HAW HAMBURG

Bachelorarbeit

Hannes Putz

Risiko-Analyse bei der Nutzung von Satelliten-Internet

Fakultät Technik und Informatik
Department Informatik

Faculty of Computer Science and Engineering
Department Computer Science

Hannes Putz

Risiko-Analyse bei der Nutzung von Satelliten-Internet

Bachelorarbeit eingereicht im Rahmen der Bachelorprüfung
im Studiengang *Bachelor of Science Angewandte Informatik*
am Department Informatik
der Fakultät Technik und Informatik
der Hochschule für Angewandte Wissenschaften Hamburg

Betreuender Prüfer: Prof. Dr. Klaus-Peter Kossakowski
Zweitgutachter: Prof. Dr. Jens von Pilgrim

Eingereicht am: 26. Mai 2021

Hannes Putz

Thema der Arbeit

Risiko-Analyse bei der Nutzung von Satelliten-Internet

Stichworte

Satelliten, Internet, Risikoanalyse, Drahtlosnetzwerke, Megakonstellationen

Kurzzusammenfassung

Durch den Einsatz von Satelliten in niedriger Erdumlaufbahn, können die Latenzen der Signale zwischen Boden und Satellit deutlich verringert werden. Deswegen wird der Einsatz von Satelliten-gebundenen Internetzugängen eine realistische Alternative. Die Bachelorarbeit beschäftigt sich mit der Frage, ob bei der Nutzung von Satelliteninternet erhöhte Sicherheitsmaßnahmen ergriffen werden sollten. Hierfür wird eine Risikoanalyse durchgeführt.

Hannes Putz

Title of Thesis

Risk-Analysis for the Usage of Satellite-Internet

Keywords

Satellites, Internet, Risk Analysis, Wireless Networks, Megaconstellations

Abstract

Since Satellite constellations get deployed in a low orbit, the latencies of signals between the ground and the satellite decrease. Therefore the usage of a satellite bound internet connection becomes feasible. The bachelor thesis evaluates the question, whether higher security measurements should be applied while using satellite internet. This is done in a risk analysis.

Inhaltsverzeichnis

Abbildungsverzeichnis

Begriffserklärungen

Megakonstellation - Eine Megakonstellation ist eine sehr große Gruppe von Satelliten, die sich ähnlich sind und gemeinsam an einer Aufgabe arbeiten.

Beam - Ein Beam (Strahl) wird bei Antennen eingesetzt um gezielte Verbindungen zu Empfängern aufzubauen.

ISL - ISL steht für Inter-Satellite-Link und ist eine Direktverbindung zwischen Satelliten.

Cubesat - Cubesats sind sehr kleine würfelformige Satelliten (max. 1,33kg).

LEO - LEO steht für Low-Earth-Orbit (200-2.000km). In dieser Höhe findet der Großteil der bemannten Raumfahrt statt (z.B. ISS), doch auch viele Satelliten, die nicht an einen geografischen Ort gebunden sind, fliegen in dieser Höhe.

MEO - MEO steht für Medium-Earth-Orbit (2.000-36.000km). Mittelgroße Satellitenkonstellationen (z.B. Navigationssatelliten) befinden sich in dieser Höhe.

GEO - geostationär - GEO steht für Geostationary Orbit (35.786km). Satelliten im geostationären Orbit befinden sich über dem Äquator und bleiben stets über der gleichen geografischen Position auf der Erde. Hier werden Kommunikationssatelliten wie Fernsehsatelliten aber auch Internetsatelliten eingesetzt.

RF-Wellen - RF steht für Radio Frequency (Hochfrequenz). In der Elektrotechnik wird ab 9kHz aufwärts von Hochfrequenz gesprochen.

Kessler-Syndrom - Das Kessler-Syndrom ist eine Kettenreaktion, bei der ein Trümmerteil im Erdorbit andere Satelliten zerstört und somit mehr Trümmerteile erzeugt, bis der komplette Weltraum um die Erde mit Trümmern übersät ist.

1 Einleitung

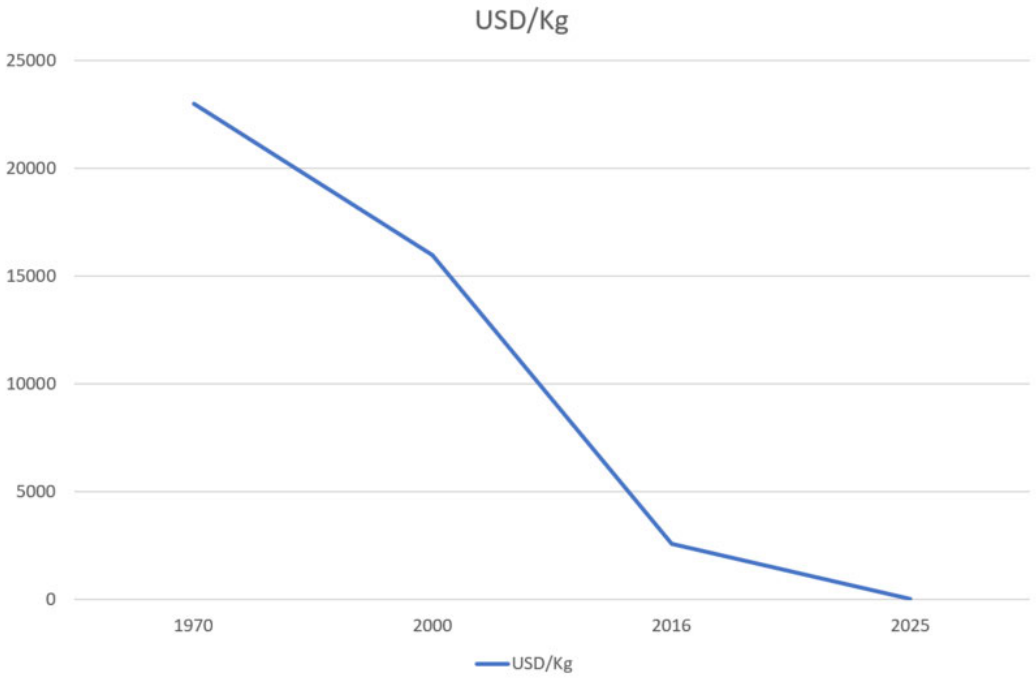
1.1 Motivation

Durch die Entwicklung von kostengünstigen Satelliten ist es ökonomisch tragfähig geworden, eine Vielzahl dieser Satelliten in erdnahe Umlaufbahnen zu bringen (Low-Earth-Orbit, LEO). Im Ergebnis liegen sogenannte Megakonstellationen vor, die in der Lage sind, große geografische Räume drahtlos mit einem leistungsfähigen Internetzugang zu versorgen. Insbesondere für abgelegene und unterentwickelte Weltregionen ergibt sich daraus die Möglichkeit, an der digitalen Welt zu partizipieren. Doch selbst in Ländern wie Deutschland sind satellitengebundene Internetzugänge bei der Erschließung neuer Gebiete in Zukunft eine Option, da bodengebundene Leitungen teuer sind. Gedacht hauptsächlich für strukturschwache Regionen, können sie in Zukunft aber auch in Gebieten mit schnellen Internetzugängen, konkurrenzfähig sein. So kann ein moderner Internetzugang über Satellit etwa für jeden Haushalt ohne Glasfaseranschluss schon eine interessante Alternative sein.

Sinkende Startkosten

Seit den Anfängen der Raumfahrt, welche zunächst nur durch staatliche Organisationen betrieben wurde, hat es einige Änderungen bei den Raketenbetreibern gegeben. Laut einer Studie von Statista haben sich die Kosten eines Kilogramms, der in einen LEO befördert wird, bis zum Jahr 2016 von etwa 23000 USD auf etwa 2600 USD gesenkt.[21] Durch die Privatisierung und das Aufkommen von neuen Launchprovidern wird dieser Preis voraussichtlich auch in den nächsten Jahren weiter sinken. SpaceX plant zum Beispiel, die aktuell in der Entwicklung befindliche Starship-Rakete auf Dauer für einen Preis von 2 Mio. USD zu starten.[42] Sie soll dabei in der Lage sein, 100 Tonnen in einen LEO zu befördern.[34] Dies würde zu einem Preis von 20 USD pro Kilogramm führen. Bei

Abbildung 1.1: Sinkende Kosten pro Kilogramm im LEO seit 1970

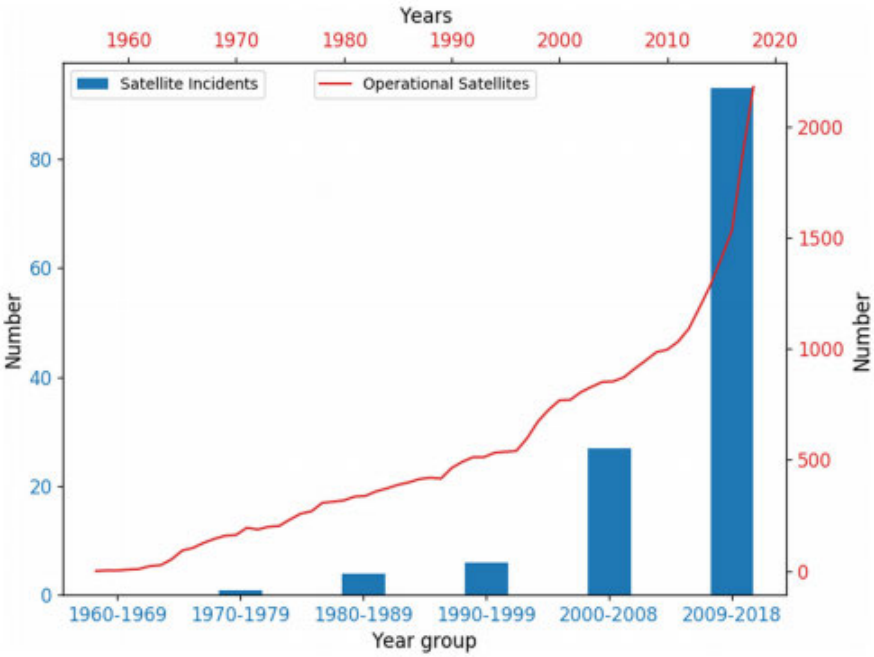


derart niedrigen Preisen wird es in Zukunft auch für Privatanwendern möglich sein, eigene Satelliten in eine Erdumlaufbahn zu bringen. Dies wird die Anzahl von potenziellen Angreifern für Satelliteninternet deutlich vergrößern. Allerdings wird etwa SpaceX kaum Satelliten in eine Erdumlaufbahn bringen, die ihrer eigenen Megakonstellation Schaden zufügen können. Doch je mehr Raketenbetreiber es gibt, desto unregulierter und unkontrollierter werden die einzelnen Satelliten werden, da Launchprovider den Kunden immer mehr entgegen gehen müssen, wenn sie preislich sonst nicht mithalten können.

Angriffe auf Satelliten werden attraktiver

Durch die zunehmende Privatisierung und Kommerzialisierung des Weltraums und auch die größere Verbreitung von Satelliteninternet steigt auch das kriminelles Interesse an Satelliten. Im Jahr 2017 wurde der Weltraummarkt global auf 269 Mio. Dollar eingeschätzt. Die Grafik 1.2 zeigt eine eindeutige Entwicklung, nicht nur bei der Anzahl von operativen Satelliten, sondern auch bei der Anzahl von sicherheitsbezogenen Vorfällen im Zusammenhang mit Satelliten. Nach zunächst linearem Anstieg, steigt die Anzahl seit

Abbildung 1.2: Anzahl von Angriffen auf Satelliten und Anzahl von operativen Satelliten[25]



2009 exponentiell. Hier ist erwartbar, dass sich diese Entwicklung auch in den nächsten Jahren weiter so fortsetzt.[25] Es muss schon jetzt bei jedem Satellit, der gestartet wird, darauf geachtet werden, dass er über notwendige Sicherheitsvorkehrungen, auch für die nächsten Jahre, verfügt. Gerade Hardwareänderungen sind bei Satelliten in den meisten Fällen nicht umzusetzen, weswegen hier weit im Voraus geplant werden muss. Außerdem dauert die Entsorgung bei Satelliten relativ lange (in den meisten Fällen einige Jahre), weswegen veraltete Satelliten den Weltraum um die Erde vermüllen können.

Führt die Nutzung von Satelliteninternet zu erhöhten Risiken?

Jede Art Internetzugang hat seine eigenen Vor- und Nachteile, aber auch seine eigenen Sicherheitsrisiken. Ein kabelgebundener Zugang gilt aber im Allgemeinen als sicherer als ein kabelloser Zugang, da Funkwellen sich unkontrolliert ausbreiten und leichter mitgehört oder sogar verändert werden können. Satelliteninternet versucht, anderen Arten von Internetzugängen Konkurrenz zu machen und muss somit auch bedenkenlos einsetzbar sein. Man kann einen Internetzugang über Satellit als sehr weitläufiges Drahtlosnetz

sehen, das einige Risiken mit sich bringt. Hier stellt sich die Frage, ob es ein erhöhtes Sicherheitsrisiko darstellt, Internet über Satelliten zu nutzen, oder die Risiken im Vergleich zu den Risiken bei der herkömmlichen Internetnutzung, nicht schwerwiegender sind.

1.2 Ziel der Arbeit

Das Ziel meiner Arbeit ist, eine Analyse und Bewertung der IT-Security Risiken durchzuführen, die im Zusammenhang mit der Nutzung von Satelliteninternet entstehen. Es geht hierbei hauptsächlich um Low-Earth-Orbit-Konstellationen und nicht um herkömmliches Satelliteninternet von geostationären Satelliten. Hierzu untersuche ich, was für Angriffe es in der Vergangenheit auf Satelliten (-internet) gab und in wie weit diese Angriffe auch auf moderne Megakonstellationen durchgeführt werden könnten. Weiterhin wird untersucht, welche Art Angriffe es auf herkömmliche (Drahtlos-) Netzwerke gibt und ob Satellitennetzwerke für diese Angriffe auf ähnliche Weise anfällig sind. Diese Risiken werden anhand der Eintrittswahrscheinlichkeit und der gefährdeten Ziele bewertet. Dabei werde ich auch mögliche Sicherheitskonzepte aufzeigen, die bei Satelliten eingesetzt werden oder eingesetzt werden könnten. Die Einschätzung muss zum einen unterschieden werden in Angriffe, die in näherer Zukunft oder erst langfristig möglich sind, und ob es sich um gezielte oder ungezielte Angriffe handelt.

1.3 Für wen ist die Arbeit

Die Literatur ist in diesem spezifischen Feld noch unvollständig, aufgrund der Neuheit von massentauglichen Internetzugängen über Satellit. Diese Arbeit ist für potentielle Kunden von Satelliten-Internet, die sich einen Überblick verschaffen wollen, ob Satelliteninternet eine mögliche Alternative darstellt. Weiterhin bietet sie einen Einstieg in das Gebiet des Satelliteninternets und ist somit auch für Sicherheitsexperten, die sich weiterbilden wollen geeignet. Der häufigste Grund, Internet über Satelliten zu beziehen, ist aktuell, die mangelnde Verfügbarkeit von anderen Internetanschlüssen. Durch die Entwicklung von LEO-Megakonstellationen können Satelliteninternetanschlüsse der Zukunft herkömmlichen Kabelanschlüssen zunehmend Konkurrenz bieten und durch Direktverbindungen zwischen den Satelliten über lange Strecken teilweise sogar geringere Latenzen und höhere Datenraten ermöglichen. Es muss aber zunächst eingeschätzt werden, ob die Sicherheitsstandards bei Satelliteninternet den Anforderungen entsprechen.

1.4 Abgrenzungen

Es werden in dieser Arbeit nicht einzelne Protokolle, die bei Satelliten-Internet verwendet werden, vollständig untersucht. Es werden keine praktischen Experimente durchgeführt. Es werden, abgesehen von Beispielszenarien, keine Einzelfälle, weder im Anbieter- noch im Kundenbereich, betrachtet. Es wird für den Vergleich mit anderen Arten von Internetzugängen nicht detailliert auf deren Sicherheitsrisiken eingegangen, denn das würde den Rahmen dieser Arbeit übersteigen und ist daher nicht zielführend.

1.5 Kapitelübersicht

Im Anschluss an die Einleitung wird in Kapitel 2 werden zunächst aktuelle Entwicklungen in der Satellitentechnik im Bezug auf Satelliten-Internet beschrieben. Hierbei wird auch auf allgemeine Sicherheitsfunktionen bei Satellitenprotokollen eingegangen. Es folgt eine Zusammenfassung über aktuelle und zukünftige Satelliteninternetanbieter in Deutschland. Zuletzt gibt es noch eine Beschreibung der Methodik einer Risikoanalyse und für diese Arbeit wichtige Definitionen.

Kapitel 3 ist die eigentliche Risikoanalyse. Nach einer kurzen Abgrenzung der behandelten Risiken werden die möglichen Gefahren in der Risikoerkennung gesammelt und dann in der Risikobewertung detailliert beschrieben. Am Ende befindet sich noch eine Zusammenfassung der Risiken und eine kompakte Darstellung in tabellarischer Form. Diese Zusammenfassung wird außerdem anhand von Beispielszenarien veranschaulicht.

Im letzten Kapitel gibt es zunächst einen Ausblick auf kommenden Jahre, und einen Überblick inwieweit sich die Verhältnisse im Bereich der Sicherheit von Satelliten ändern könnten. Am Ende wird eine allgemeine Einschätzung über die Frage, ob bei der Nutzung von Satelliten-Internet zusätzliche Sicherheitsmaßnahmen ergriffen werden müssen, gemacht.

2 Grundlagen

2.1 Stand der Satellitentechnik und Protokolle

2.1.1 Aktuelle Entwicklungen bei Satellitenkommunikation

Satellitenkommunikation ist ein immer wichtigerer Teil unseres Lebens geworden, zum Beispiel durch Fernsehsignale, Navigationsassistenten oder auch Wetterbeobachtungen. Durch die zunehmende Anzahl von Endgeräten müssen einzelne Satelliten deutlich mehr Nutzer abdecken. Es wurde deswegen bei der Kommunikation mit Satelliten von Single-Beam zu Multi-Beam umgestellt. Außerdem sind moderne Satelliten in der Lage, Daten digital zu verarbeiten, und müssen nicht mehr nur auf analoge Hardware zurückgreifen. Für die Boden-zu-Boden-Kommunikation über Satelliten ist die wohl größte Neuerung aus den letzten Jahren die Einführung von LEO-Konstellationen, die zwar anfangs nicht sehr erfolgreich waren, sich jedoch mittlerweile durchsetzen und wahrscheinlich geostationäre Satelliten langfristig ablösen werden. Hierfür müssen allerdings neuartige Netzwerkparadigmen entwickelt werden, um die komplexen Routing-Herausforderungen zu bewältigen. Außerdem wird deutlich mehr Bandbreite benötigt, um die Nachfrage auf Dauer zu decken.[8]

Das Bandbreitenproblem wird zu großen Teilen durch die Nutzung vom gesamten Ka-Band (17.7-19.7 GHz) und dem EHF-Band (über 40GHz) angegangen. Außerdem müssen Konzepte eingesetzt werden, um das Teilen von einer Frequenz mit mehreren Nutzern zu verbessern. Signale im EHF-Band können jedoch von atmosphärischen Effekten beeinflusst werden und sind deswegen für kritische Nachrichten nicht zu empfehlen. Hier müsste dann aber unterschieden werden, welche Pakete wichtig sind und welche eine niedrigere Priorität haben. Dies wird in einigen Netzwerken bereits eingesetzt und nennt sich Quality of Service (QoS). Hierbei wird der Netzwerkverkehr in drei Prioritätsstufen (Generelles Browsing, Datenübertragung und Streaming, Mission Critical) eingeteilt.[16] Es kann aber auch mit Redundanz bei den Bodenstationen gegen die Beeinflussung durch

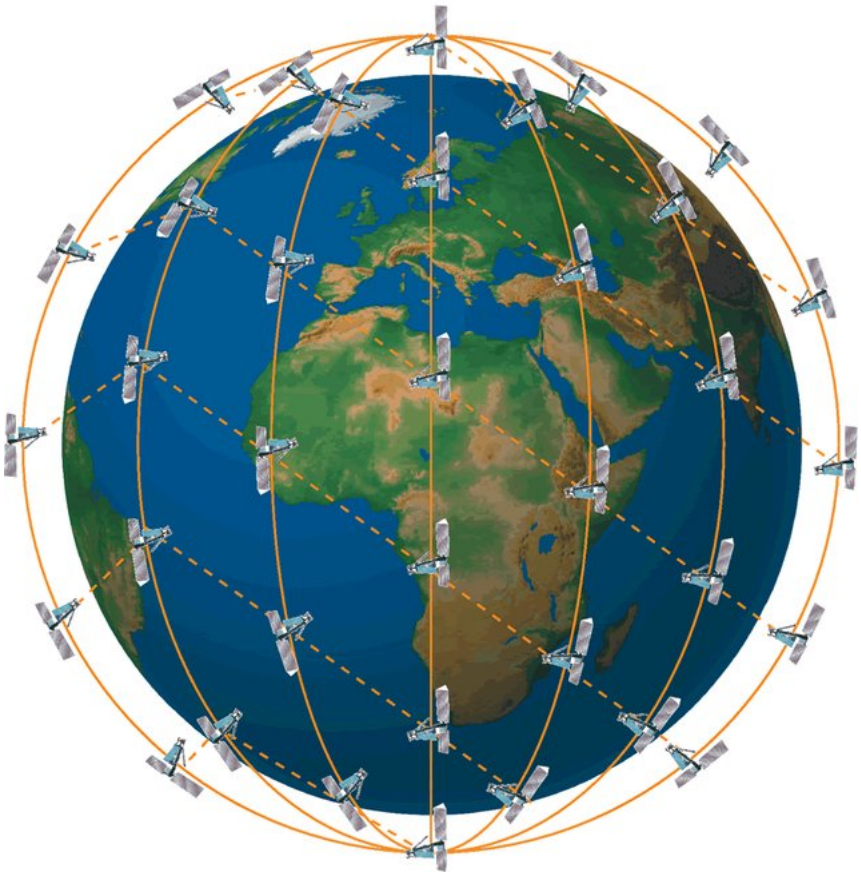
Wettereffekte gewirkt werden. Dies führt aber zu noch größeren Problemen für das Border Gateway Protocol, welches nicht für derart geografisch große Netzwerke ausgelegt ist. Außerdem wird hierfür eine Smart Gateway Diversity Architecture (SGDA) benötigt, denn es gibt hierbei keine Eins-zu-Eins Verbindung mehr. Die SGDA muss in Echtzeit erkennen können, welcher Link welche aktuelle Fehlerrate vorweist und Pakete entsprechend aufteilen. Hierfür müssen alle Bodenstationen miteinander verbunden sein, jedes Nutzerpaket kann von jeder Bodenstation verarbeitet werden und Datenverkehr kann bei Ausfällen schnell umgeleitet werden. Weiterhin gibt es eine Umstellung bei der Payload-Architektur, vom verbreiteten Single Feed per Beam (SFPB) hin zum Multi Feed Per Beam (MFPB). Beim SFPB wurde ein Strahl nur für einen Nutzer reserviert, beim MFPB hingegen kann ein Strahl auf mehrere Nutzer aufgeteilt werden, indem die Pakete vom einem Scheduler eingeteilt werden. Dadurch können einzelne Satelliten mehr Nutzer gleichzeitig bedienen, ohne mehr Antennen zu benötigen. Es ist hierbei auch wichtig, dass die Auslastung der einzelnen Beams gleichmäßig verteilt ist.[8]

Eine weitere größere Entwicklung ist der vermehrte Einsatz von LEO-Konstellationen, die aufgrund der deutlich geringeren Distanz zum Boden eine wesentlich niedrigere Latenz ermöglichen. Bei geostationären Satelliten beträgt die Latenz mindestens 520 ms, während sie bei einer theoretischen Flughöhe von 100 km nur etwa 1 ms betragen würde.[17] Die Satelliten in diesen Konstellationen, werden teilweise auch mit Inter-Satellite-Links (ISL, Links zwischen den Satelliten) ausgestattet. Dadurch ergeben sich aber neue Probleme für das Routing, an denen im Moment geforscht wird.[44] Außerdem müssen bei diesen Konstellationen häufig Handover durchgeführt werden, da die Satelliten sich relativ zum Boden bewegen. Diese Handover müssen schnell und unbemerkt geschehen, aber trotzdem ausreichend gesichert sein. Dies führt auch dazu, dass Antennen, die auf dem Boden genutzt werden, dem Satelliten möglichst weit folgen können sollten und nicht starr wie eine herkömmliche Fernsehsatellitenschüssel sein können.[8] SpaceX hat für die Schüsseln, die bei Starlink eingesetzt werden, einen Motor eingebaut, damit sie sich selbstständig im optimalsten Winkel ausrichten. (Mehr zu Starlink in Kapitel 2.2)[10]

2.1.2 Protokolle

Die meisten bei Satelliten genutzten Funkprotokolle sind missionsspezifische Protokolle. Dadurch, dass viele dieser Missionen wissenschaftlicher Natur sind, sind sie nicht verschlüsselt und legen keinen großen Wert auf Geheimhaltung. Bei militärischen Missionen

Abbildung 2.1: Beispieldarstellung einer LEO-Konstellation [31]



ist natürlich das Gegenteil der Fall, jedoch sind aus nahe liegenden Gründen kaum Informationen über die Protokolle öffentlich.

Das am meisten genutzte Protokoll für Satellitenübertragungen ist DVB. Varianten von diesem Protokoll werden für Satellitenfernsehen genutzt. Dadurch sind diese Übertragungen weltweit standardisiert. Eine neue Entwicklung hingegen sind optische Kommunikationswege mittels Visible Light Communication (VLC). VLCs haben den Vorteil, dass sie nicht dieselben Frequenzen wie Hochfrequenzsignale nutzen. Außerdem sind durch sie deutlich größere Übertragungsraten möglich. Der Nachteil ist jedoch, dass VLCs durch Hindernisse wie etwa Wolken blockiert werden. Deswegen sind sie nicht für Boden-Satellit Kommunikation geeignet, sondern nur für Satellit-Satellit Kommunikation.[25] Ein häufig genutztes Protokoll für kleine Cubesats, ist der Amateurfunkstandard AX.25. Dieser Standard ist jedoch schon wegen der geringen Bandbreite nicht für Satelliteninternet nutzbar.[30]

Ein weiterer Punkt neben den Funkprotokollen ist die Anwendbarkeit von bekannten Internetprotokollen über Satelliten. Viele Internetprotokolle, vor allem das meist verwendete TCP, werden durch hohe Latenzen und Fehlerraten stark eingeschränkt. Deswegen sind sie für Satellitenverbindungen nicht sonderlich geeignet. Für aktuell genutzte Internetsatelliten, die sich im geostationären Orbit befinden, werden teilweise Proxyserver (Performance Enhancement Proxy, PEP) verwendet. Dadurch ist zwar die Latenz für den Endnutzer immer noch sehr groß, allerdings können die Datenraten und Verbindungen stabil gehalten werden. So lassen sich beispielsweise Downloads problemlos durchführen, jedoch etwa Gespräche haben eine Verzögerung von einer Sekunde.[6]

2.1.3 Angebotene Sicherheitsfunktionen

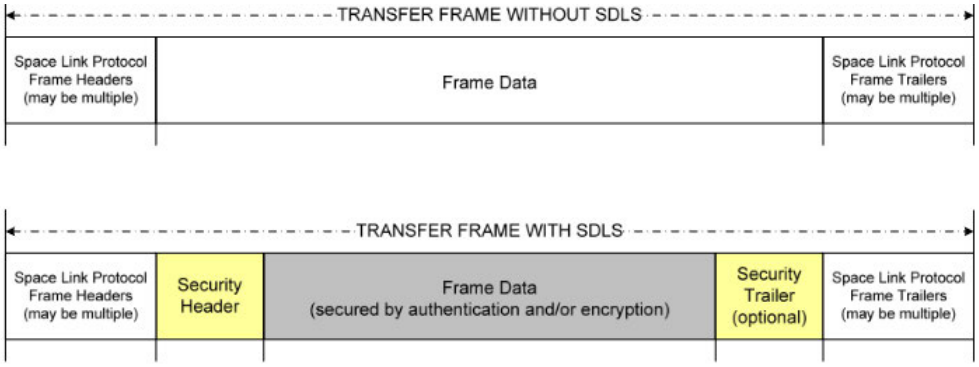
Die verwendeten Protokolle haben teilweise eigene Sicherheitsfunktionen. Allerdings schränken sie teilweise auch Sicherheitsmechanismen anderer Protokolle ein. Das Consultative Committee for Space Data Systems (CCSDS) entwickelt Standards für Datenübertragungen im Weltraum. Unter anderem hat das CCSDS einen Standard für Security entwickelt, der für die Allgemeinverwendung gedacht ist.

Die teilweise genutzten Performance Enhancement Proxies haben den Nachteil, dass sie nicht funktionieren, wenn TCP-Header verschlüsselt sind. Sie können also nur eingesetzt werden, falls sich die Verschlüsselung auf die Nutzdaten beschränkt. Wenn also eine komplette Ende zu Ende Verschlüsselung, wie etwa bei einem VPN, gefordert ist, sind PEPs nicht geeignet.[6]

CCSDS hat einen Standard entwickelt (CCSDS Recommended Standard for Space Data Link Security), der sich auf die Security bei Datenübertragung im Weltraum spezialisiert. Das Ziel dieses Standards ist, eine Standardmethode zu entwickeln, die unabhängig von den verwendeten kryptografischen Algorithmen in praktisch jeder Weltraummission verwendet werden kann. Weiterhin soll die Methode möglichst mit allen vorher verwendeten Standards kompatibel bleiben, sowie mit anderen CCSDS Standards. Außerdem soll hierdurch eine Vereinfachung bei der Interoperabilität zwischen Satellitenbetreibern geschaffen werden. Das Security Protocol beinhaltet Security Header und Trailer, um die notwendigen kryptografischen Parameter innerhalb eines Übertragungsfensters mitzugeben. Das Security Protocol wird komplett im Space Data Link Protocol eingebettet, wodurch dessen Nutzbarkeit erhalten bleibt. Dadurch wird die maximale Länge der zu übertragenden Daten abhängig vom genutzten Space Data Link Protocol eingeschränkt.

Das Security Protocol beinhaltet Funktionen für die Authentifizierung, Verschlüsselung

Abbildung 2.2: Einbettung des Security Protokolls in das Space Data Link Protocol [39]



und authentifizierte Verschlüsselung. Es werden dabei Sessions verwendetet, das Protokoll ist also nicht stateless. Dadurch werden Authentifizierung, Datenintegrität, Replayschutz und Data-Confidentiality gewährleistet. Die Dienste des Protokolls sind in zwei Funktionen definiert. Einmal gibt es die "ApplySecurity" Methode beim Sender und die "ProcessSecurityFunction" Methode beim Empfänger. Diese Methoden bekommen jeweils den Inhalt des Frames übergeben und nutzt gespeicherte Einstellungen für die "Security Association" um den Inhalt zu kodieren oder dekodieren. Wenn beim Dekodieren Fehler auftreten, werden passende Fehlercodes zurückgegeben. Dadurch können zum Beispiel Replay-Angriffe nicht nur verhindert, sondern auch aufgedeckt werden. [39]

Neue Megakonstellationen können mehrschichtig aufgebaut sein. Das bedeutet, dass es Satelliten in niedrigem Orbit gibt, die Verbindungen zu Bodenstationen und Klienten haben, aber auch Satelliten in höheren Orbits, die als Management- oder Routingsatelliten fungieren. Dies, kombiniert mit Direktverbindungen zwischen den Satelliten, ermöglicht ein vom terrestrischen Netz unabhängiges Netzwerk. [44] Damit können, wenn wichtige Rechenzentren eigene Zugänge zum Satellitennetz bekommen, sämtliche Regulierungen und Abhörmöglichkeiten vom herkömmlichen Internet umgangen werden. Außerdem werden hierdurch Angriffsmöglichkeiten auf Bodenstationen minimiert, da in diesem Fall das Rechenzentrum direkt angegriffen werden müsste (wodurch noch ganz andere Angriffsmöglichkeiten entstehen würden).

2.2 Anbietersituation beim Satelliteninternet

2.2.1 Aktuelle Satelliteninternetanbieter

Da die meisten Anbieter Internet über geostationäre Satelliten anbieten, welche nur regionale Gebiete abdecken, werden nicht alle Anbieter weltweit betrachtet, sondern nur jene, die im Gebiet Deutschland/Europa, einen Internetzugang ermöglichen. Der Internetzugang wird in Deutschland in den meisten Fällen nicht von Satellitenbetreibern selbst angeboten, sondern von lokalen Vertriebspartnern. Stand 2018 waren acht Servicebetreiber in Deutschland aktiv. Diese haben mit der Ausnahmen von Filiago, welche einen Satelliten von Avanti nutzen, auf Satelliten von SES S.A. und Eutelsat zurückgegriffen. Die einzelnen Angebote unterscheiden sich technisch kaum, nur die Preise, Datenvolumen oder Geschwindigkeiten unterscheiden sich. Es muss in allen Fällen Hardware installiert werden, welche entweder gemietet oder gekauft werden kann. Es gab 2018 nur drei Angebote mit Flatrate für Privatkunden in Deutschland. Die Preise lagen zwischen 50€ und 65€ monatlich und einmaligen Kosten zwischen 500€ und 600€. Dafür bekommt man eine Downloadrate von 25 bzw. 60 Mbit/s und eine Uploadrate von 2 bzw. 6 Mbit/s. Geschäftliche Kunden, die die Zugänge etwa bei Arbeiten an abgelegenen Orten oder auf Schiffen verwenden, gibt es mehr Auswahlmöglichkeiten, aber zu höheren Preisen. Die Preisentwicklung tendiert aber nach unten. Satelliteninternet ist allerdings noch deutlich teurer als vergleichbare Anschlüsse über DSL oder Mobilfunkangebote.[29] Der große Nachteil von all diesen Angeboten ist jedoch, dass es sich um geostationäre Satelliten handelt, welche aufgrund der großen Entfernung über eine sehr hohe Latenz verfügen. Dies stellt viele gängige Protokolle vor größere Herausforderungen.

Eine Möglichkeit, Middle-Earth-Orbit (MEO) Satelliten für Internet zu benutzen, besteht in Deutschland im Moment nur bei der Nutzung von Iridium-Satelliten, welche jedoch eigentlich für Telefonie und Pagernachrichten entwickelt wurden und nur sehr geringe Bandbreiten für Internet zur Verfügung stellen. Angebote über Iridium haben aber auch den Vorteil, dass der Anschluss überall auf der Welt genutzt werden kann, er ist also geeignet für Schiffe und Flugzeuge. [18]

2.2.2 Zukünftige Satelliteninternetanbieter

Bei der Betrachtung von zukünftigen Satelliteninternetanbietern muss vor allem auf LEO-Konstellationen eingegangen werden. Es gibt zwar auch ständige Verbesserungen und

Bandbreitenerhöhungen bei den vorhandenen Anbietern, allerdings wird die hohe Latenz immer ein Problem bleiben. Es gibt derzeit mehrere Konstellationen, die in Planung oder im Aufbau sind. Dieses Unterfangen ist jedoch immer ein großes Risiko und Unternehmen wie Iridium[43] oder OneWeb[37] mussten schon Insolvenz anmelden. Die beiden vielversprechendsten Konstellationen sind zum einen Starlink[35] von SpaceX und zum anderen Kuiper[28] von Amazon.

Starlink ist in manchen Teilen der Welt sogar schon in Betrieb. Auch in Deutschland kann ein Internetanschluss über Starlink vorbestellt werden, jedoch ob die versprochene Inbetriebnahme dieses Jahr noch stattfindet, hängt von der Zulassung durch europäische Regulationen ab. Die Kosten für einen Starlink-Anschluss betragen aktuell 500€ einmalig für den Kauf der Satellitenschüssel und 99€ monatlich für den Betrieb. Hierfür würde man im Moment etwa 100 Mbit/s Download und 20 Mbit/s Upload bekommen, bei kaum höherer Latenz als bei einem herkömmlichen DSL-Anschluss. Außerdem wäre dieser Anschluss eine Flatrate.[35] Weiterhin sollen die Raten in den nächsten Jahren noch erhöht werden, wenn weitere Satelliten der Konstellation (SpaceX hat die Erlaubnis, bis zu 42.000 Satelliten zu betreiben) hinzugefügt werden. Im aktuellen Testbetrieb sind die Anschlüsse noch lokal gebunden, da sichergestellt werden soll, dass keine Gebiete überlastet werden, jedoch wird ein Starlink-Anschluss in Zukunft auch theoretisch weltweit nutzbar sein.[10] Starlink nutzt für das Ku-Band für die Kommunikation mit Nutzern und Ka-Band für die Kommunikation mit eigenen Bodenstationen.[9]

Projekt Kuiper ist eine weitere LEO-Megakonstellation, die von Amazon geplant wird. Diese ist bis jetzt für 3.236 Satelliten ausgelegt, also nicht ganz so groß wie Starlink. Es gibt hierfür durch das Federal Communications Committee (FCC) gesetzte Fristen, so müssen bis Mitte 2026 mindestens die Hälfte der Satelliten im Orbit sein, und bis 2029 muss das Projekt abgeschlossen sein. Genauere Informationen, wie etwa Preise oder Geschwindigkeiten gibt es bis jetzt nicht. Die genutzten Antennen sollen bei Geostationären Satelliten aber schon eine Bandbreite von 400 Mbit/s Download und 50 Mbit/s Upload erreichen können, welche bei LEO-Satelliten noch mehr sein dürfte (Die Bandbreite wird aber durch die Satelliten und Anzahl der Kunden limitiert, ähnlich wie bei Starlink).[28]

2.2.3 Zusätzliche Bedenken gegen Satelliteninternet

Es wäre vor allem für das Routing von Paketen zwischen Satelliten hilfreich, wenn das Netzwerk auf Metadaten zugreifen kann, jedoch bringt dies einige Nachteile mit sich, weswegen es, wenn irgendwie möglich, vermieden werden sollte. Weiterhin kann die geografische Größe der Netzwerke vor allem Content Delivery Networks vor Herausforderungen stellen, da quasi ein paralleles Internet zu dem Netz auf der Erde aufgebaut wird. [7]

Es kann sein, dass Amazon mit Kuiper Daten über Kunden sammeln will. Amazon macht dies beispielsweise bereits mit Diensten wie AWS, welches von Netflix genutzt wird, wodurch Amazon einiges über die Kunden lernen konnte. Es würde hier also zu einer Vermischung zwischen Internetanbieter und und Werbeanbieter kommen. [24]

Bei einer Untersuchung aus dem Jahr 2005 ergab, dass vielen Nutzern nicht bewusst ist, dass Internetzugänge über Satellit Broadcastübertragungen sind. So konnten viele Daten unbefugt abgerufen werden, da die Übertragungen nicht verschlüsselt waren. Es muss also sichergestellt sein, dass dem Nutzer immer bewusst ist, dass seine Daten von Dritten mitgehört werden können.[3] Allerdings hat sich in der Zeit seitdem in Richtung Sicherheit und Verschlüsselung einiges getan, weshalb heutzutage diese Probleme nicht mehr so akut sind. So wird beispielsweise heute fast jede Website nur noch per Hypertext Transfer Protocol Secure (https) aufgerufen und nicht mehr mit der unverschlüsselten Variante. Das grundsätzliche Problem wird aber bei Broadcastübertragungen immer bestehen, und man kann sich nur auf die gegebene Sicherheit durch die verwendeten Verschlüsselungen und Protokolle verlassen.

Weiterhin gibt es viele Gegner für die Megakonstellationen. Vor allem Astronomen haben Bedenken, dass die Satelliten ihre Forschung einschränken können. Dies gilt sowohl für die Nutzung von Infrarotteleskopen als auch für optische Teleskope.[14] Gerade dies wird auch von vielen Hobbyastronomen bemängelt. Starlink testet seit Anfang 2020 Methoden, um die Reflektivität der Satelliten zu verringern. Es ist nicht möglich, einen Satelliten einfach schwarz anzumalen, da möglichst viel Sonnenlicht reflektiert werden muss, um Temperaturen im Griff zu behalten. Deswegen wurde eine Art Sonnenschild entwickelt, welches auf dem Satelliten montiert ist und so positioniert wird, dass es den Satelliten immer möglichst im Schatten hält.[10]

2.3 Methodik der Risikoanalyse

2.3.1 Allgemeine Definitionen

Risiko

Ein Risiko ist etwas Bedrohliches oder Gefährliches. Ein Risiko wird zum einen durch die zu erwartende Häufigkeit des Eintritts und dem beim Eintritt zu erwartendem Schadensausmaß beschrieben.[19]

Sicherheit

Der deutsche Begriff Sicherheit kann zwei Dinge bedeuten. Zum einen den englischen Begriff "Security", welcher den Schutz eines Systems vor gezieltem und ungezieltem Schaden beschreibt durch Bedrohungen von außen. Zum anderen den Begriff "Safety", der den Schutz eines Systems vor unerwünschten Zuständen schützt, wie zum Beispiel der Ausfall der Verfügbarkeit. Safety beinhaltet das Gefühl, sicher zu sein.[15]

Abbildung 2.3: Das Parkerian Hexad [13]

Confidentiality (Vertraulichkeit)

Informationen dürfen nicht von unautorisierten Dritten abrufbar sein. Dies ist das wohl wichtigste Element, da fast alle Informationen nicht öffentlich zugänglich sein sollten.[13]

Integrity (Integrität)

Integrity bedeutet die Sicherheit, dass Daten nicht unautorisiert verändert werden können. Hier gilt allerdings auch, dass vor ungewollten Änderungen durch autorisierte Parteien geschützt wird.[13]

Availability (Verfügbarkeit)

Es muss sichergestellt sein, dass eine Ressource oder Information verfügbar ist, wenn sie benötigt wird.[13]

Possession or control (Besitz oder Kontrolle)

Dieses Element schützt vor dem Fall, dass vertrauliche Daten sich in physischem Besitz unautorisierter Dritter befinden. Ein Beispiel hierfür wäre, wenn Informationen zwar ausreichend verschlüsselt sind, sich allerdings auf einer Festplatte befinden, die sich in unautorisierten Händen befindet.[13]

Authenticity (Authentizität)

Authenticity stellt sicher, dass man weiß, mit wem man kommuniziert. Wenn es zu einem Informationsaustausch kommt, muss sichergestellt sein, dass die Informationen von der Quelle kommen, von der man sie erwartet. Hierfür wird ein Identitätsbeweis benötigt.[13]

Utility (Nutzbarkeit)

Daten müssen trotz allem Schutz nutzbar bleiben. Utility ist das Element, in dem nicht vor Angriffen Dritter geschützt wird, sondern vor der Gefahr, etwas so stark zu schützen, dass es selbst für autorisierte Parteien schwer oder gar unmöglich wird, es zu nutzen.[13]

2.3.2 Was ist zu schützen?

Da diese Risikoanalyse an keinem praktischen Beispiel durchgeführt wird, gibt es nur theoretische zu schützende Elemente. Deswegen wird auf das "Parkerian hexad" zurückgegriffen, welches auf dem CIA-Modell basiert und es erweitert. Es werden die in Grafik 2.3 dargestellten, zu schützenden Elemente definiert.[13]

2.3.3 Konzept der Risikoanalyse

Eine Risikoanalyse dient zur Einschätzung und Einsortierung von Risiken im Bezug auf ein Projekt. Durch sie können in weiteren Schritten Maßnahmen entwickelt und bewertet werden, aber auch eine Risikoüberwachung implementiert werden. Sie folgt dabei in der Regel einem festen Muster.[27]

Abgrenzung des Analysebereichs

Es muss klar festgelegt sein, welche Bereiche analysiert werden und welche vernachlässigt werden, da eine Risikoanalyse nicht zwingend alle Gefahren aufdeckt. Es müssen schutzbedürftige Objekte aufgezeigt und beschrieben werden. Hierbei ist auch zu beschreiben, wie diese Objekte zusammenhängen und mögliche Ursache-Wirkungs-Beziehungen zu finden.[2]

Risikoerkennung

In dieser Phase wird eine Sammlung von Risiken erstellt, die bei der Nutzung von Satelliteninternet auftreten können. Diese Sammlung benennt ein Risiko und enthält eine kurze Beschreibung. Hierzu werden zum einen bekannte Angriffe auf Satelliten betrachtet, aber auch bekannte Angriffe auf herkömmliche Drahtlosnetzwerke. Zum Schluss gibt es noch

weitere Überlegungen über mögliche zukünftige Risiken. Es ist damit nicht garantiert, dass alle Risiken gefunden werden, aber es kann eine Einschätzung gemacht werden, ob Internet über Satelliten unsicherer ist als ein herkömmlicher Internetzugang.

Risikobewertung

In dieser wichtigen Phase werden gefundene Risiken beschrieben. Hierbei werden die Risiken auch den schutzbedürftigen Objekten zugeordnet, um mögliche Schäden abzuschätzen. Dies wird hier in hinsichtlich vier Bereichen pro Risiko durchgeführt: Jeder mögliche Angriff wird zunächst beschrieben, dann wird herausgestellt, was das Ziel des Angriffs ist, als Nächstes wer den Angriff durchführen kann, wie aufwändig der Angriff ist und zum Schluss noch, was es aktuell oder herkömmlich für Verteidigungsstrategien gegen diesen Angriff gibt. Außerdem wird pro Angriff ein Beispiel beschrieben (wenn es ein bekanntes Beispiel gibt). Der Angriffsaufwand wird in eine von drei Kategorien eingeteilt. Geringer Aufwand besteht, wenn keine spezielle Hardware oder physischer Zugang benötigt wird. Hierunter würden klassische Netzwerkangriffe fallen, selbst wenn diese als solches nicht unbedingt in die Kategorie "Geringer Aufwand" fallen würden. Mittlerer Aufwand besteht, wenn spezielle Hardware, wie etwa ein eigener Sender benötigt wird, oder Insiderwissen über das System. Hoher Aufwand bedeutet, dass der Angriff für Privatpersonen üblicherweise nicht umsetzbar sind. Hierzu zählt zum Beispiel, wenn ein eigener Satellit benötigt wird. Diese Angriffe können (und wurden in der Vergangenheit) von staatlichen Raumfahrtorganisationen oder großen Unternehmen durchgeführt werden.

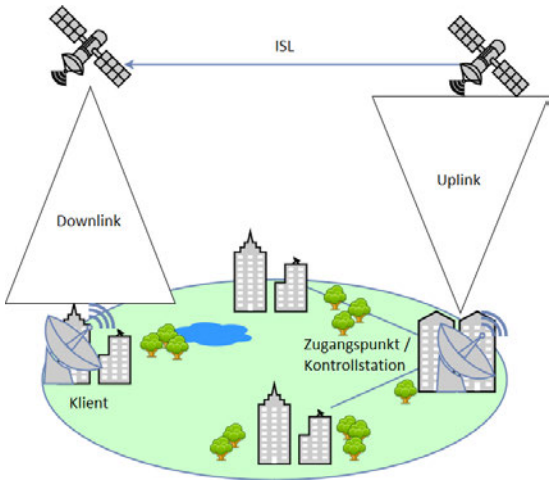
Darstellung der Ergebnisse

Abschließend muss eine Übersicht erstellt werden, mit der eingeschätzt werden kann, welche Maßnahmen ergriffen werden müssen. Dies geschieht generell in allgemein verständlicher Sprache, da Entscheidungsträger nicht zwangsläufig mit IT-Sicherheitsbegriffen vertraut sind.[2] In diesem Fall wird eine Tabelle erstellt, die einen Überblick über alle abgedeckten Risiken/Angriffe bietet und aufzeigt, wie wahrscheinlich das Eintreten ist und welche Elemente betroffen wären. Anschließend werden noch drei mögliche Szenarien beschrieben und eine Empfehlung abgegeben, ob und wie Satelliteninternet eingesetzt werden kann.

3 Risikoanalyse

3.1 Abgrenzung des Analysebereichs

Abbildung 3.1: Verbindung Internet zu Client



Es werden nur mögliche Risiken betrachtet, die zwischen dem Client-Netzwerk und dem Internetzugang des Serviceproviders liegen. Es gehören dabei aber auch Risiken dazu, welche die Kontrollstationen des Betreibers betreffen, da sie direkten Einfluss auf die Satelliten haben können. Hierbei wird bei LEO-Konstellationen zwischen Upload und Download unterschieden. In der Grafik 3.1 kann gesehen werden, dass auf dem Boden Nachrichten für einen Klienten mithörbar sind, während bei Grafik 3.2 Nachrichten für alle Klienten empfangbar sind. Bei GEO-Verbindungen (Abbildung 3.3) ist das Netzwerk zwar vereinfacht, aber auch ohne Redundanz. Betrachtet werden der Klientzugangspunkt, die Verbindung zwischen Boden und Satellit, der Satellit, eine eventuelle Verbindung zwischen Satelliten und Bodenstationen des Betreibers.

Abbildung 3.2: Verbindung Client zu Internet

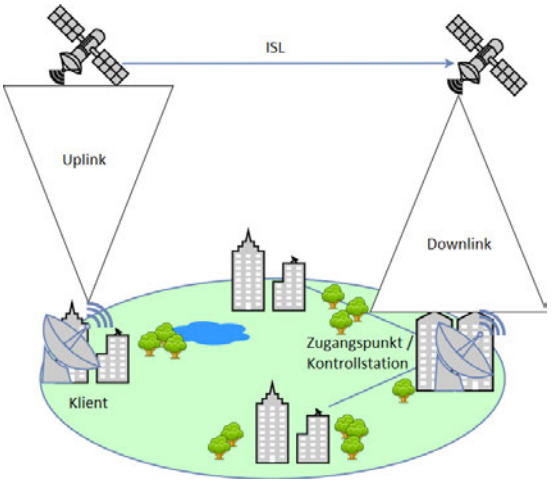
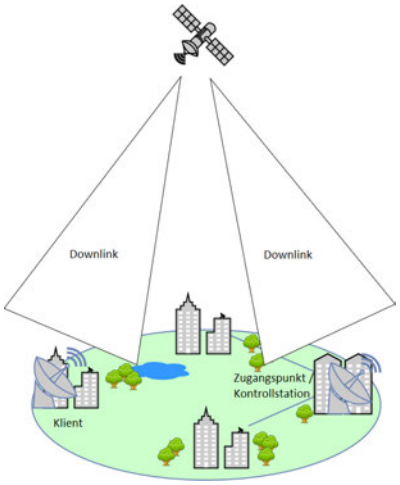


Abbildung 3.3: Geostationärer Satellit



3.2 Risikoerkennung

Es werden zwei Schriften zur Sammlung von möglichen Risiken herangezogen. Zum Einen einen Artikel von M. Manulis, und zum anderen eine Risikoanalyse von S. Abdalla. Die in diesen Schriften aufgelisteten Risiken werden, sofern sie bei der Nutzung von Satelliteninternet eine Rolle spielen können, in der Reihenfolge, in der sie aufgeführt wurden, hier übernommen. Bei zu großen Überschneidungen werden sie ignoriert.

3.2.1 Manulis - Cyber Security in new Space

Der Artikel von M. Manulis analysiert mögliche Gefahren und Angriffe auf Satellitensysteme. Für die Bodenstationen hat Manulis folgende Angriffe identifiziert:

Physische Attacken - ein Angreifer kann sich Zugang zu Bodenstationen verschaffen.

Computer Network Exploitation - ein Angreifer kann das Netzwerk der Bodenstation angreifen.

Angriff auf Cloudinfrastruktur - laut Manulis werden die meisten Satelliten über Cloud computing gesteuert.

Datenveränderung/-korruption - dies kann absichtlich oder unabsichtlich geschehen.

Supply Chain Attacks - es könnte z.B. Source-Code geleakt werden.

Veraltete Software und Standards - Jegliche verwendete Software mit bekannten Sicherheitslücken ist eine Gefahr.

Als nächstes beschäftigt sich Manulis mit möglichen Gefahren, die bei der Kommunikation zwischen Bodenstation und Satellit auftreten:

Jamming - Die Signale werden blockiert.

Eavesdropping - Insbesondere Signale vom Satelliten Richtung Boden können von jedem in ungefährer Nähe des Empfängers, empfangen werden.

Hijacking - dies fällt in den Kommunikationsbereich, da bei jeder Zweckentfremdung eines Satelliten die Kommunikationsprotokolle geändert werden.

Spoofing - ein Angreifer kann eigene Signale zwischen legitimen verstecken, die legitim erscheinen.

Anschließend gibt es noch das Weltraumsegment, wo es zwar im Moment noch recht wenige bekannte Angriffe gibt, was sich jedoch in Zukunft ändern kann und wird.

DoS - Clogging - Ein Satellit kann lahmgelegt werden, zum Beispiel durch das Senden von leicht falschen oder unvollständigen Paketen, die die Fehlerkorrektur des Satelliten überfordern.

[25]

3.2.2 Abdalla - Risikoanalyse drahtloser Netze am Beispiel des IEEE 802.11-Standards

Samer Abdalla analysiert Risiken bei der Nutzung von Drahtlosnetzen anhand des IEEE 802.11-Standards. Da Satelliteninternet im Grunde nur ein Drahtlosnetz im großen Stil ist, kann man einige Risiken übertragen. Zunächst werden allgemeine Angriffe auf Netzwerke betrachtet:

Replay - ein Angreifer zeichnet eine authentische Nachricht auf (z.B. Handshake) und spielt sie später ab.

DoS - Message Flooding - ein Satellit oder Endpunkt kann durch viele Nachrichten überfordert werden.

Hijacking - Bodenstation - es kann z.B. durch DoS die eigentliche Bodenstation ausgeschaltet werden und dann in deren Namen weitergesendet werden.

Man in the Middle - bei diesem klassischen Angriff schafft es der Angreifer sich zwischen Sender und Empfänger einzuklinken.

Malware - unter dem Begriff Malware wird bösartige Software zusammengefasst (z.B. Viren, Würmer etc.).

Weiterhin betrachtet Abdalla 802.11 spezifische Risiken, die jedoch zu großen Teilen sehr nah am Standard liegen und abzüglich einiger Ausnahmen, nicht übertragbar sind:

Unkontrollierte Ausbreitung der Funkwellen - die RF-Signale von Satelliten lassen sich selbst durch moderne Spot-Beams nur auf einen Bereich von etwa 300km^2 eingrenzen.

MAC-Spoofing - durch das Fälschen einer MAC-Adresse kann sich ein Angreifer als jemand anders ausgeben.

Schwachstellen bei der Authentifizierung - sind z.B. gewählte Schlüssel zum Authentifizieren stark genug.

Bedrohung der Verfügbarkeit - RF-Wellen können durch verschiedene Quellen gestört werden (z.B. Mikrowellen).

Generierung von Bewegungsprofilen - Anhand der Authentifizierung kann immer zurückverfolgt werden, wo sich ein Clientzugangspunkt befindet.

Als Nächstes wird auf einige organisatorische Risiken eingegangen:

Insiderangriffe - jeder Angriff von einer autorisierten Person ist ein Insiderangriff.

Menschliches Fehlverhalten - menschliches Fehlverhalten ist immer eine Gefahr und der häufigste Angriffspunkt.

Diebstahl - bei einem Diebstahl einer Komponente im Netz kann meist das gesamte Netz angegriffen werden.

Unautorisierte Hardware - werden nicht geprüfte Geräte im Netz in Betrieb genommen, können damit jegliche Sicherheitsvorkehrungen umgangen werden.

Physikalische Risiken - Ausfälle, verursacht durch Naturkatastrophen und Ähnliches zählen hierzu.

[2]

Weitere Überlegungen

Hier füge ich noch ein paar eigene Überlegungen über mögliche Angriffswege auf Megakonstellationen hinzu.

Unbefugtes Hinzufügen eines Satelliten zur Konstellation - ein Angreifer könnte einen Satelliten in einer großen Konstellation "verstecken".

Physische Modifikation eines Satelliten - wenn ein Satellit im Orbit ist, kann er vom Boden aus kaum noch gegen physische Angriffe geschützt werden.

Einklinken in Sat-Sat-Laserverbindungen - dies kann sowohl für Eavesdropping als auch für Man-In-The-Middle genutzt werden.

3.3 Risikobewertung

Jetzt folgt die detaillierte Behandlung der gefundenen Risiken und eine Einschätzung über mögliche Auswirkungen und Verteidigungsmaßnahmen. Dies geschieht anhand eines immer gleich bleibenden Musters.

3.3.1 Denial of Sevice (DoS) eines einzelnen Satelliten

Angriff

Ein DoS Angriff ist ein Angriff, der eine bestimmte Ressource überfordert, indem sie mit sehr vielen oder sehr rechenintensiven Anfragen bombardiert wird. Ein DoS Angriff auf einen Satelliten kann aber auch durch Jamming der genutzten Frequenzen geschehen. Wenn es dem Angreifer gelungen sein sollte, die Kontrolle über den Satelliten zu erlangen, kann er ihn auch gezielt abschalten. Bei LEO-Konstellationen wechselt der für einen Internetzugang zuständige Satellit allerdings alle paar Minuten. Wenn der Angreifer also einen Nutzer des Diensts angreifen will, muss er immer den gerade zuständigen Satelliten angreifen.

Ziel

Das Ziel dieses Angriffs ist die Availability, da die angegriffene Ressource nicht mehr oder nur sehr langsam auf Anfragen reagiert. In diesem Fall ist die Verfügbarkeit des Internetzugangs für die von dem angegriffenen Satelliten versorgten Gebiete das Ziel.

Angreifer

Dieser Angriff muss nicht unbedingt ein gezielter Angriff sein, ein DoS kann auch durch einen Fehler oder eine hohe reguläre Beanspruchung des Systems auftreten. Wenn er jedoch gezielt durchgeführt wird, passiert dies meist durch Botnets, deren Preis in den letzten Jahren kontinuierlich gesunken ist. Dies wird auch Distributed Denial of Service

(DDoS) genannt. Der Angreifer könnte als Ziel einen Nutzer des Internetdiensts haben, oder er versucht dem Anbieter des Diensts Schaden zu zufügen.

Aufwand

Mittel, es wird entweder Jamming-Hardware gebraucht oder Insiderwissen über das Satellitennetzwerk. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Eine typische Verteidigung gegen einen DDoS Angriff besteht aus Firewalls, die DDos typische Pakete erkennen und herausfiltern können.[38] Außerdem kann eine gute Anfragenverteilung einen DoS Angriff abschwächen. Hierfür ist allerdings Redundanz der Ressource notwendig. Gegen Jamming könnten Satelliten die genutzten Frequenzen ändern[25], jedoch wird hierdurch die verfügbare Bandbreite eingeschränkt.

Weitere Informationen

Software Defined Radio (SDR) ist eine Zusammenfassung von Konzepten für Hochfrequenz-Sendern und Empfängern. Es werden dabei viele Dinge mit Software gelöst, wodurch jedoch auch Softwareangriffe, wie etwa das erzeugen von einem Buffer-Overflow möglich werden. Diese Software beinhaltet unter anderem Korrekturen, um Bitfehler bei der Übertragung zu korrigieren. Wenn man also absichtlich falsche Signale sendet, kann diese Software überfordert werden. [33][25]

3.3.2 Denial of Sevice (DoS) eines Clientzugangspunkts

Angriff

Ein DoS auf einen Clientzugangspunkt kann auf herkömmliche Art durchgeführt werden. Der Zugangspunkt gleicht gewöhnlich einem herkömmlichen Router. Dementsprechend kann er auch auf gleiche Weise angegriffen werden. Jamming ist hier auch möglich, allerdings ist physische Nähe für den Angreifer dabei vorteilhaft. Da die Spotbeams moderner

Satelliten eine Fläche von 300km² (Radius etwa 10km) abdecken, ist die physische Nähe allerdings nicht unbedingt erforderlich. Sie wäre vergleichbar mit dem Radius beim Mobilfunknetz.[11]

Ziel

Das Ziel dieses Angriffs ist die Availability, da die angegriffene Ressource nicht mehr oder nur sehr langsam auf Anfragen reagiert. In diesem Fall ist die Verfügbarkeit des Internetzugangs für den Nutzer des angegriffenen Zugangspunkts das Ziel.

Angreifer

Auch dieser Angriff muss nicht unbedingt absichtlich durchgeführt werden, jedoch ist ein DDoS für einen Endpunkt wesentlich einfacher als für einen Satelliten. Deswegen ist dieser Angriff für jeden Angreifer durchführbar, der in der Lage ist, einen herkömmlichen DoS Angriff durchzuführen.

Aufwand

Gering, es wird keine spezielle Hardware benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Das Problem bei der Verteidigung ist, dass nicht einfach eine Redundanz aufgebaut werden kann, da mehrere Antennen in unmittelbarer Nähe sich gegenseitig stören würden. Wenn es allerdings noch einen herkömmlichen Internetanschluss gibt, kann dieser als Backup genutzt werden.

Weitere Informationen

Die Boeing EA-18 Growler ist ein amerikanischer Kampfjet, welches spezielle ”Jamming pods” an Bord hat. Diese werden für Aufklärungseinsätze eingesetzt, allerdings können sie auch feindliche Geräte jammen. [5]

3.3.3 Physische Attacken auf Bodenstationen

Angriff

Ein Satellit wird in den meisten Fällen direkt von Bodenstationen aus gesteuert. Wenn ein Angreifer also Zugang zu einer dieser Bodenstationen bekommt, kann er häufig den Satelliten für seine eigenen Zwecke missbrauchen. Alternativ kann er durch Beschädigung der Bodenstation zu Ausfällen im Betrieb sorgen.

Ziel

Das Ziel dieses Angriffs ist die Possession or Control, da der Angreifer dem Satelliten eigene Befehle geben kann und ihn somit unter Kontrolle hat. Daraus folgend kann er theoretisch auch alle anderen Elemente angreifen.

Angreifer

Dieser Angriff kann nur erschwert von einem außenstehenden Angreifer durchgeführt werden, da er physischen Zugang zu einer Bodenstation braucht. Es ist also wahrscheinlicher, dass dieser Angriff durch autorisiertes Personal durchgeführt wird. Dies kann auch unabsichtlich durch menschliche Fehler geschehen.

Aufwand

Mittel, es wird Zugang zur Station benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Der rein physische Zugang sollte nicht ausreichen, um einem Satelliten Befehle zu geben. Weiterhin werden gerade die modernen Megakonstellationen deutlich weniger vom Boden aus gesteuert, sondern fliegen weitestgehend autonom.[10]

Weitere Informationen

Im Jahr 2011 wurde ein unverschlüsselter NASA Laptop gestohlen, auf dem die Algorithmen zur Kommandierung und Kontrolle der ISS gespeichert waren. [40]

3.3.4 Computer Network Exploitation

Angriff

Ein Angreifer kann das Netzwerk der Bodenstationen kompromittieren und somit ähnlich wie bei dem physischen Angriff, dem Satelliten Befehle senden. Dies geschieht meist durch Ausnutzung falscher Konfigurationen oder angreifbarer Technologien. Hierbei besteht auch die Gefahr, dass mehrere Bodenstationen kompromittiert werden.

Ziel

Das Ziel dieses Angriffs ist die Possession or Control, da der Angreifer dem Satelliten eigene Befehle geben kann und ihn somit unter Kontrolle hat. Daraus folgend kann er theoretisch auch alle anderen Elemente angreifen.

Angreifer

Dieser Angriff kann im Gegensatz zur physischen Attacke von jedem ortsunabhängig durchgeführt werden.

Aufwand

Gering, es wird keine spezielle Hardware benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Zum Einen muss sichergestellt sein, dass das Netzwerk ausreichend gesichert ist. Zum anderen werden in einigen Fällen (z.B. ISS), die Netzwerke zum Steuern des Satelliten physisch vom Internet getrennt. Dadurch können Befehle nur von jemandem vor Ort gesendet werden.

Weitere Informationen

Die NASA berichtete in den Jahren 2010 und 2011 von insgesamt 5.408 Computer Security Vorfällen, die insgesamt einen Schaden von mehr als 7 Mio. US-Dollar angerichtet haben. [40]

3.3.5 Angriff auf Cloudinfrastruktur

Angriff

Satelliten werden häufig mithilfe von Cloudcomputing gesteuert. Cloudsysteme sind allerdings nicht frei von Attacken. Eine Attacke auf die Cloudinfrastruktur kann ähnliche Gefahren wie die Computer Network Exploitation bringen oder den Betrieb aufhalten.[25] Hierbei geht es jedoch eher um die Steuerung des Satelliten und weniger um den Inhalt der Kundenübertragungen.

Ziel

Das Ziel dieses Angriffs ist die Availability, kann jedoch schlimmstenfalls auch andere Elemente, wie etwa Possession or Control betreffen.

Angreifer

Dieser Angriff kann im Gegensatz zur physischen Attacke von jedem ortsunabhängig durchgeführt werden.

Aufwand

Hoch, ein robustes, großes System wie AWS (welches häufig für die Kontrolle von Satelliten genutzt wird)[4] ist schwer anzugreifen. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Um gegen einen Ausfall der Cloud gewappnet zu sein, kann es hilfreich sein, eine eigene lokale Version der Steuerung zu haben. Außerdem sollten nur Cloudanbieter genutzt werden, die ihre System ausreichend schützen.

3.3.6 Datenveränderung/-korruption

Angriff

Es ist die Modifikation von Daten gemeint, entweder in den Bodenstationen oder bei der Übertragung. Korrupte Daten können zu Bugs oder Software-Fehlern führen. Es kann bei solchen Fehlern auch zum Verlust des Satelliten kommen.[25] Die Datenveränderung kann sich aber auch direkt auf den übertragenen Inhalt des Internetdiensts beziehen.

Ziel

Das Ziel dieses Angriffs ist die Integrity, kann sich aber auf andere Elemente wie die Availabilty ausweiten.

Angreifer

Dieser Angriff muss nicht zwangsläufig von einem Angreifer durchgeführt werden, sondern kann auch durch andere Umstände, wie zum Beispiel Bitkorruption entstehen.

Aufwand

Mittel, Zugang zu Kontrollstationen wird benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Wichtige Daten sollten immer auf Konsistenz geprüft werden. Außerdem sollte es für alle Informationen Backups geben.

3.3.7 Supply Chain Attacks

Angriff

Dies ist ein Angriff auf die Herstellung von Komponenten. Dies kann entweder ein Angriff auf die Herstellung von Satelliten sein oder ein Angriff auf die Herstellung der Bodenstationen der Nutzer. Es geht hierbei um die mögliche Veränderung von Komponenten, um so unautorisierte Zugänge oder Sicherheitslücken zu erzeugen, die dann im Betrieb ausgenutzt werden können. [25]

Ziel

Das Ziel dieses Angriffs kann jedes Element sein, abhängig von den Änderungen, die der Angreifer durchführt.

Angreifer

Der Angreifer braucht für diesen Angriff Zugriff auf die Herstellung der Komponente, die er angreifen will. Wenn er nur die Software angreifen will, muss er aber nicht vor Ort sein.

Aufwand

Mittel, es wird Zugang zu Fabriken von Komponenten benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Es sollten möglichst alle kritischen Komponenten selbst hergestellt werden, damit sichergestellt werden kann, dass nichts kompromittiert wurde. Ansonsten müssen Sicherheitsvorkehrungen vertraglich vereinbart und festgehalten werden.

3.3.8 Veraltete Software und Standards

Angriff

Die Verwendung von veralteter Software ist immer ein Sicherheitsrisiko. Dies gilt sowohl für Kontrollstationen als auch für die Übertragung und die Client-Bodenstationen. Veraltete Standards im Satellitenbereich sind nicht darauf ausgelegt, privaten Angriffen standzuhalten.

Ziel

Das Ziel dieses Angriffs sind die Confidentiality und Integrity.

Angreifer

Dieser Angriff kann von quasi jedem durchgeführt werden, da Beschreibungen für mögliche Angriffe meist frei verfügbar sind.

Aufwand

Gering, mögliche Angriffe sind meist bekannt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Wie in jedem Netzwerk muss regelmäßig geprüft werden, ob alle Komponenten und Standards auf dem aktuellen Stand sind und ausreichende Sicherheitsmaßnahmen implementieren.

Weitere Informationen

Iridium ist ein Satellitenkommunikationssystem, dass im Jahr 1998 in Betrieb genommen wurde. Iridium bietet Telefonie, Pagernachrichten und auch Internetzugang über Satelliten an. Allerdings sind die Nachrichten nicht ausreichend verschlüsselt. Jeder, der vollständigen Zugriff auf einen Empfänger hat, kann Pakete, die für andere Personen gedacht waren, mithören und auslesen. Der wahrscheinlichste Grund hierfür ist, dass bei der Entwicklung des Systems Security nicht als großer Faktor mitbedacht wurde. [32]

3.3.9 Eavesdropping

Angriff

Dadurch, dass Satellitenverbindungen zwangsläufig immer Drahtlosverbindungen sind, wird es immer die Gefahr von Eavesdropping geben. Selbst moderne Spotbeams können auf einer Fläche von etwa 300km^2 abgehört werden.[11] Signale, die vom Boden zum Satelliten gesendet werden, können jedoch auf dem Boden nur in einem deutlich geringeren Umkreis abgehört werden. Dies könnte jedoch durch Empfänger in großer Höhe umgangen werden (z.B. durch Heliumballons in der Stratosphäre).

Ziel

Das Ziel dieses Angriffs sind die Confidentiality.

Angreifer

Dieser Angriff kann von jedem durchgeführt werden, der in ungefährer geographischer Nähe des Ziels ist.

Aufwand

Mittel, es wird ein geeigneter Empfänger und ungefähre geographische Nähe benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Gegen diesen Angriff gibt es keine direkte Verteidigungsstrategie, allerdings sollten immer alle Verbindungen verschlüsselt sein, da man auch unabhängig von der Nutzung von Satelliteninternet nicht davon ausgehen kann, dass eine Verbindung nicht abgehört wird.

Weitere Informationen

Auch hier lässt sich das Beispiel Iridium aus dem Kapitel Veraltete Software und Standards anführen.

3.3.10 Hijacking - Satellit

Angriff

Mit Hijacking ist die komplette Übernahme eines Satelliten gemeint. Dies kann geschehen, wenn es dem Angreifer möglich ist, nicht nur die Kontrolle zu erlangen, sondern auch den eigentlichen Inhaber des Satelliten auszuschließen. Da der Satellit für Klienten allerdings immer noch normal erscheint, wäre dies ein besonders großes Problem.

Ziel

Das Ziel dieses Angriffs ist die Possession or Control und damit folglich auch alle anderen Möglichkeiten, so könnte zum Beispiel jeglicher Internetverkehr, der durch den betroffenen Satelliten abgewickelt wird, mitgelesen werden.

Angreifer

Der Angreifer braucht eine Möglichkeit, um mit dem Satelliten zu kommunizieren, um ihm Befehle zu geben. Außerdem muss er interne Details über die Steuerungs- und Kontrollalgorithmen des Satelliten kennen, um ihn übernehmen zu können.

Aufwand

Mittel, es wird spezielle Hardware, aber vor allem Insiderwissen benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Alle nötigen Informationen zu Übernahme sollte so gut geschützt sein, dass der Angriff quasi nur von einem Insider ausgeführt werden kann. Außerdem sollte es eine Methode geben, um Klient-Zugängen mitzuteilen, dass ein Satellit kompromittiert ist, damit sie sich nicht mehr mit ihm verbinden.

3.3.11 Spoofing

Angriff

Spoofing ist eine Verschleierung oder Veränderung des Absenders eines Pakets, sodass der Empfänger den eigentlichen Absender nicht kennt. Dieser Angriff kann sich auf die Verbindung zur Steuerung des Satelliten richten, indem getarnte Steuerbefehle gesendet werden, um die Kontrolle über den Satelliten zu übernehmen. Er kann sich aber auch auf die Internetverbindung zwischen Satellit und Bodenstationen richten. Dies geht jedoch in erster Linie nur Richtung Satellit, da ansonsten ein Sender in großer Höhe oder ein eigener Satellit genutzt werden müsste.

Ziel

Das Ziel dieses Angriffs ist die Authenticity und Integrity.

Angreifer

Der Angreifer kann jeder mit einem geeigneten Empfänger und Sender sein, da die Protokolle abhörbar sind.

Aufwand

Mittel, ein Sender wird benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Protokolle müssen ausreichend verschlüsselt sein und das Key Management muss ausreichend gesichert sein.

3.3.12 DoS - Clogging

Angriff

Satelliten haben eingebaute Hardware und Software zur Fehlerkorrektur von Signalen. Ein Angreifer könnte jedoch gezielt fehlerhafte Pakete senden, um diese Fehlerkorrektur auszulasten. Dies kann entweder nur diese Fehlerkorrektur überlasten oder zu einem erhöhten Stromverbrauch führen und damit schlimmstenfalls zu einem Komplettausfall führen. Es kann zum Beispiel ein reguläres Paket aufgezeichnet werden und dann einzelne Bits verändert werden. Wenn dann ein Replay durchgeführt wird, sollte die Fehlerkorrektur des Satelliten eingreifen.

Ziel

Das Ziel dieses Angriffs die Availability.

Angreifer

Der Angriff kann von jedem durchgeführt werden, der in der Lage ist, reguläre Pakete aufzuzeichnen und dann verändert zu senden. Es kann aber auch durch natürliche Störelemente, wie etwa Wetterphänomene oder Sonnenstürme zu fehlerhaften Signalen kommen, die DoS - Clogging herbeiführen können.

Aufwand

Gering, es wird zugängliche Sendehardware benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Es muss für den Satelliten aus dem Paket schnell erkennbar sein, ob ein Paket regulär ist oder nicht. Es gibt aber keine wirklich effiziente Verteidigung, da Fehlerkorrektur bei großen Distanzen immer einer Neuübertragung vorzuziehen ist.

3.3.13 Replay

Angriff

Klassische Replay Attacken auf Drahtlosnetzwerke können verschiedene Dinge bezwecken. Eine Möglichkeit wäre zum Beispiel das Mitschneiden von Authentifizierungsnachrichten um dann, wenn das Protokoll dies zulässt, ein eigenes Gerät zu authentifizieren. Replay kann aber auch dazu genutzt werden, um eine Verbindung zum Erliegen zu bringen, wenn zum Beispiel veraltete Acknowledgements gesendet werden.

Ziel

Das Ziel dieses Angriffs kann nicht klar definiert werden, da Replay viele Dinge angreifen kann. Bei jedem Protokoll kann aber immer die Availability durch Replay angegriffen werden.

Angreifer

Dieser Angriff kann ohne viel Vorwissen von jedem durchgeführt werden, der das rohe Protokoll auslesen und senden kann.

Aufwand

Gering, simple Empfänger und Senderhardware wird benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Die Protokolle müssen immer verschlüsselt sein und der Handshake muss gesichert sein, sodass jede Nachricht immer einem bestimmten Klient zugeordnet werden kann. Alle Nachrichten sollten mit einer verschlüsselten laufenden Nummer ausgestattet sein, damit veraltete Nachrichten schnell als solche erkannt werden können.

3.3.14 Hijacking - Bodenstation

Angriff

Wenn eine Bodenstation für Satelliten kompromittiert wird, kann der Angreifer mit dem Satelliten theoretisch alles machen. Er könnte entweder das Netzwerk der Bodenstation angreifen und sich so Zugang verschaffen, oder er bekommt örtlichen Zugang und kommt so in das System.

Ziel

Das Ziel dieses Angriffs die Possession or Control.

Angreifer

Der Angreifer kann am einfachsten von einem Insider durchgeführt werden, jedoch ein Angriff auf das Netzwerk der Bodenstation kann auch von jedem mit ausreichend Vorwissen durchgeführt werden.

Aufwand

Mittel, örtlicher Zugang oder Zugang zum Netzwerk wird benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Selbst ein physischer Zugang zu der Bodenstation sollte nicht die vollständige Kontrolle über den Satelliten ermöglichen. Außerdem sollte es unabhängige Backup-Stationen geben, sodass sobald eine Station kompromittiert ist, sie abgeschaltet werden kann. Eventuell könnte ein Satellit sogar über Zwei-Faktor-Methodiken gesteuert werden, sodass eine andere unabhängige Bodenstation jeden Befehl bestätigen muss.

3.3.15 Man in the Middle

Angriff

Bei einer Man in the Middle Attacke schaltet sich der Angreifer zwischen die Kommunikation der angegriffenen Parteien. Dies könnte bei Satelliteninternet zum Beispiel geschehen, wenn der Angreifer Kontrolle über den Satelliten hat, dann kann er an der Stelle sich für beide Seiten als die jeweils andere Partei ausgeben. Die Verbindung zwischen Klient und Satellit ist hier aber nicht so einfach anzugreifen, da die Originalnachrichten abgehört, blockiert und ersetzt werden müssen. Es ist also wahrscheinlicher, dass entweder das Satellitensegment betroffen ist, oder einer der Zugangspunkte.

Ziel

Das Ziel dieses Angriffs ist die Integrity.

Angreifer

Dieser Angriff benötigt einen sehr großen Aufwand, kann also entweder von einem Insider durchgeführt werden oder von jemandem, der bereit ist, sehr viele Ressourcen aufzubringen. Eine Ausnahme hierfür wäre jedoch eine Schwachstelle im Klientzugangspunkt, welche auch ohne großen Aufwand einen Man in the Middle Angriff ermöglichen kann.

Aufwand

Mittel bis hoch, es wird Hardware zum Unterdrücken der Originalnachrichten benötigt oder ein Zugang zu einer Komponente im Netz. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Man in the Middle Angriffe sind auch in herkömmlichen Netzwerken immer eine Gefahr und verlangen die Verschlüsselung der Kommunikation. Vor allem eine geeignete Key-Infrastruktur ist hierfür von Bedeutung. Hier gibt es bei Satelliteninternet keine größeren Unterschiede.

3.3.16 Malware

Angriff

Malware kann grundsätzlich jedes System befallen, das Software nutzt. Es kann also sowohl die Klientzugangspunkte als auch den Satelliten und die anderen Boden- oder Kontrollstationen treffen. Herkömmlich ist Malware meist ungezielt, jedoch in diesem Fall müsste die Malware speziell darauf ausgelegt sein, diese Systeme zu befallen.

Ziel

Das Ziel dieses Angriffs kann praktisch alles sein, eventuell die Usability, da generelle Schutzmaßnahmen gegen Malware eingeführt werden müssen.

Angreifer

Malware kann von jedem, der programmieren kann, entwickelt werden. Da die Klientzugangspunkte für jeden zugänglich sind, muss auch damit gerechnet werden, dass versucht wird, sie anzugreifen.

Aufwand

Mittel, es wird Insiderwissen benötigt, um gezielte Malwareangriffe auf das Netzwerk durchzuführen. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Die häufigste Verteidigung gegen Malware sind Virenschutzprogramme, welche jedoch in speziellen Systemen wie Satelliten wegen des hohen Energieverbrauchs, kaum eingesetzt werden können. Ein Satellit sollte jedoch möglichst gar nicht mit dem Payload interagieren, sodass er zumindest nicht über die Internetverbindung mit Malware infiziert werden kann.

3.3.17 Unkontrollierte Ausbreitung der Funkwellen

Angriff

Drahtlosnetzwerke haben fast immer das Problem, dass sich Funkwellen unkontrolliert ausbreiten. Bei Satellitenverbindungen geschieht dies zwar nicht komplett ungesteuert, da gerichtete Beams genutzt werden. Allerdings sind diese Beamspots immer noch etwa 300km^2 groß und Reststrahlung wird auch noch in größeren Flächen messbar sein.[11] Es ist außerdem aufgrund der Natur von Strahlung auch unmöglich festzustellen, ob sie von einem Empfänger empfangen werden. Es kann also nie festgestellt werden, wer die Funkwellen empfängt. Dies kann zu Eavesdropping führen, aber auch eine gegenseitige Störung mit anderen Funkquellen erzeugen.

Ziel

Das Ziel dieses Angriffs ist die Confidentiality und Availability.

Angreifer

Der Angreifer muss sich nur in ungefährer geografischer Nähe zu seinem Ziel befinden und empfängt alle Funkwellen, die für das Ziel bestimmt sind.

Aufwand

Gering, ein Empfänger wird benötigt. Dieses Risiko ist ein akutes Risiko.

Verteidigung

Die Verteidigung hierfür ist ähnlich wie beim WLAN-Standard, die Verbindung muss verschlüsselt sein. Gegen die Störungen kann vorgegangen werden, indem man sich an die zugewiesenen Frequenzen hält.

3.3.18 MAC-Spoofing

Angriff

MAC-Spoofing kann bei WLAN angewendet werden. Inwieweit dies auch für ein Satellitennetz anwendbar ist, hängt vom verwendeten Standard ab. Es kann aber davon ausgegangen werden, dass eine Art MAC-Adresse verwendet wird, um die einzelnen Zugangspunkte zu identifizieren und authentifizieren. Diese könnte dann auch modifiziert werden, um sich als jemand anderes auszugeben.

Ziel

Das Ziel dieses Angriffs ist die Authenticity.

Angreifer

Der Angreifer kann jeder sein, der vollständige Kontrolle über einen Sender hat. Ein Empfänger wäre außerdem hilfreich, damit andere Adressen empfangen werden können und nicht geraten werden müssen.

Aufwand

Gering, es wird ein Sender benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Die MAC-Adresse sollte niemals allein zur Authentifizierung genutzt werden. Es muss immer ein Shared-Secret geben, dass in Kombination mit der MAC-Adresse genutzt wird. Dies gilt natürlich auch für alle äquivalenten Adressen, die ein Zugangspunkt verwenden könnte.

3.3.19 Schwachstellen bei der Authentifizierung

Angriff

Die Authentifizierung von Geräten in Drahtlosnetzwerken ist immer eine Gefahrenstelle. Hier können verschiedene Bedrohungen entstehen, wie etwa die Preisgabe von Keys oder anderen Shared Secrets. Dadurch können Verbindungen danach abgehört oder modifiziert werden. Diese Schwachstellen können aber hier nicht genau bewertet werden, da nicht auf die konkreten Protokolle eingegangen werden kann.

Ziel

Das Ziel dieses Angriffs ist die Confidentiality, Integrity und Authenticity. Jedoch ist hier auch die Utility zu beachten, da es bei LEO-Konstellationen sehr viele Neuauthentifizierungen stattfinden und sie deswegen sehr performant sein müssen.

Angreifer

Der Angreifer kann jeder sein, der die Pakete zur Authentifizierung empfangen kann.

Aufwand

Gering, mögliche Angriffe sind meist bekannt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Eventuell können Sicherheitsmechanismen aus bestehenden Standards wie WLAN verwendet werden, jedoch muss hierbei auf die Utility geachtet werden.

3.3.20 Bedrohung der Verfügbarkeit

Angriff

Hiermit ist gemeint, dass Funkwellen durch viele Materialien abgeschirmt werden. Satellitenschüsseln können auf Dächern von Häusern verwendet werden oder auf Flugzeugen und Schiffen. Bei Autos oder LKWs hingegen sind Satellitennetzwerke nicht ohne Weiteres einzusetzen, da Tunnel oder Brücken und selbst Bäume und hohe Häuser die Verbindung immer wieder unterbrechen oder stören würden.

Ziel

Das Ziel dieses Angriffs ist die Availability.

Angreifer

Dieser Angriff hat keinen aktiven Angreifer, sondern ist eher eine Prüfung der Nutzbarkeit von Satelliteninternet in bestimmten Einsatzgebieten. Ein Angreifer könnte aber auch ein Hindernis platzieren, welches die Signale stört.

Aufwand

Gering, mögliche Angriffe sind meist bekannt. Dieses Risiko ist ein akutes.

Verteidigung

Es muss sichergestellt sein, dass über der Satellitenschüssel keine Objekte sind, die Funkwellen stören können. Dabei muss auch beachtet werden, dass dies auch für die Dauer der Nutzung der Fall bleibt.

Weitere Informationen

Elon Musk kündigte an, Starlink Terminals vorerst nicht in Autos verbauen zu wollen. Die Schüsseln seien zu groß, und die Verbindungen würden zu oft durch Hindernisse unterbrochen. Für LKWs oder Wohnwagen hingegen sei der Einsatz naheliegender. [26]

3.3.21 Generierung von Bewegungsprofilen

Angriff

Hier ist nicht wie etwa bei einem Smartphone eine genaue Ortung von Personen gemeint, jedoch kann anhand der Satelliten ungefähr geortet werden, wo sich der Empfänger befindet. Wenn man die Schüssel zum Beispiel auf einem Schiff verwendet, würde der Betreiber immer die etwaige Position bestimmen können.

Ziel

Das Ziel dieses Angriffs liegt eher im Bereich des Datenschutzes als im Bereich des Parkerian hexad.

Angreifer

Diese Informationen können von jemandem abgerufen werden, der die Satellitenkonstellation kontrolliert. Es kann davon ausgegangen werden, dass etwa Geheimdienste der USA verlangen werden, staatlichen Zugang zu solchen Informationen zu bekommen.

Aufwand

Mittel, kann in erster Linie nur vom Betreiber durchgeführt werden. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Wenn man nicht gefunden werden will, sollte man keine Verbindung zur Außenwelt aufbauen. Außerdem sollte hiermit keine exakte Bestimmung des Aufenthaltsorts möglich sein.

3.3.22 Insiderangriffe

Angriff

Autorisierte Personen haben häufig Zugang zu sehr kritischen Ressourcen. Wenn also jemand diesen Zugang zu eigenen Zwecken missbraucht, kann damit sehr viel Schaden angerichtet werden. Hier geht es hauptsächlich um die Steuerung und Kontrolle der Satelliten, da alle anderen Systeme automatisch ablaufen. Bei modernen Megakonstellationen ist allerdings selbst die Steuerung der Satelliten autonom, weswegen Insider weniger Kontrolle über sie haben sollten. Trotzdem ist es erwartbar, dass alles von Menschen überschrieben werden kann, weswegen Insider am Ende trotzdem sehr mächtig sind.

Ziel

Das Ziel dieses Angriffs ist die Possession or control, da autorisierte Personen die Kontrolle über wichtige Ressourcen bekommen können.

Angreifer

Dieser Angriff kann nur von Insidern ausgeführt werden.

Aufwand

Mittel, kann nur von autorisierten Personen durchgeführt werden. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Es müssen für alle Personen, die eingestellt werden, besonders in kritischen Bereichen gründliche Backgroundchecks durchgeführt werden. Außerdem sollte niemals eine Person allein genug Wissen haben, um größere Angriffe durchzuführen. Es könnte weiterhin ein Vier-Augen-Prinzip eingeführt werden, bei dem an entscheidenden Kontrollstationen immer mehr als eine Person vor Ort sind.

3.3.23 Menschliches Fehlverhalten

Angriff

Dies ist kein direkter Angriff, sondern mögliche Fehler, die von beteiligten Personen gemacht werden können. In fast jedem System entstehen die größten Sicherheitslücken durch menschliches Fehlverhalten. Dies kann in Form von falscher Konfiguration oder durch Preisgabe von kritischen Informationen geschehen. Es kann aber auch etwas simples, wie die Verwendung eines privaten USB-Sticks sein.

Ziel

Das Ziel dieses Angriffs kann alles sein, es muss aber immer auf die Usability geachtet werden.

Angreifer

Es gibt keinen direkten Angreifer, es kann jeder, der an dem Prozess beteiligt ist, Fehler machen und damit unerwünschte Zustände oder Sicherheitslücken erzeugen.

Aufwand

Gering, Fehler können immer passieren. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Mitarbeiter können sich gegenseitig kontrollieren, und jeder sollte ausreichend ausgebildet werden, um Verantwortung zu übernehmen. Weiterhin könnte es Regeln geben, dass sämtliche Privatgegenstände (Smartphones, USB-Sticks, usw.) beim Betreten des Geländes abgegeben werden müssen, um die Gefahr von Zwischenfällen zu minimieren. Menschliches Fehlverhalten lässt sich allerdings nie ganz ausschließen.

3.3.24 Diebstahl

Angriff

Jegliche Komponenten können gestohlen werden. Sowohl Hardware, die im Bodensegment genutzt wird, aber auch ein ganzer Satellit könnte gestohlen werden, auch wenn davon aktuell aufgrund des Aufwands nicht auszugehen ist. Es könnte aber zum Beispiel bei einem Fehlstart einer Rakete Trümmerteile geben, die Satelliten enthalten, wodurch kritische Informationen ausgelesen werden können.

Ziel

Das Ziel dieses Angriffs Possession or Control.

Angreifer

Der Angreifer braucht physischen Zugang zu der zu stehlenden Komponente, es ist also recht wahrscheinlich, dass Insider beteiligt sind.

Aufwand

Mittel, es wird Zugang zu der zu stehlenden Komponente benötigt. Dieser Angriff kann aktuell durchgeführt werden.

Verteidigung

Der reine physische Zugang sollte nicht zur kompletten Kontrolle über eine Komponente führen und alle Bodensegmente müssen ausreichend geschützt werden. Der physische Schutz im Weltraumsegment ist allerdings aktuell nicht umzusetzen.

Weitere Informationen

Die NASA hat zwischen April 2009 und April 2011, 48 mobile Geräte teilweise mit kritischen Daten als gestohlen gemeldet. Es wird deswegen daran gearbeitet, alle Geräte ausreichend zu verschlüsseln. [40] Das Problem sollte inzwischen gelöst sein, aber es wurden keine neueren Daten hierzu gefunden.

3.3.25 Unautorisierte Hardware

Angriff

Klassischerweise wird hiermit etwas wie ein unautorisierter Accesspoint gemeint, der nicht den Standards des Netzwerks entspricht. Meist geschieht dies durch temporäre Bequemlichkeitslösungen oder schnelle Fehlerkorrekturen, die nicht ausreichend geprüft werden. Bei einer Satellitenverbindung könnte hier etwa ein inoffizieller Klientzugangspunkt verwendet werden, der nicht den Sicherheitsstandards entspricht. Dies kann nicht nur Sicherheitslücken erzeugen, sondern auch die Performance beeinflussen.

Ziel

Das Ziel dieses Angriffs ist die Integrity, wobei hier eher die Integrität des gesamten Systems gemeint ist.

Angreifer

Der Täter ist hier jemand, der meist aus Bequemlichkeit oder um Geld zu sparen, andere Hardware verwendet, als eigentlich gedacht ist. Es kann aber auch jemand sein, der absichtlich falsche Hardware nutzt, um Sicherheitslücken zu erzeugen.

Aufwand

Mittel, es wird kompatible Hardware benötigt. Dieser Angriff kann in näherer Zukunft, wenn die verwendete Hardware bekannt genug ist, durchgeführt werden.

Verteidigung

Das System sollte erkennen können, ob alle Komponenten autorisiert sind und bei unautorisierter Hardware Warnungen geben oder sie gar nicht erst akzeptieren.

3.3.26 Physikalische Risiken

Angriff

Dies ist kein aktiver Angriff, sondern Ausfälle, welche durch Naturkatastrophen oder Ähnliches verursacht werden. So können zum Beispiel Bodenzugangsstellen für die Internetverbindung durch Feuer oder Erdbeben bedroht werden. Dies sollte allerdings keinen großen Einfluss auf die Verfügbarkeit haben, da es sehr viele von diesen Stationen geben wird und die Satelliten untereinander kommunizieren können. Wenn es allerdings zu Katastrophen im Weltraumsegment kommt, wird es gravierender. Hier kann es zum Beispiel zu einem Sonnensturm kommen, der Satelliten zum Ausfall bringen kann. Weiterhin gibt es viele Befürchtungen, dass es zu dem Kessler-Syndrom kommen kann.[12] Sollte dies

geschehen, würden nahezu sämtliche Satelliten ausfallen und auch nicht ohne Weiteres ersetzt werden können.

Ziel

Die Folge eines Unfalls wäre die Einschränkung der Availability.

Angreifer

Es gibt hier in der Regel keinen Angreifer, sondern es sind Unfälle, die auf Naturkatastrophen basieren. Das Kessler-Syndrom könnte allerdings durch einen Abschuss eines Satelliten erzeugt werden. Es gibt einige Nationen, die über Antisatellitenwaffen verfügen.[36]

Aufwand

Gering, kann immer passieren. Diese Risiken sind nicht unbedingt akut, können jedoch immer eintreten.

Verteidigung

Im Bodensegment kann Redundanz verwendet werden. Im Weltraumsegment gibt es Möglichkeiten, Satelliten vor Sonnenstürmen zu schützen.

Weitere Informationen

2019 hat Indien einen eigenen Kommunikationssatelliten mit einer Abwehrrakete abgeschossen, um sie zu testen. Dies hat ein Trümmerfeld erzeugt, welches auch andere Satelliten bedroht. Indien ist allerdings nicht das einzige Land mit Antisatellitenwaffen (USA, Russland, China).[36]

Sonnenstürme oder auch "Koronare Massen-Auswürfe" sind Partikelwolken, die zu geomagnetischen Stürmen führen können und zu Ausfällen bei Satelliten führen können. Sie sind zwar vorhersehbar, aber nicht verhinderbar.[22]

3.3.27 Unbefugtes Hinzufügen eines Satelliten zur Konstellation

Angriff

Vom Boden aus sind einzelne Satelliten kaum voneinander zu unterscheiden. Der Klientzugangspunkt kann einzelne Satelliten nur anhand der Signale identifizieren. Wenn diese Signale aber imitiert werden, kann sich ein fremder Satellit als ein anderer ausgeben. Dies kann für Man-In-The-Middle oder aber auch Eavesdropping genutzt werden. Außerdem kann der Konstellationsbetreiber kaum etwas gegen einen fremden Satelliten unternehmen.

Ziel

Das Ziel dieses Angriffs ist die Authenticity, da sich ein Satellit als ein anderer ausgeben kann und die Confidentiality, da ein Satellit in einem ähnlichen Orbit alle Pakete mithören kann.

Angreifer

Dieser Angriff ist sehr ressourcenintensiv, da ein Satellit im richtigen Orbit benötigt wird. Deswegen ist davon auszugehen, dass dies zurzeit nur von Staaten oder ähnlich großen Organisationen durchführbar wäre. Es kann aber auch durch die Übernahme eines Satelliten geschehen.

Aufwand

Hoch, es muss ein Satellit in die korrekte Umlaufbahn gebracht werden. Dieser Angriff ist akut nicht zu befürchten.

Verteidigung

Es muss sichergestellt werden, dass ein Klient nur mit autorisierten Satelliten kommunizieren kann.

3.3.28 Physische Modifikation eines Satelliten

Angriff

Sobald ein Satellit im Orbit um die Erde fliegt, kann er physisch kaum noch geschützt werden. Wenn ein Angreifer versucht, ihn physisch zu verändern, dann kann dies entweder zum Ausfall führen (Antisatellitenwaffen), oder aber wenn Komponenten auf ihm installiert werden, kann er auch übernommen werden oder Datenverkehr mitgehört oder modifiziert werden.

Ziel

Hierdurch sind alle zu schützenden Ziele bedroht, da mit dem Satelliten alles gemacht werden kann.

Angreifer

Dieser Angriff ist sehr ressourcenintensiv, da ein Satellit im richtigen Orbit benötigt wird, um Zugang zum Zielsatelliten zu bekommen. Deswegen ist davon auszugehen, dass dies zurzeit nur von Staaten oder ähnlich großen Organisationen durchführbar wäre.

Aufwand

Hoch, es wird physischer Zugang zu einem Satelliten im Orbit benötigt. Dieser Angriff ist akut nicht zu befürchten.

Verteidigung

Zur Zeit werden quasi alle Satelliten in Erdumlaufbahn vom Boden aus beobachtet. Wenn also ein Satellit sich einem anderen nähert, wird dies auffallen. Der Zielsatellit könnte dann Ausweichmanöver durchführen oder schlimmsten Falls ganz abgeschaltet werden. In wieweit diese Beobachtung aber in Zukunft noch möglich sein wird, ist unklar, da Satellitenkonstellationen immer größer werden.

Weitere Informationen

Das Unternehmen Northrop Grumman Corporation hat ein Raumschiff entwickelt, welches sich an Satelliten andocken kann, denen der Treibstoff ausgegangen war. Dadurch kann die Lebenszeit eines Satelliten im Orbit verlängert werden. Diese Technik könnte aber natürlich auch für andere Zwecke missbraucht werden, und wenn so ein Satellit über fortgeschrittenere Technik verfügt, könnte er einen Satelliten auch modifizieren.[41]

3.3.29 Einklinken in Sat-Sat-Laserverbindungen

Angriff

Starlink-Satelliten, aber auch andere Kommunikationssatelliten können Verbindungen untereinander aufbauen. Bei Starlink soll dies durch Laserverbindungen geschehen. Dadurch würden solche Verbindungen eventuell gar nicht mehr durch herkömmliche Leitungen auf dem Boden gehen. Ein Angreifer könnte aber einen Satelliten zwischen der Konstellation positionieren, der dann diese Laserverbindung abhört und eventuell modifiziert.

Ziel

Das Ziel dieses Angriffs ist die Confidentiality, kann aber auch die Integrity sein.

Angreifer

Dieser Angriff ist sehr ressourcenintensiv, da ein Satellit im richtigen Orbit benötigt wird. Deswegen ist davon auszugehen, dass dies zurzeit nur von Staaten oder ähnlich großen Organisationen durchführbar wäre. Wenn aber ein Satellit aus der Konstellation übernommen wird, kann dieser hierfür verwendet werden, da er die nötigen Kommunikationsgeräte an Bord hat.

Aufwand

Hoch, es muss ein Satellit in die korrekte Umlaufbahn gebracht werden. Dieser Angriff ist erst langfristig zu befürchten.

Verteidigung

Die Laserverbindungen sind sehr gebündelt und haben nicht viel Reststrahlung. Deswegen müsste ein Angreifer sich direkt im Pfad befinden, wodurch die Originalverbindung unterbrochen werden würde.

3.4 Darstellung und Einordnung der Ergebnisse

Die Tabelle 3.1 zeigt einen Überblick, welchen Risiken wie aufwändig sind und was durch diese Risiken bedroht ist. Außerdem zeigt die Tabelle, welche Risiken eine akute Gefahr darstellen und welche erst langfristig bedacht werden müssen. Für Nutzer von Satelliteninternet gibt es fast nie eine direkte Möglichkeit, sich vor diesen Risiken zu schützen. Der Schutz ist in fast allen Fällen etwas, dass der Betreiber des Netzes beachten muss. Die wohl wahrscheinlichsten geplanten Angriffe gegen Kunden von Satelliteninternet sind entweder Eavesdropping oder Angriffe auf die Availability. Es muss also sichergestellt sein, dass sämtlicher Verkehr über das Netz ausreichend verschlüsselt ist. Gegen Angriffe auf die Availabilty kann man sich nur schützen, wenn man einen anderen Zugang zum Internet hat. Sollte dieser andere Zugang auch über Satellit gehen, besteht jedoch die Gefahr, dass zum Beispiel durch Jamming, beide Zugänge gestört werden. Wenn also Satelliteninternet die einzige Möglichkeit ist, einen Zugang zum Internet zu bekommen (z.B. sehr abgelegene Lage oder Fahrzeuge), kann man sich gegen diese Risiken kaum schützen. Eine Möglichkeit wäre hier, verschiedene Anbieter zu nutzen. Wenn Availability aber von sehr großer Bedeutung ist, etwa bei Online-Dienstleistungen, ist von der Nutzung von Satelliteninternet abzuraten. Die Technik ist momentan noch zu neu, um von einem stabilen Betrieb auszugehen, und langfristig wird es zu viele Möglichkeiten geben, die Availability anzugreifen. Wenn man einen herkömmlichen Breitbandanschluss zur Verfügung hat, sollte man das Satellitennetz eher als Backup nutzen, falls das herkömmliche Netz eine Störung hat. Es gibt aber Fälle, wo das Satellitennetz schneller sein kann als herkömmliche Netze und in diesen Fällen wäre dann der herkömmliche Anschluss das Backup.

Bedrohung	Conf.	Inte.	Avai.	Poss.	Auth.	Util.	Aufwand	Akut
Denial of Sevice (DoS) eines einzelnen Satelliten			X				Mittel	X
Denial of Sevice (DoS) eines Clientzugangspunkts			X				Gering	X
Physische Attacken auf Bodenstationen				X			Mittel	X
Computer Network Exploitation				X			Gering	X
Angriff auf Cloudinfrastruktur			X	(X)			Hoch	X
Datenveränderung/-korruption		X	X				Mittel	X
Supply Chain Attacks	(X)	(X)	(X)	(X)	(X)	(X)	Mittel	X
Veraltete Software und Standards	X	X					Gering	X
Eavesdropping	X						Mittel	X
Hijacking - Satellit			X				Mittel	X
Spoofing		X			X		Mittel	X
DoS - Clogging			X				Gering	X
Replay	(X)	(X)	X	(X)	(X)	(X)	Mittel	X
Hijacking - Bodenstation				X			Mittel	X
Man in the Middle		X					Mittel/Hoch	X
Malware	X	X	X	X	X	X	Mittel	X
Unkontrollierte Ausbreitung der Funkwellen	X		X				Gering	X
MAC-Spoofing					X		Gering	X
Schwachstellen bei der Authentifizierung	X	X			X	(X)	Gering	X
Bedrohung der Verfügbarkeit			X				Gering	X
Generierung von Bewegungsprofilen	(X)						Mittel	X
Insiderangriffe				X			Mittel	X
Menschliches Fehlverhalten						X	Gering	X
Diebstahl				X			Mittel	X
Unautorisierte Hardware		X					Mittel	(X)
Physikalische Risiken			X				Gering	(X)
Unbefugtes Hinzufügen eines Satelliten zur Konstellation	X				X		Hoch	
Physische Modifikation eines Satelliten	X	X	X	X	X		Hoch	
Einklinken in Sat-Sat-Laserverbindungen	X	X					Hoch	

Tabelle 3.1: Zusammenfassung der Bedrohungen

Es folgen nun drei einfache Szenarien mit Einschätzungen für die Sinnhaftigkeit des Einsatzes von Satelliteninternet in Bezug auf die Sicherheit.

Szenario 1: Privatanwender

Jemand hat sich gerade ein neues Haus in einer ländlichen Region gekauft. Ein Internetanschluss ist dort über DSL zwar verfügbar, allerdings gibt es eine maximale Downloadrate von 8000 Kbit/s. Dies ist zwar für eine grundlegende Nutzung des Internets ausreichend, allerdings ab dem Moment, wo mehrere Personen gleichzeitig das Internet nutzen, oder ein Film gestreamt werden soll, kommt es schnell zu Problemen. Ein Internetanschluss über einen geostationären Satelliten wäre hier nicht empfehlenswert, da die Latenzen zu groß sind, aber ein Zugang über eine LEO-Konstellation wie Starlink ist eine Alternative. Verfügbarkeit ist in diesem Fall keine sehr große Sorge, da durch eventuelle Ausfälle keine finanziellen Verluste gemacht werden. Weiterhin ist von gezielten Angriffen auf die Availability nicht auszugehen. Die kritischsten Daten, die übertragen werden, sind Online-Banking Daten. Da jedoch die Bank über verschlüsselte Protokolle erreicht wird, ist nicht davon auszugehen, dass eine dritte Person die Daten mitlesen kann. In diesem Fall ist ein Internetanschluss über Satellit ohne zusätzliche Sicherheitsvorkehrungen einsetzbar.

Szenario 2: Rechenzentrumsbetreiber

Ein Betreiber eines Rechenzentrums möchte einen Satelliteninternetanschluss als Backup für seinen Internetanschluss nutzen und ihn als Vorteil bewerben, da er einen vom regionalen Anschluss unabhängigen Zugang ermöglicht, der über große Distanzen eine niedrigere Latenz ermöglicht. Aufgrund der benötigten Datenraten und niedrigen Latenz kommen nur LEO-Konstellationen infrage. Die Availability spielt hier eine große Rolle und ist auch ein lukratives Angriffsziel. Deswegen muss etwa mit Jamming-Angriffen gerechnet werden. Die anderen Elemente sind für den Betreiber des Rechenzentrums von untergeordneterer Bedeutung, da sie von den Kunden durch den Einsatz von genügend geschützten Protokollen gesichert werden. Alternativ könnte der Betreiber auch ein verschlüsseltes VPN anbieten, indem er als zweiten Endpunkt einen weiteren Satellitenzugang, an einem anderen geografischen Ort installiert. Doch gerade durch die Wichtigkeit der Availability, sollte der Satelliteninternetzugang nicht als Hauptzugang genutzt werden. Er könnte

für interessierte Kunden jedoch als Zusatzoption angeboten werden und als generelles Backup dienen, wenn der kabelgebundene Zugang ein Problem hat.

Szenario 3: Logistikunternehmen

Ein Logistikunternehmen, welches Schiffe und Transportflugzeuge betreibt, prüft die Möglichkeit, jedes Fahrzeug mit einem Internetanschluss über Satellit auszustatten. Dies wird hauptsächlich für Standortübertragungen, aber auch für eventuelle Planänderungen und privaten Gebrauch genutzt. Ein geostationärer Anschluss wäre hier denkbar, da hohe Latenzen bei vereinzelten Nachrichten kein Problem darstellen. Allerdings sind geostationäre Satelliten an einen Ort gebunden, weswegen eine weltweite Nutzung nicht möglich ist. Es wäre also auch in diesem Fall eine LEO oder MEO-Konstellation die geeignetere Alternative. Hier ist vor allem die Authenticity und die Integrity von großer Bedeutung, aber nicht so sehr die Confidentiality. Die Availability spielt bei langsameren Fahrzeugen wie Schiffen keine so große Bedeutung, sie ist aber auch nicht so leicht angreifbar, da sie der geografische Standort des Zugangs permanent ändert. Außerdem ist sie nicht durch natürliche Abschirmung wie Tunnel oder Berge gefährdet, wie es bei LKWs der Fall wäre. Es müsste also entweder der Zugangspunkt oder das gesamte Netz angegriffen werden, um zu einem Ausfall zu führen. Der Einsatz von Satelliteninternet ist auch hier zu empfehlen, allerdings muss intern darauf geachtet werden, dass die Kommunikation ausreichend gesichert ist, um eine potentielle Manipulation durch Dritte zu verhindern.

4 Fazit

4.1 Ausblick in die Zukunft

Schutz der Availability durch Publish-Subscribe

Das ”publish-subscribe” Paradigma ist ein sich zunehmend durchsetzendes Paradigma, welches ”send-receive” ablöst. Bei send-receive gibt es ein Ungleichgewicht zwischen Sender und Empfänger, welches durch publish-subscribe abgeschwächt wird. Dadurch sollte es wesentlich weniger DDoS Attacken geben. Außerdem kann die Identität, sowohl vom Sender als auch vom Empfänger, versteckt gehalten werden, da nur der Inhalt der Information wichtig ist. Weiterhin kann Multicast verwendet werden, was gerade bei Satelliten einen großen Vorteil bringen kann, da der Downlink sowieso ein Broadcast ist. Dazu kommt, dass die Verbindung unidirektionaler wird, was für Satelliten ein Vorteil ist.[8]

5G über Satellit

Es gibt Überlegungen, Satelliten zur Übertragung des 5G-Mobilfunks zu nutzen. 5G bedarf einer sehr großen Anzahl von Funkmasten, weswegen es eventuell effektiver wäre, die Abdeckung durch Satelliten zu erzeugen. Dies ist allerdings momentan eher eine theoretische Idee, da 5G eine Latenz von einer Millisekunde fordert, was nur bei niedrigsten Höhen erreichbar wäre. Außerdem müssten hierfür Endgeräte wie etwa Smartphones mit ausreichend starker Hardware ausgestattet werden, um mit einem Satelliten zu kommunizieren. Sollte es aber zu einer Umsetzung dieses Projekts kommen, würde dies das herkömmliche Internet komplett ablösen, da Endgeräte sich direkt mit Satelliten verbinden, welche dann eine direkte Verbindung zu anderen Endgeräten aufbauen würden. Dieses Netz würde für Angreifer ein sehr attraktives Ziel darstellen und müsste deswegen besonders stark gesichert werden. [1]

Einbindung von Internet und Interplanetaren Netzen

Durch die zu erwartende Ausbreitung der Menschen in unserem Sonnensystem wird es zwangsläufig ein Netzwerk geben, das dem Internet ähnelt, jedoch im gesamten Sonnensystem nutzbar ist. Das Problem ist hierbei, dass die Distanzen hier deutlich größer sind, und selbst bei Signalen mit Lichtgeschwindigkeit mit Verzögerungen im Minuten und Stundenbereich zu rechnen ist. Damit sind fast alle herkömmlich genutzten Internetprotokolle nicht anwendbar. Es müssen also für dieses Netz neue Protokolle entwickelt werden, die auch für das bestehende Internet anwendbar sind. Hierdurch entstehen neue Herausforderungen und Risiken für den Security-Bereich.[20] Die für Astronauten kurzfristig nächstliegendste Lösung ist die, die auf der ISS momentan verwendet wird. Es wird eine Remoteverbindung zu einem Computer auf der Erde hergestellt, welcher normal mit dem Internet verbunden ist. Dadurch werden Sicherheitsrisiken für die ISS minimiert und Latenzschwankungen können aufgefangen werden. [23]

4.2 Ergebnis

Die Frage, ob durch die Nutzung von Satelliten-Internet, mehr Risiken entstehen als bei der Nutzung von herkömmlichen Breitbandanschlüssen oder Drahtlosnetzen kann mit Nein beantwortet werden. Man muss sich bei der Nutzung zwar immer bewusst sein, dass alle Signale über große Flächen empfangen werden können, allerdings gilt auch bei anderen Verbindungen, dass man davon ausgehen sollte, dass dritte Parteien den Datenverkehr mitlesen können. Dies würde nicht gelten, wenn das Satellitennetz als privates Netz genutzt würde, wie etwa Amazon Kuiper für interne Dienste verwenden wird, aber es ist nicht risikobehafteter als das öffentliche Internet. Die meisten gefundenen Risiken betreffen eher den Satelliteninternet-Anbieter oder Satellitenbetreiber als den Endkunden. Die Betreiber müssen also versuchen durch geeignete Maßnahmen ihr eigenes Netz zu schützen. Die Möglichkeit, hohe Übertragungsraten mit niedriger Latenz an jedem Standort zu bekommen, ermöglicht ein Backup für jeden kritischen Internetanschluss, da die Satellitennetze unabhängig vom lokalen Netz funktionieren. Dadurch können viele herkömmliche Risiken umgangen werden. Es ist aber auch zu erwarten, dass durch die sinkenden Kosten für Operationen im Erdorbit, und durch die steigende Attraktivität in Zukunft mehr Angriffe auf Satelliten stattfinden werden. In schlimmsten Szenarien muss sogar von einem globalen Ausfall jeglicher Satellitenkommunikation gerechnet werden. Deswegen sollte, wenn möglich, sich nicht auf einen Satelliteninternetanschluss verlassen

werden. Gerade im geschäftlichen Bereich kann Satelliteninternet jedoch als Absicherung verwendet werden. Für strukturschwache Länder, in denen Breitbandanschlüsse keine Garantie sind, kann die Einführung von bezahlbarem Satelliteninternet kurzfristig große Vorteile bringen. Hier überwiegen die Vorteile vom Satelliteninternet klar den potenziellen Sicherheitsrisiken.

Literaturverzeichnis

[1] 5G-Anbieter.info: *5G über Satellit | Pläne, Möglichkeiten und Folgen.* 19.05.2021. – URL https://www.5g-anbieter.info/5g-ausbau/via-satellit.html. – Zugriffsdatum: 19.05.2021

[2] Abdalla, Samer: *Risikoanalyse drahtloser Netze am Beispiel des IEEE 802.11.* Hamburg, Universität Hamburg, Diplomarbeit, Januar 2004. – URL https://silo.tips/downloadFile/universitt-hamburg-fachbereich-informatik-vogt-klln-strae-hamburg-diplomarbeit. – Zugriffsdatum: 2.1.2021

[3] Adelsbach, Andre ; Greveler, Ulrich: *Datenschutzverletzungen bei Internetzugängen via Satellit.* – URL https://1lab.de/pub/AdGr_Dana2005.pdf. – Zugriffsdatum: 6.4.2021

[4] Amazon: *Was ist AWS Ground Station? - AWS Ground Station.* 19.05.2021. – URL https://docs.aws.amazon.com/de_de/ground-station/latest/ug/what-is-aws-ground-station.html. – Zugriffsdatum: 22.05.2021

[5] BIELAWSKI, Radosław: Space as a New Category of Threats to National Security. In: *Safety & Defense* 5 (2020), Nr. 2, S. 1–7

[6] Border, J. ; Kojo, M. ; Griner, J. ; Montenegro, G. ; Shelby, Z. ; The Internet Society (Hrsg.): *RFC 3135: Performance Enhancing Proxies Intended to Mitigate Link-Related Degradations.* 2001. – URL https://www.ietf.org/rfc/rfc3135.txt. – Zugriffsdatum: 04.04.2021

[7] Casey Handmer: *Starlink packet routing.* 2020. – URL https://caseyhandmer.wordpress.com/2020/09/23/starlink-packet-routing/. – Zugriffsdatum: 20.03.2021

[8] Cola, Tomaso de ; Ginesi, Alberto ; Giambene, Giovanni ; Polyzos, George C. ; Siris, Vasilios A. ; Fotiou, Nikos ; Thomas, Yiannis: Network and Protocol Architectures for Future Satellite Systems. In: *Foundations and Trends® in Networking* 12 (2017), Nr. 1-2, S. 1–161. – ISSN 1554-057X

[9] Del Portillo, Inigo ; Cameron, Bruce G. ; Crawley, Edward F.: A technical comparison of three low earth orbit satellite constellation systems to provide global broadband. In: *Acta Astronautica* 159 (2019), S. 123–135. – ISSN 00945765

[10] ElonX.net: *Starlink Compendium – ElonX.net*. 2019. – URL https://www.elonx.net/starlink-compendium/#satellites. – Zugriffsdatum: 24.01.2021

[11] FCC: *Technical Appendix - Application of Kuiper Systems LLC for Authority to Launch and Operate a Non-Geostationary Satellite Orbit System in Ka-band Frequencies*. 30.7.2020

[12] From Space With Love: Satelliten-Mega-Konstellationen : Alles was Sie wissen müssen und Neuigkeiten. In: *From Space With Love* (07.06.2018). – URL https://www.fromspacewithlove.com/de/satellite-mega-constellations-de/. – Zugriffsdatum: 28.02.2021

[13] Georgie Pender-Bey: *The Parkerian Hexad: The CIA Triad Model Expanded*, Lewis University, Dissertation. – URL http://cs.lewisu.edu/mathcs/msisprojects/papers/georgiependerbey.pdf. – Zugriffsdatum: 2.1.2021

[14] Hainaut, Olivier R. ; Williams, Andrew P.: *Impact of satellite constellations on astronomical observations with ESO telescopes in the visible and infrared domains*. – URL https://www.eso.org/public/archives/releases/sciencepapers/eso2004/eso2004a.pdf. – Zugriffsdatum: 23.3.2021

[15] Health and Safety: Difference Between the Safety and Security. In: *Health and Safety Blog* (23.04.2018). – URL https://www.hseblog.com/difference-between-the-safety-and-security/. – Zugriffsdatum: 04.01.2021

[16] Herbst, Jim: Prioritizing Network Traffic. In: *Summit 360* (22.08.2018). – URL https://www.summit360.com/2018/08/22/prioritizing-network-traffic/. – Zugriffsdatum: 16.05.2021

[17] Hofmann, Marc: *Die Rolle der Satellitenkommunikation beim Breitbandausbau: Informationspapier des DLR Raumfahrtmanagement*. – URL https://

www.telespazio.de/images/pdf/informationspapier_satkom.pdf. – Zugriffsdatum: 27.4.2021

[18] Iridium Satellite Communications: *Network*. 19.03.2021. – URL https://www.iridium.com/network/. – Zugriffsdatum: 19.03.2021

[19] ISO/IEC: *Safety aspects - Guidelines for their inclusion in standards*. – URL https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiKoOL-84LuAhUJ8hQKHfO3AHsQFjACegQIARAC&url=https%3A%2F%2Fwww.vde-verlag.de%2Fiec-normen%2Fdownload-kostenloses-dokument%2F220702%2F&usg=AOvVaw0fTNbTna3XCgnh4ZUUwDNW. – Zugriffsdatum: 4.1.2021

[20] Jackson, Joab: *The Interplanetary Internet: NASA researchers quarrel over how to network outer space*. 2005. – URL https://spectrum.ieee.org/telecom/internet/the-interplanetary-internet. – Zugriffsdatum: 14.04.2021

[21] Keller, Sarah: *Satellitentransport - Kosten in einem niedrigen Orbit 2016 | Statista*. 2016. – URL https://de.statista.com/statistik/daten/studie/1068964/umfrage/kosten-fuer-einen-satellitentransport-in-einem-niedrigen-orbit/. – Zugriffsdatum: 12.04.2021

[22] Knauer, Roland ; Lemm, Dennis: Sonnensturm rast zur Erde: Gefahr für Satelliten. In: *Hamburger Abendblatt* (21.01.2012). – URL https://www.abendblatt.de/ratgeber/wissen/article107721366/Sonnensturm-rast-zur-Erde-Gefahr-fuer-Satelliten.html. – Zugriffsdatum: 09.03.2021

[23] Kuksov, Igor: Internet im Weltall: von der ISS zum Mars. In: *Kaspersky* (20.11.2019). – URL https://www.kaspersky.de/blog/internet-in-space/20704/. – Zugriffsdatum: 14.04.2021

[24] Larry Press: *Amazon's Orbiting Infrastructure*. 2019. – URL https://www.circleid.com/posts/20190411_amazons_orbiting_infrastructure/. – Zugriffsdatum: 20.03.2021

[25] Manulis, M. ; Bridges, C. P. ; Harrison, R. ; Sekar, V. ; Davis, A.: Cyber security in New Space. In: *International Journal of Information Security* (2020). – ISSN 1615-5262

[26] Mattke, Sascha: SpaceX-Internet soll mobil genutzt werden – laut Musk aber nicht in Tesla-Elektroautos. In: *Teslamag.de* (09.03.2021). – URL https://teslamag.de/news/spacex-internet-mobil-nutzung-antrag-musk-wirklich-nicht-teslas-34765. – Zugriffsdatum: 21.04.2021

[27] Niklas, Cornelia: Risikoanalyse. In: *Projektmagazin* (30.10.2018). – URL https://www.projektmagazin.de/glossarterm/risikoanalyse. – Zugriffsdatum: 10.05.2021

[28] Petereit, Dieter: Starlink-Konkurrent: Amazon gibt Einblicke in Project Kuiper. In: *t3n Magazin* (17.12.2020). – URL https://t3n.de/news/starlink-amazon-project-kuiper-1345894/. – Zugriffsdatum: 22.03.2021

[29] Puhl, Pirmin ; Lundborg, Martin: *Breitbandzugang über Satellit in Deutschland: Stand der Marktentwicklung und Entwicklungsperspektiven.* Bad Honnef, Diskussionsbeitrag, Juli 2019. – URL https://www.wik.org/uploads/media/WIK_Diskussionsbeitrag_Nr_444.pdf. – Zugriffsdatum: 19.3.2021

[30] S. M. Dilek ; A. Ayranci ; A. Şeker ; O. Ceylan ; H. B. Yagci: AX.25 protocol compatible reconfigurable 2/4 FSK modulator design for nano/micro-satellites. In: *2012 20th Telecommunications Forum (TELFOR)*, 2012, S. 416–419

[31] Sağ, Emirhan ; Kavas, Aktül: Modelling and Performance Analysis of 2.5 Gbps Inter-satellite Optical Wireless Communication (IsOWC) System in LEO Constellation. In: *Journal of Communications* (2018), S. 553–558. – ISSN 23744367

[32] Sec und schneider: *media.ccc.de - Iridium Hacking: please don't sue us.* 2015. – URL https://media.ccc.de/v/camp2015-6883-iridium_hacking. – Zugriffsdatum: 29.01.2021

[33] Seth Hitefield: *GRCon16 - Exploiting Vulnerabilities in Software Radios.* 2016. – URL https://www.youtube.com/watch?v=bN4IN4EGhDg. – Zugriffsdatum: 08.03.2021

[34] SpaceX: *SpaceX Starship.* 2021. – URL https://www.spacex.com/vehicles/starship/. – Zugriffsdatum: 12.04.2021

[35] Starlink: *Starlink.* 19.03.2021. – URL https://www.starlink.com/. – Zugriffsdatum: 19.03.2021

[36] Süddeutsche Zeitung: Nasa: Indischer Satelliten-Abschuss gefährdet ISS. In: *Süddeutsche Zeitung* (02.04.2019)

[37] Sürig, Dieter: Satellitenfirma Oneweb insolvent. In: *Süddeutsche Zeitung* (29.03.2020). – URL https://www.sueddeutsche.de/wirtschaft/raumfahrt-satellitenfirma-oneweb-insolvent-1.4860854. – Zugriffsdatum: 19.03.2021

[38] T-Systems International GmbH: *So wehren sich Unternehmen gegen DDoS-Attacken.* 04.01.2021. – URL https://www.t-systems.com/de/blickwinkel/security/distributed-denial-of-service/ddos-495040. – Zugriffsdatum: 04.01.2021

[39] The Consultative Committee for Space Data Systems: *Space Data Link Security Protocol.* September 2015. – URL https://public.ccsds.org/Pubs/355x0b1.pdf. – Zugriffsdatum: 30.3.2021

[40] US Government Publishing Office: *NASA CYBERSECURITY: AN EXAMINATION OF THE AGENCY'S INFORMATION SECURITY: HEARING BEFORE THE SUBCOMMITTEE ON INVESTIGATIONS AND OVERSIGHT Committee on science, space, and technology.* 2012. – URL https://www.govinfo.gov/content/pkg/CHRG-112hhrg72919/html/CHRG-112hhrg72919.htm. – Zugriffsdatum: 08.03.2021

[41] Vicki Cox: *Northrop Grumman Successfully Completes Historic First Docking of Mission Extension Vehicle with Intelsat 901 Satellite.* 2020. – URL https://news.northropgrumman.com/news/releases/northrop-grumman-successfully-completes-historic-first-docking-of-mission-extension-vehicle-with-intelsat-901-satellite. – Zugriffsdatum: 09.03.2021

[42] Wall, Mike: Starship and Super Heavy: SpaceX's Mars-Colonizing Transportation System. In: *Space* (09.10.2019). – URL https://www.space.com/spacex-starship-super-heavy.html. – Zugriffsdatum: 12.04.2021

[43] Weidner, Markus: Einigung im Iridium-Insolvenzverfahren erzielt. In: *teltarif.de* (22.05.2008). – URL https://www.teltarif.de/arch/2008/kw21/s30032.html. – Zugriffsdatum: 19.03.2021

[44] Xin Yang: *Low Earth Orbit (LEO) Mega Constellations: Satellite and Terrestrial Integrated Communication Networks.* Guildford, Surrey, University of Surrey, Dissertation, November 2018. – URL https://core.ac.uk/download/pdf/188571367.pdf. – Zugriffsdatum: 2.1.2021

Erklärung zur selbstständigen Bearbeitung einer Abschlussarbeit

Gemäß der Allgemeinen Prüfungs- und Studienordnung ist zusammen mit der Abschlussarbeit eine schriftliche Erklärung abzugeben, in der der Studierende bestätigt, dass die Abschlussarbeit „— bei einer Gruppenarbeit die entsprechend gekennzeichneten Teile der Arbeit [(§ 18 Abs. 1 APSO-TI-BM bzw. § 21 Abs. 1 APSO-INGI)] — ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt wurden. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich zu machen."

Quelle: § 16 Abs. 5 APSO-TI-BM bzw. § 15 Abs. 6 APSO-INGI

Erklärung zur selbstständigen Bearbeitung der Arbeit

Hiermit versichere ich,

Name: [redacted]

Vorname: [redacted]

dass ich die vorliegende Bachelorarbeit – bzw. bei einer Gruppenarbeit die entsprechend gekennzeichneten Teile der Arbeit – mit dem Thema:

Risiko-Analyse bei der Nutzung von Satelliten-Internet

ohne fremde Hilfe selbständig verfasst und nur die angegebenen Quellen und Hilfsmittel benutzt habe. Wörtlich oder dem Sinn nach aus anderen Werken entnommene Stellen sind unter Angabe der Quellen kenntlich gemacht.

[redacted]	[redacted]	[redacted]
Ort	Datum	Unterschrift im Original