zuverlässiger und sicherer gestalten. Nach der Umsetzung unserer Hardening-Massnahmen prüfen externe und unabhängige Security Partner mit Sicherheitstests (Pen-test) die SCION-Services kontinuierlich auf mögliche Schwachstellen. Mit diesen Sicherheitsvorkehrungen und einer angemessenen Überwachung sollen SCION-Kompromittierungen bestmöglich verhindert oder zumindest festgestellt werden. Kein Unternehmen spricht gerne über Sicherheitsverletzungen, doch leider gibt es keinen 100%-igen Schutz und Vorsorge muss trotz allem frühzeitig getroffen werden.

Als ergänzende Massnahmen leisteten wir, rund ums Thema SCION, durch die vorangegangenen Ausführungen und forensischen Analysen, einen beträchtlichen Beitrag zu den forensischen Dead- und Live-Analysen. Mit relativ einfachen Mitteln und wissenschaftlich anerkannten Methoden (Differential Forensic Analysis und Timeline Analysis) ermittelten wir, mit der Zustandsmethode, erfolgreich die charakteristischen Spuren der jeweiligen SCION-Installationsschritten und dem SCION-Benchmarking. Es entstand sozusagen eine Wissensdatenbank. Sie vereinfacht das zukünftige Ziehen von Schlussfolgerungen oder ermöglicht das effizientere Prüfen von Hypothesen.

Bei den Analysen durften wir uns auf makellose Untersuchungsobjekte verlassen. Somit konnte bei den CE-Spurenermittlungen nahezu auf eine Inhaltsdatenanalyse verzichtet werden. Lediglich Log-Dateien wurden situationsbedingt miteinbezogen. In einigen Problemstellungen benötigte es, insbesondere im Zusammenhang mit gelöschten Dateien, während den differentiellen Analysen fortgeschrittenes Wissen. Vor allem über die Funktionalitäten der forensischen Tools und die Ext4-Dateisystem-Eigenschaften. Während der Arbeit machte sich daher schnell die Notwendigkeit für den Einsatz einer zweiten Analysetechnik erkennbar. Nur so war es möglich, die Glaubwürdigkeit der Spuren abzuschätzen und andererseits die Begründungen herzuleiten und plausibel zu erklären. In bevorstehenden Untersuchungen müssen diese Punkte und selbstverständlich auch mögliche Verschleierungstechniken (Anti-Forensik) stets betrachtet und gegebenenfalls miteinbezogen werden. Den Analysen zufolge hatte sich gezeigt, dass die eingeschobenen und leider notwendigen Systemveränderungen in der P-Phase glücklicherweise keine gravierenden Seiteneffekte auf die CE-Spurenbilder hatten. Die privaten SSH-Keys standen nicht zur Verfügung und ein SSH-Login mit Passwort war nicht gestattet. Fortan sind auf solche Massnahmen unbedingt zu verzichten und dürfen in der Produktion nicht mehr notwendig sein. Infolge der erlangten SCION-Vorkenntnisse, aus dem Bereich der Applikationsanalysen, konnten dann die Spuren richtig gedeutet und verifiziert werden.

Das SCION-Konstrukt kann für Laien, auf dem System selbst, sehr komplex ausschauen, aber grundsätzlich wurde es sehr übersichtlich und schlank konzipiert. Der Docker Container-basierte Ansatz wirkt sich positiv auf die vorgefundenen CE-Spurenbilder aus. Dank der UNIX-Eigenschaft - alles ist eine Datei - kann fast jedes Artefakt eindeutig einer Konfigurationsänderung oder Aktion zugewiesen werden. Die einzige Interpretationsschwierigkeit liegt bei Anwendungsinstallationen, da dort unzählige Daten wie z. B. Bibliotheken installiert werden und praktisch nicht den Programmen zugeordnet werden können. Daher ist eine ganzheitliche Systemsicht, so wie es eine Supertimeline liefert, in Untersuchungen als empfehlenswerte Methode nicht wegzudenken. Für Detailinformationen bleibt natürlich eine Konsultation der Inhaltsdaten immer noch notwendig. Sehr spannend sind die forensischen Resultate nach einem Lynis Audit. Durch das SCION Benchmarking, wird wegen den umfangreichen Tests, auf sehr viel Dateien zugegriffen und abge-

²⁴<https://nzzas.nzz.ch/wissen/internet-architektur-scion-wie-die-eth-das-netz-sicherer-macht-ld.1489169?reduced=true>

fragt. Das wirkt sich eindeutig und auffällig auf den A-Zeitstempel (Last Data Access) aus. Lynis verwendet für seine Prüfungen erhöhte Berechtigungen (sudo) und lediglich die systemeigenen Linux-Bordmittel oder die bereits vorinstallierten Anwendungen wie z. B. Docker und Docker Compose. So wie alle anderen Anwendungen mit erhöhten Berechtigungen steht auch Lynis einen erhöhten Schutz gegen Manipulation zu. Verbliebene Artefakte gibt es grundsätzlich nicht, da im Nachgang alle temporären Dateien wieder bereinigt werden.

Ergänzend zu diesem abschliessenden Schwerpunkt möchten noch ein paar wichtige und unerwähnte Punkte auf den Weg zur erfolgreichen SCION-Integration bei SIX mitgegeben werden:

- * SCION Forensic Readiness²⁵
- * SCION Container Forensics²⁶
- * SCION Forensic Knowledge Base²⁷
- * SCION Memory Forensics
- * SCION Forensic Optimizations

Die obere Liste ist keinesfalls vollständig anzusehen, denn sie verfolgt lediglich das Ziel, nochmals wichtige, abzuschliessende Themen anzudeuten oder weitere unbearbeitete Punkte auf den Tisch zu bringen. Die digitale Forensik besteht aus sechs (6) Hauptbereichen²⁸ und nebst den vielen anderen Cyber Security Themen ist es ein eigener, sehr umfangreicher Bereich. Es wird immer eine noch sicherere und widerstandsfähigere SCION-Infrastruktur angestrebt und daher soll die SCION Forensik nicht vernachlässigt, stets ausgebaut und optimiert werden.

²⁵Der SIC-Service untersteht bekanntlich den Regularien der FINMA und daher ist eine formale Überprüfung der Forensic Readiness innerhalb der SIX geboten. Gegebenenfalls sind daraus Massnahmen zu definieren und Anpassungen vorzunehmen.

²⁶Um infizierte SCION Container zu identifizieren, Komponenten zu erfassen und sicher zu analysieren, ist ein Verständnis für die Vergänglichkeit und Isolation von Containern erforderlich. Viele Unternehmen sind sich den „neuen“ Herausforderungen resp. Änderungen nicht klar bewusst und daher benötigt es im SOC erweiterte Methodiken bezüglich Incident Response und Forensics.

²⁷Unter diesem Punkt sind Vervollständigungen oder Erweiterungen der Wissensdatenbank angesprochen. Das untersuchte SIG war nach seiner Inbetriebnahme bisher noch nicht im produktiven Einsatz. Auch alle anderen SCION-Services sind noch ausstehend und sollen mit ihren Spurenbilder die Datenbank bereichern.

²⁸Reverse Engineering, Memory Forensics, Network Forensics, Mobile Forensics, Cloud Forensics und Post Mortem/Disk Forensics

FAZIT

Ziel dieser Arbeit war es ein SCION Security Benchmark and Forensics Framework aufzubauen und ein SCION Audit Tool zu implementieren, welches mit SCION-abgestimmten Sicherheitstests OS-agnostisch das Hardening vom Betriebssystem und der SIG Services überprüft und bewertet.

Die kurze Einführung in die SCION Internet Architektur und das vermittelte Grundlagenwissen über die SCION Services ermöglicht den Sicherheitsexperten aus unterschiedlichsten Bereichen den notwendigen und dadurch schnellen, sowie vereinfachten Einstieg in die Welt von SCION beim Endkunden. Der praxisnahe Ansatz veranschaulicht klar, verständlich und fokussiert die potentiellen Angriffsflächen anhand der Implementierungsart von SCION. Die Weichen und der Fokus können so in zukünftigen Erweiterungen, Optimierungen und Sicherheitsüberprüfungen effizienter und besser gewählt werden.

Alle SCION-relevanten Sicherheitskontrollen (Security Controls) wurden vor allem mit Hilfe der globalen IT Community (CIS) ausgearbeitet. Das automatisierte SCION Security Auditing wurde mit dem Open Source Tool „Lynis“ realisiert. Es verfügte bereits out-of-the-box über viele von den benötigten Kontrollen und unterstützt die gängigsten UNIX-Betriebssysteme. Aufgrund der umfangreichen und unverzichtbaren Sicherheitschecks war eine Beschränkung auf das Wesentlichste notwendig. Bei der Ausarbeitung der Tests wurde daher besonders auf die Erweiterbarkeit und Portierbarkeit geachtet. Enterprise Unternehmen wie SIX setzen oftmals auf Produkte von namhaften Herstellern wie Tripwire. Die gewählten Controls können damit relativ einfach übernommen oder abgelöst werden.

Der ausgiebige Sicherheitscheck des Ubuntu-Betriebssystems zeigte grundsätzlich aus Sicht eines gehärteten Serversystems eine solide und relativ sichere Konfiguration. Ein Serversystem steht grundsätzlich immer mit einem Basisschutz hinter einer DMZ-Firewall. Das SIG wird aber konzeptionell meistens exponiert in der Access Platform (AP) platziert und benötigt daher zusätzliche Hardening- und Überwachungsmaßnahmen. Sehr ähnlich ergeht es den Sicherheitsüberprüfungen der SCION Services. Es gibt einige essenzielle und sicherheitsrelevante Punkte, die nochmals überarbeitet, justiert oder angemessen aktiviert werden müssen. Ein massgeblicher zusätzlicher Beitrag an die Sicherheit resp. Systemstabilität gäbe ein adäquates aktives Docker-Audit-Logging, restriktivere Zugriffsregeln (z. B. Filterung mittels ACLs), strengere Container-Berechtigungen (Privileges/Capabilities), strengere Dateizugriffsberechtigungen auf die SCION-Service-Spezifikationen und eine Begrenzung des Systemressourcenverbrauchs. Bei manchen kundenspezifischen Einstellungen ist eine manuelle und/oder zusätzlich Prüfung unumgänglich. Leider können nicht alle Verbesserungsvorschläge direkt ohne vorherige Acceptance Tests in die finale Konfiguration übernommen werden, da einige Massnahmen das System mehr auslasten und womöglich negativ beeinflussen oder den operativen Betrieb markant erschweren können. Zudem empfiehlt es sich, schon in einem frühen Stadium bei der SCION Integration, an eine Überwachung durch das SOC zu denken. Nur so können bereits in der Pilotphase die ersten Erfahrungen gesammelt und die Lernkurve massgeblich gesteigert werden. Da etliche Optimierungspunkte aufgedeckt wurden, erscheint momentan die OS-Basiskonfiguration und der Schutz bezüglich SCION Services noch nicht ideal abgestimmt zu sein, um die Anforderungen einer vollumfäng-

lichen SIX Compliance zu erfüllen. Schlussendlich schützt nur eine ganzheitliche Sicherheitskonfiguration mit einem entsprechenden Logging, Monitoring und Alerting das SIG effektiv gegen Cyber Angriffe. Abschliessend zu diesem Themenbereich „SCION Security Benchmark“ möchte lobenswert erwähnt werden, dass bereits während der Thesis-Ausarbeitung einige Verbesserungen wie z. B. die Anbindung an das Docker-Repository über JFrog Artifactory erfolgreich in der Praxis bei der SIX umgesetzt werden konnten. Auch an kritischeren Massnahmen wie das Einschränken von Ressourcenlimits gegen mögliche DDoS Angriffe wird bereits gearbeitet.

Im Themenbereich „SCION Forensics Framework“ wird sozusagen mit einer forensischen Wissensdatenbank gestartet und die ersten SCION Artefakte gewonnen. Wie bekannt stand für diese Arbeit ein funktionsfähiges SIG mit kundenspezifischer SIX-Konfiguration zur Verfügung. Jedoch konnten nicht alle SCION Services ohne die entsprechenden Netzwerkschnittstellen zum Border Router gestartet werden. Die Thesis beschränkt sich daher vorerst auf eine praktische Anwendungsanalyse und eine limitierte Post-mortem-Analyse. Mit der Anwendungsanalyse wird einem Forensiker die Einarbeitung in die SCION Thematik vereinfacht und beschleunigt. Infolge der detaillierten Dateisystemanalyse wurden anhand von Artefakten die eindeutigen, strukturierten und übersichtlichen SCION Service Installationen und Konfigurationen untermauert. Im Vergleich zu herkömmlichen Anwendungen hinterlässt SCION sehr wenige Spuren. Aufgrund der Eigenheiten und Tücken des Ext4-Dateisystems wurden die Analysen merklich erschwert und erforderten zur Stärkung der Glaubwürdigkeit ergänzend zur Differential Forensic Analysis eine zweite (2) anerkannte Methode. Mittels der Supertimeline konnte nebst der Festigung der persistenten Spuren auch die zeitlichen Aspekte aufgezeigt werden. Diese Kenntnisse verhelfen bereits sehr zur Unterscheidung von SCION Spuren. Die erfolgreich ausgewerteten Spurenbilder veranschaulichen jegliche Spuren der drei (3) Installations- und Konfigurationsschritte, die durch einen SCION Integrator oder Administrator seitens Anapaya Systems AG bei der SIG Inbetriebnahme hinterlassen wurden. Dank diesen Informationen können die Arbeitsschritte bestätigt, nachgewiesen, sowie mögliche Abweichungen künftig erkannt werden. Diese Informationen unterstützen und beschleunigen zukünftige forensische Untersuchungen nach einem Sicherheitsvorfall. Eine zusätzlich wichtige Untersuchung stand dem SCION Auditing Tool zu. Durch diese Analysen konnten zwei (2) bedeutsame Aussagen belegt werden. Es kann definitiv bestätigt werden, dass keine Konfigurationsänderungen (read-only) verursacht werden und die SCION Appliance nicht durch Lynis kompromittiert wird. Das ist eine essenzielle Feststellung und Grundvoraussetzung für das weitere Bestehen der Auditing-Lösung.

AUSBLICK

Mit der Arbeit wurde einen sehr hohen Stellenwert auf die praxisnahe SCION Integration bei den Endkunden gelegt. Für eine vollumfängliche Sicherheitsüberprüfung sind mehrere hundert von Security Controls notwendig. In der zur Verfügung gestandenen Bearbeitungszeit gehörte den sicherheitsrelevantesten Empfehlungen die Aufmerksamkeit. Bei zukünftigen Weiterentwicklungen sind weiterführende Kontrollen und eine automatisierte Umsetzung der Hardening-Richtlinien vorstellbar. Es empfiehlt sich bereits im Entwicklungs- und Implementationsprozess die Massnahmen weiterzuentwickeln, auszutesten und umzusetzen. Sodass beim Endkunden nur noch anhand dem Audit-Report gegebenenfalls die Feinjustierungen durchzuführen sind.

Als Teil der Thesis waren einst drei (3) Cyber Security Themenschwerpunkte angedacht. Angesichts der Grösse und Komplexität der Themenbereiche musste auf die Bearbeitung bezüglich SCION Penetration Testing verzichtet werden. Wie geschildert, sind wiederkehrende Pentests in der Praxis nicht mehr wegzudenken und sie sind teilweise bereits fest in Enterprise Unternehmen prozessual verankert. Da SCION noch immer in der Entwicklung ist und das tiefgründige Wissen und die Erfahrungen in der Industrie fehlen, empfiehlt sich daher eine Wiederaufnahme. Mit erprobten Systemen entwickelt und aufgebaut durch Insiderwissen von SCION Experten, könnte dies zukünftig eine Art von Zertifizierung seitens Anapaya Systems AG bedeuten. Die ausgelieferten SCION Appliance erhält durch die ausgiebigen Sicherheitsüberprüfungen sozusagen ein Gütesiegel.

Unter dem Thema SCION Forensics konnte erfolgreich mit einer Wissensdatenbank gestartet werden, die zukünftige Untersuchungen von Sicherheitsverletzungen bereits merklich unterstützten. Die Forensik besteht aus sechs (6) Hauptbereichen und daher empfiehlt es sich in weiterführenden Arbeiten die Post-mortem-Analyse durch Ermittlung der persistenten Spuren eines produktiven SIG abzuschliessen und noch unbeachtete SCION Services aufzunehmen. Gelöschte Daten mit Fokus auf SCION sind noch unerforscht und würden die Wissensdatenbank zusätzlich bereichern. Nebst den bekannten Methoden des File Carvings bietet das Ext4-Journaling gewisse forensische Vorteile. Historische Informationen¹ werden im Journal gehalten und könnten dafür nützlich sein. Im Bereich der Anwendungsanalysen beschränkte sich die Arbeit vorerst auf SICON in funktioneller Hinsicht. Damit noch mehr über die SCION Services auf der Appliance in Erfahrung gebracht werden kann, erscheint es als angemessen die Services vertiefter im Arbeitsspeicher zu betrachten und zu dokumentieren. Es zeigt sich immer wieder, dass ein adäquates Logging, Monitoring und Alerting zusammen mit entsprechenden Anwendungsfällen im SOC unentbehrlich sind. Die generelle Integrität muss bewahrt werden und daher ist es erforderlich sich laufend über Optimierungen² auch Gedanken zu machen und einzuführen.

¹Erweiterte Analysen des Ext4-Dateisystem-Journals [<https://unix.stackexchange.com/questions/245129/what-kind-of-d-ata-is-stored-in-the-ext4-file-systems-journal>]

²Ansatz zum Schutz der Logging-Informationen [https://www.researchgate.net/publication/2363097_Forward_Integrity_For_Secure_Audit_Logs]

Abkürzungsverzeichnis

ACL	Access Control List
AD	Autonomous Domain
AIDE	Advanced Intrusion Detection Environment
API	Application Programming Interface
AP	Access Platform
APT	Advanced Packaging Tool
AS	Autonomous System
BFD	Bidirectional Forwarding Detection
BGPsec	BGP Security Extension
BGP	Border Gateway Protocol
BIOS	Basic Input/Output System
BR	Border Router
BS	Beacon Server
CA	Certificate Authority
CDN	Content Delivery Network
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity and Availability
CIS	Center for Internet Security
COVID-19	Coronavirus Disease 2019
CP-PKI	Control Plane PKI
CP	Control Plane
CRL	Certificate Revocation List
CS	Control Services
CVE	Common Vulnerabilities and Exposures
DDoS	Distributed Denial of Service

DMZ	Demilitarized Zone
DNSsec	DNS Security Extensions
DNS	Domain Name System
DP	Data Plane
DRKey	Dynamically Recreable Key
ETH	Eidgenössischen Technische Hochschule
FIA	Future Internet Architecture
FINMA	Eidgenössischen Finanzmarktaufsicht
FTP	File Transfer Protocol
GRUB	Grand Unified Bootloader
HA	High Availability
HE	Hop Entry
HF	Hop Field
HPS	Hidden Path Server
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol Secure
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
ICN	Information Centric Networking
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
INF	Info Field
IPsec	Internet Protocol Security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IP	Internet Protocol
ISD	Isolation Domain
ISO	International Organization for Standardization

ISP	Internet Service Provider
ITU	International Telecommunication Union
IT	Informationstechnik
JSON	JavaScript Object Notation
LSM	Layered Security Masterplan
MAC	Message Authentication Code
MD5	Message-Digest Algorithm 5
MITM	Man in the Middle
MPLS	Multiprotocol Label Switching
MTU	Maximum Transmission Unit
NDN	Named Data Networking
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSM	Network Security Masterplan
NTP	Network Time Protocol
OPT	Origin and Path Trace
OSPF	Open Shortest Path First
OS	Operating System
PAM	Pluggable Authentication Modules
PCB	Path-Segment Construction Beacon
PCFS	Packet-Carried Forwarding State
PCI-DSS	Payment Card Industry - Data Security Standard
PCI	Payment Card Industry
PIM-SM	Protocol Independent Multicast - Sparse Mode
PKI	Public-Key Infrastructure
PnP	Preproduction and Production
PoC	Proof of Concept
PVF	Path Validation Field
QoS	Quality of Service
QUIC	Quick UDP Internet Connections
RFC	Request for Comments

RHEL	Red Hat Enterprise Linux
RINA	Recursive InterNetwork Architecture
Rlogin	Remote login
RPC	Remote Procedure Call
RPKI	Resource Public Key Infrastructure
RSH	Remote Shell
RTT	Round-Trip Time
SCB	Secure Configuration Baseline
SCCM	SCION Supply Chain Management
SCION	Scalability, Control, and Isolation On Next-Generation Networks
SCMP	SCION Control Message Protocol
SCP	Secure Copy Protokoll
SDN	Software-Defined Networking
SHA	Secure Hash Algorithm
SIBRA	Scalable Internet Bandwidth Reservation Architecture
SIEM	Security Information and Event Management
SIG	SCION IP Gateway
SIX	Swiss Stock Exchange
SNB	Schweizerische Nationalbank
SNMP	Simple Network Management Protocol
SOC	Security Operations Center
SQL	Structured Query Language
SSFN	Secure Swiss Finance Network
SSH	Secure Shell
SSL	Secure Socket Layer
SVC	Service Address
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SWITCH	Schweizer Wissenschaftsnetzes der Hochschulen
TCB	Trusted Computing Base
TCP	Transmission Control Protocol
TLS	Transport Layer Security

TRC	Trusted Root Configuration
TTL	Time to Live
TTM	Time-to-Market
UDP	User Datagram Protocol
UEFI	Unified Extensible Firmware Interface
UNIX	Uniplexed Information and Computing Service
UTM	Unified Threat Management
VM	Virtual Machine
vPC	Virtual Personal Computer
VPN	Virtual Private Network
WAN	Wide Area Network
XIA	eXpressive Internet Architecture
XML	Extensible Markup Language
ZISC	Zurich Information Security and Privacy Center

LITERATUR

- [1] Pascal Ackerman. *Industrial Cybersecurity: Efficiently secure critical infrastructure systems*. Packt Publishing, Okt. 2017. ISBN: 9781788395984. URL: <https://books.google.ch/books?id=Fh1KDwAAQBAJ>.
- [2] M. Ambrosin et al. „Security and Privacy Analysis of National Science Foundation Future Internet Architectures“. In: *IEEE Communications Surveys Tutorials* 20.2 (Jan. 2018), S. 1418–1442. ISSN: 1553-877X. DOI: 10.1109/COMST.2018.2798280.
- [3] Marc Ammann et al. *SSFN ISD Operations*. Techn. Ber. SIX Group Services AG, Apr. 2021.
- [4] Simeon Blatchley. *SANS Hardening Linux Systems*. Jan. 2016. URL: <https://www.sans.org/score/checklists/linux>.
- [5] Brian Carrier. *File System Forensic Analysis*. Addison-Wesley Professional, März 2005. ISBN: 0321268172.
- [6] Chen Chen et al. „HORNET: High-speed Onion Routing at the Network Layer; Proceedings of the ACM Conference on Computer and Communications Security (CCS)“. In: *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security - CCS '15* (Okt. 2015). DOI: 10.1145/2810103.2813628. URL: <http://dx.doi.org/10.1145/2810103.2813628>.
- [7] Jiachen Chen et al. „Exploiting ICN for Efficient Content Dissemination in CDNs“. In: *2016 Fourth IEEE Workshop on Hot Topics in Web Systems and Technologies (HotWeb)*. Okt. 2016, S. 14–19. DOI: 10.1109/HotWeb.2016.11.
- [8] Zhe Chen et al. „NEW IP Framework and Protocol for Future Applications“. In: *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*. Apr. 2020, S. 1–5. DOI: 10.1109/NOMS47738.2020.9110352.
- [9] Jonathan Lewis Christopherson et al. *CIS Ubuntu Linux 18.04 LTS Benchmark*. März 2020. URL: https://www.cisecurity.org/benchmark/ubuntu_linux/.
- [10] Mauro Conti et al. „The Road Ahead for Networking: A Survey on ICN-IP Coexistence Solutions“. In: *IEEE Communications Surveys Tutorials* 22.3 (Mai 2020), S. 2104–2129. DOI: 10.1109/COMST.2020.2994526.
- [11] Robert G Byrnes Daniel J Barrett Richard E Silverman. *Linux Security Cookbook*. 9780596003913. O'Reilly Media, Juni 2003. URL: <https://www.oreilly.com/library/view/linux-security-cookbook/0596003919/>.
- [12] Andreas Dewald und Felix Freiling. *Grundlagen digitaler Forensik*. 3. Aufl. Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Jan. 2017.
- [13] Andreas Dewald und Sabine Seufert. „AFEIC: Advanced forensic Ext4 inode carving“. In: *Digital Investigation* 20 (März 2017). DFRWS 2017 Europe, S83–S91. ISSN: 1742-2876. DOI: <https://doi.org/10.1016/j.diin.2017.01.003>. URL: <https://www.sciencedirect.com/science/article/pii/S1742287617300270>.

- [14] W. Ding, Z. Yan und R. H. Deng. „A Survey on Future Internet Security Architectures“. In: *IEEE Access* 4 (Juli 2016), S. 4374–4393. ISSN: 2169-3536. DOI: 10.1109/ACCESS.2016.2596705.
- [15] Y. Diogenes und E. Ozkaya. *Cybersecurity - Attack and Defense Strategies: Infrastructure security with Red Team and Blue Team tactics*. Packt Publishing, Jan. 2018. ISBN: 9781788473859. URL: <https://books.google.ch/books?id=pyZKDwAAQBAJ>.
- [16] *Docker Documentation: Docker Security*. Jan. 2021. URL: <https://docs.docker.com/engine/security/>.
- [17] Ericsson AB 2020. „Future Network Architecture“. In: (Jan. 2020). URL: <https://www.ericsson.com/491de3/assets/local/future-technologies/doc/future-network-architecture-doc.pdf>.
- [18] Rafael Fedler. „Prefix Hijacking-Angriffe und Gegenmaßnahmen“. In: *Network Architectures and Services - Seminar Future Internet SS 2012* 1 (Aug. 2012).
- [19] Simone Ferlin und Michelle Alvarez. „BGP Internet Routing: What Are the Threats?“ In: *Security Intelligence* (Dezember 2017). URL: <https://securityintelligence.com/bgp-internet-routing-what-are-the-threats/>.
- [20] Felix Freiling und Christian Riess. *Browser- und Anwendungsforensik*. 7. Aufl. Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Okt. 2018.
- [21] Felix Freiling und Martin Wundram. *Live Analyse*. 6. Aufl. Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), Apr. 2019.
- [22] Fritz Steinmann et al. *SSFN Abgestimmte Eckpunkte Regelwerk*. Techn. Ber. SIX Group Services AG, Apr. 2021.
- [23] Simson Garfinkel, Alex J. Nelson und Joel Young. „A general strategy for differential forensic analysis“. In: *Digital Investigation* 9 (Aug. 2012). The Proceedings of the Twelfth Annual DFRWS Conference, S50–S59. ISSN: 1742-2876. DOI: <https://doi.org/10.1016/j.diin.2012.05.003>. URL: <https://www.sciencedirect.com/science/article/pii/S174228761200028X>.
- [24] Giacomo Giuliani et al. „COLIBRI: A Collaborative Lightweight Inter-domain Bandwidth-Reservation Infrastructure“. INTERNAL DRAFT. Jan. 2020.
- [25] Aaron Grattafiori. „Understanding and Hardening Linux Containers“. In: *NCC Group Publication* v1.1 (Juni 2016).
- [26] Oliver Guggenbuehl. „Security Configuration Baselines for Docker“. In: *SIX Group Services AG* v1.0.3 (Aug. 2019), S. 45.
- [27] Jesse Hertz. „Abusing Privileged and Unprivileged Linux Containers“. In: *NCC Group Publication* (Juni 2016), S. 53.
- [28] Samuel Hitz. *Network Administrator Training Program - SCION AS Details*. PowerPoint Anapaya Systems AG. Sep. 2020.
- [29] Samuel Hitz. *Network Administrator Training Program - SCION Concepts*. PowerPoint Anapaya Systems AG. Sep. 2020.
- [30] Samuel Hitz. *The SSFN Isolation Domain*. Draft. Anapaya Systems AG, Sep. 2019.
- [31] Wu Jianping, Liu Lili und Li Dan. „The road towards future Internet“. In: *Journal of Communications and Information Networks* 1.1 (Juni 2016). ISSN: 2509-3312. DOI: 10.1007/bf03391548. URL: <http://dx.doi.org/10.1007/BF03391548>.
- [32] Tajinder Kalsi. *Practical Linux Security Cookbook: Secure your Linux environment from modern-day attacks with practical recipes, 2nd Edition*. 2nd Edition. Packt Publishing, Aug. 2018. ISBN: 9781789136005. URL: <https://books.google.ch/books?id=avFsDwAAQBAJ>.
- [33] Ramon Keller. *SSFN PKI Integration Concepts*. Techn. Ber. SIX Group Services AG, Dez. 2020.
- [34] Ramon Keller. *SSFN PKI Integration Risk Analysis*. Techn. Ber. SIX Group Services AG, März 2021.

- [35] Markus Legner et al. „EPIC: Every Packet Is Checked in the Data Plane of a Path-Aware Internet“. In: *29th USENIX Security Symposium (USENIX Security 20)*. USENIX Association, Aug. 2020, S. 541–558. ISBN: 978-1-939133-17-5. URL: <https://www.usenix.org/conference/usenixsecurity20/presentation/legner>.
- [36] Li Richard et al. „Towards a New Internet for the Year 2030 and Beyond“. In: *ITU-T, SG 13* (Juli 2018).
- [37] Chris Matthieu. „Technologische Innovationen 2018: AI, IoT, VR und Robotik“. In: (Jan. 2018). URL: <https://www.computerweekly.com/de/meinung/Technologische-Innovationen-2018-AI-IoT-VR-und-Robotik>.
- [38] Rory Mccune et al. *CIS Docker Benchmark*. März 2020. URL: <https://www.cisecurity.org/benchmark/docker/>.
- [39] R. McKendrick und S. Gallagher. *Mastering Docker*. Third Edition. Packt Publishing, Okt. 2018. ISBN: 9781789616606. URL: <https://books.google.ch/books?id=w6eAvQEACAAJ>.
- [40] Gerhard Mezger. „Layered Security Masterplan“. In: *SIX Group Services AG v1.4* (Dez. 2017), S. 78.
- [41] Gerhard Mezger. „Network Security Masterplan“. In: *SIX Group Services AG v2.8* (Okt. 2020), S. 67.
- [42] Ian Miell und Aidan Hobson Sayers. *Docker in Practice*. ISBN: 9781617292729. Manning Publications Co., Apr. 2016. URL: <https://livebook.manning.com/book/docker-in-practice/chapter-10/26>.
- [43] Adrian Mouat. *Docker Security Using Containers Safely in Production*. O’Reilly Media, Incorporated, Jan. 2016. ISBN: 9781491936603. URL: <https://www.oreilly.com/library/view/docker-security/9781492042297/>.
- [44] Paul Müller und Bernd Reuther. „Future Internet Architecture - A Service Oriented ApproachFuture Internet Architecture - Ein serviceorientierter Ansatz“. In: *it - Information Technology* 50 (Jan. 2008), S. 383–389. DOI: 10.1524/itit.2008.0510.
- [45] Muhammad Ali Naeem, Shahrudin Awang Nor und Suhaidi Hassan. „Future Internet Architectures“. In: *Emerging Trends in Intelligent Computing and Informatics*. Hrsg. von Faisal Saeed, Fathey Mohammed und Nadhmi Gazem. Cham: Springer International Publishing, Nov. 2020, S. 520–532. ISBN: 978-3-030-33582-3.
- [46] Yathi Naik. „Hardening Docker containers, images, and host - security toolkit | StackRox“. In: (Aug. 2017). URL: <https://www.stackrox.com/post/2017/08/hardening-docker-containers-and-hosts-against-vulnerabilities-a-security-toolkit/>.
- [47] John Naughton. „The evolution of the Internet: from military experiment to General Purpose Technology“. In: *Journal of Cyber Policy* 1.1 (Feb. 2016), S. 5–28. DOI: 10.1080/23738871.2016.1157619. URL: <https://doi.org/10.1080/23738871.2016.1157619>.
- [48] J. Pan, S. Paul und R. Jain. „A survey of the research on future internet architectures“. In: *IEEE Communications Magazine* 49.7 (Juli 2011), S. 26–36. ISSN: 1558-1896. DOI: 10.1109/MCOM.2011.5936152.
- [49] Christos Pappas et al. „Transparency Instead of Neutrality“. In: *Proceedings of the 14th ACM Workshop on Hot Topics in Networks - HotNets-XIV* (Nov. 2015). DOI: 10.1145/2834050.2834082. URL: <http://dx.doi.org/10.1145/2834050.2834082>.
- [50] Payment Card Industry (PCI). „PCI Requirements and Security Assessment Procedures“. In: *Data Security Standard v3.2.1* (Mai 2018).
- [51] Adrian Perrig. *Research and private notes on Future Internet Projects*. Juli 2020.
- [52] Adrian Perrig et al. „SCION: A Secure Internet Architecture“. In: *Information Security and Cryptography* (Aug. 2017). ISSN: 2197-845X. DOI: 10.1007/978-3-319-67080-5. URL: <http://dx.doi.org/10.1007/978-3-319-67080-5>.

- [53] Jennifer Rexford und Constantine Dovrolis. „Future Internet Architecture: Clean-Slate Versus Evolutionary Research“. In: *Commun. ACM* 53 (Sep. 2010), S. 36–40. DOI: 10.1145/1810891.1810906.
- [54] Liz Rice. *Container Security: Fundamental Technology Concepts That Protect Containerized Applications*. O'Reilly Media, Incorporated, Apr. 2020. ISBN: 9781492056706. URL: <https://books.google.ch/books?id=6aoSywEACAAJ>.
- [55] Martin Rieger, Patrick Eisoldt und David Schlichtenberger. *Datenträgerforensik*. 6. Aufl. Hochschule Albstadt-Sigmaringen, Juni 2018.
- [56] Martin Rieger, Patrick Eisoldt und David Schlichtenberger. *Unix Forensik*. 2.1. Hochschule Albstadt-Sigmaringen, Aug. 2019.
- [57] Samuel Hitz et al. *TRC Signing Ceremony*. Techn. Ber. Anapaya Systems AG, Apr. 2020.
- [58] Samuel Hitz et al. *Trust Root Configuration (TRC) Specification*. Techn. Ber. Anapaya Systems AG, Juni 2020.
- [59] Society for Worldwide Interbank Financial Telecommunication (SWIFT). „SWIFT Customer Security Controls Framework“. In: (Juli 2019), S. 99.
- [60] Kamila Soucková. „FPGA-based line-rate packet forwarding for the SCION future Internet architecture“. en. Magisterarb. Zurich: ETH Zurich, Sep. 2019. DOI: 10.3929/ethz-b-000372370.
- [61] Murugiah Souppaya, John Morello und Karen Scarfone. *NIST Application Container Security Guide*. en. Sep. 2017. DOI: <https://doi.org/10.6028/NIST.SP.800-190>.
- [62] Fritz Steinmann. *SCION - Eine sichere Internet-Architektur für den Finanzplatz Schweiz*. öffentlich. SIX Group Services AG, Juni 2019.
- [63] Jakub Szefer. *Principles of Secure Processor Architecture Design*. Bd. v13.3. Morgan und Claypool, Okt. 2018. DOI: 10.2200/S00864ED1V01Y201807CAC045.
- [64] Alina Taran und Dmitry Lavrov. „Future internet architecture: Clean-slate vs evolutionary design“. In: *Dostoevsky Omsk State University* 3 (39) (2016), S. 142–151.
- [65] Donald A. Tevault. *Mastering Linux Security and Hardening: Secure Your Linux Server and Protect It from Intruders, Malware Attacks, and Other External Threats*. Packt Publishing, Jan. 2018. ISBN: 9781788620307. URL: <https://books.google.ch/books?id=S3kYtAEACAAJ>.
- [66] Robail Yasrab. „Mitigating Docker Security Issues“. In: (Apr. 2018). URL: <https://arxiv.org/pdf/1804.05039.pdf>.
- [67] Quan Yu et al. „Cybertwin: An Origin of Next Generation Network Architecture“. In: (Apr. 2019). URL: <https://arxiv.org/pdf/1904.11313.pdf>.
- [68] Mauro Zenoni. „SCION's Hidden Paths Design Formal Security Analysis“. en. Magisterarb. Zurich: ETH Zurich, Apr. 2020. DOI: 10.3929/ethz-b-000411121.
- [69] Michał Źy. *The Practical Linux Hardening Guide*. Nov. 2020. URL: <https://github.com/trimstray/the-practical-linux-hardening-guide>.

Abbildungsverzeichnis

1.1. SSFN Certificate Hierarchy / Trusted Root Configuration (nach [29])	3
1.2. Thesisinhaltsübersicht - SCION Security and Forensics Framework	9
1.3. SSFN Pilotaufbau - Interoperabilität zwischen legacy IP und SCION	13
6.1. SCION Packets on the wire	64
6.2. SCION Network Stack (nach [28])	65
6.3. Customer SCION Border Router - Container Overview	66
6.4. Customer SCION Border Router - Services Overview	69
7.1. Berechnung der Spurenmenge verknüpft zu den SCION-Images	97
7.2. TSK mmls - Layout der Festplatten Partitionen	100
7.3. fdisk - Layout der Festplatten Partitionen	101
7.4. Kpartx - Loopback-Geräten-Zuordnung der Partitionen	101
7.5. LVM2 - Einbindung der Partitionen	101
7.6. Ext4magic - Histogramm von gelöschten Dateien	103
7.7. Volume Group Mounting - needs journal recovery	103
7.8. File System Check - Dateisystem-Reparatur	105
7.9. Idifference2 - Fehlermeldung in „deleted_files_sorted“	106
7.10. Summarize Differential - Abschaltung der Sortierfunktion	107
7.11. Idifference2 - Ausschnitt „New files“ der fehlenden Zeitangaben	107
7.12. Idifference2 - Ausschnitt „Deleted files“ der fehlenden Zeitangaben	108
7.13. Fiwalk Hardening Report - Ausschnitt der Datei „process-exporter.prerm“	108
7.14. Fiwalk SCION Report - Ausschnitt der Datei „process-exporter.prerm“	109
7.15. Fiwalk SCION Report - Ausschnitt einer nicht zugewiesenen Datei	109
7.16. TSK fls - Auflistung des Verzeichnisses „/var/lib/dpkg/info“	109
7.17. Forensik Python Skript - Ermittlung der charakteristischen Spuren	111
7.18. Fiwalk Report - Multiple instances of the file	112
7.19. Directory and File Listening - Verification of multiple file instances	113
7.20. Merged Evidences - Zu hohe Anzahl an Spurenerscheinungen	113
7.21. Plaso Storage Information (Extract) - Warnings generated per parser	114
7.22. Lynis Auditing - Temporäre und gelöschte Dateien	128

Tabellenverzeichnis

2.1. Network Security and Privacy (nach [2])	21
4.1. Hardware Spezifikation	38
4.2. Spezifikation der virtuellen Maschinen	39
4.3. Eingesetzte Analyse- und SCION-Softwarestände	41
6.1. Übersicht der verwendeten Protokollen und Services	67
7.1. Vorbereitungen der SCION-Images (Untersuchungsobjekte)	93
7.2. Vorbereitungen der Admin-Workstation	94
7.3. Vorbereitungen der Forensik-Workstations	95
B.1. Inhalt des Datenträgers und der komprimierten Datei	155

LISTINGS

6.1. General Restriction of SCION related traffic using Iptables	78
6.2. Security Options and Capabilities of Containers	81
6.3. Protect host system against insecure containers with Seccomp	84
7.1. Idifference2 Warnings - Multiple instances of the file path	111
7.2. CE_H-Spuren - Ansible Playbook	115
7.3. CE_H-Spuren - SCION Benutzer mit SSH Konfiguration	116
7.4. CE_H-Spuren - Hostnamen-, Netzwerk- und DNS/NTP-Konfigurationen	117
7.5. CE_H-Spuren - Kernelparameter-Änderungen	118
7.6. CE_H-Spuren - Konfigurationen der IP-Router- und Monitoring-Container/Services	118
7.7. CE_S-Spuren - SCION Dienstprogramme und Plugins	120
7.8. CE_S-Spuren - APT-Paketmanagement-System-Log-Dateien	121
7.9. CE_S-Spuren - Patroni Postgresql HA-Cluster-Konfigurationen	121
7.10. CE_S-Spuren - Einrichtung der automatisierten Skript-Ausführung	123
7.11. CE_S-Spuren - Konfigurationen der SCION- und SIG-Container	123
7.12. CE_S-Spuren - Konfigurationen der SCION- und SIG-Services	124
7.13. CE_S-Spuren - Konfiguration der SIG-Netzwerkschnittstelle	126
7.14. CE_A-Spuren - Lynis überprüfte System-Konfigurationen	127
7.15. CE_A-Spuren - Lynis angelegte temporäre Dateien	127

NUTZUNGSVEREINBARUNG



Vereinbarung bezüglich einer Kollaboration und Nutzung der Masterarbeit von Andreas Maurer

Hintergrund

Andreas Maurer beabsichtigt eine Masterarbeit im Bereich Digitaler Forensik zu erarbeiten. Dabei soll ein Sicherheits-Framework erstellt werden, welches ermöglicht, gewisse sicherheitsrelevanten Aspekte sowohl der Implementierung der SCION Infrastruktur als auch deren Interaktion mit dem darunterliegenden Betriebssystem und Drittprogrammen zu analysieren. Kurz, es soll ein Sicherheits-Framework zur Analyse einer «SCION Appliance» erarbeitet werden.

Samuel Hitz, Chief Technology Officer von Anapaya Systems, hat sich bereit erklärt, die Masterarbeit zu betreuen - zusammen mit anderen Betreuern aus dem akademischen Bereich. Anapaya Systems ist der bisher einzige Hersteller einer solchen SCION Appliance. Damit die Arbeit einen höchstmöglichen praktischen Nutzen hat, sollte sie in enger Kollaboration mit Anapaya Systems durchgeführt werden:

- Anapaya Systems verfügt über das grösste Engineering Know-how, Software und Dokumentation im Bereich SCION und dessen Umsetzung
- SIX benutzt die SCION Appliances von Anapaya Systems und hat daher einen grösstmöglichen direkten Nutzen aus den Resultaten dieser Arbeit

Nutzungsvereinbarung

Anapaya Systems unterstützt und betreut Andreas Maurer in folgendem Ausmass:

1. Andreas Maurer erhält vollen Zugriff auf die proprietäre Software und Dokumentation von Anapaya Systems.
2. Anapaya Systems stellt Ingenieure zur Verfügung, welche Andreas Maurer bei seiner Arbeit unterstützen, z. B. durch Erklärungen oder Hilfe mit Design und Implementierung.
3. Samuel Hitz agiert als offizieller Betreuer der Masterarbeit.

Im Gegenzug erhält Anapaya Systems ein uneingeschränktes, nicht exklusives Nutzungsrecht an allen Artefakten (Software und Dokumentation), welche Andreas Maurer als Teil seiner Masterarbeit erarbeitet und produziert. Des weiteren ist es Anapaya Systems erlaubt, das erstellte System eigenständig weiterzuentwickeln.

Zürich, 2. April 2020

Anapaya Systems AG

Handwritten signature of Samuel Hitz in blue ink.

Samuel Hitz
CTO, CO-FOUNDER

SIX Group Services AG

Handwritten signature of Johannes Hadodo in blue ink.

Johannes Hadodo
Head Network Security Services

Handwritten signature of Andreas Maurer in blue ink.

Andreas Maurer
Senior Security Engineer

ELEKTRONISCHE FASSUNG

Auf dem beigelegten Datenträger befinden sich zur Masterthesis „SCION Security Benchmark and Forensics Framework“ folgende Inhalte:

⇒ MD5 (thesis_maurera1.pdf) =

⇒ MD5 (thesis_anhang_maurera1.7z) =

Die komprimierte Datei „thesis_anhang_maurera1.7z“ enthält die Tools und Evidenzen.

Passwort: ssb&ff31052021mdf

Name	Beschreibung
thesis_maurera1.pdf	Elektronisches Exemplar der Masterthesis
Auditing/	Audit-Dateien
A - SCION_SECURITY_AUDITS/	Audit-Log-Dateien und Audit-Videos
B - lynis-v3.0.3_SCION_VERSION/	SCION Security Auditing Tool mit Test-Skripts, Hilfsprogramm und README_SCION
C - lynis-v3.0.3_ORIGINAL_VERSION/	STANDARD Lynis Security Auditing Tool mit Test-Skripts
Forensik/	Forensik-Dateien
A - Evidenzen/	Bildausschnitte, Fiwalk- und Idifference2-Berichte, PE-, ME- und CE/SE-Dateien und (Super)Timeline
B - Python Tool/	Python-Skripte und README_FORENSICS

Tabelle B.1.: Inhalt des Datenträgers und der komprimierten Datei

