Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

Bundesamt für Cybersicherheit BACS
Analyse und Prävention

18. März 2025

Technologiebetrachtung

SCION

1 Einführung

Seit Mitte der 1960er Jahre hat sich aus einem ursprünglich für Forschungszwecke aufgebauten und nicht kommerziell genutzten paketvermittelten Netzwerk das Internet entwickelt, wie wir es heute als Medium für alle Arten von Kommunikation kennen. Trotz dieser Entwicklung werden im Internet immer noch die ursprünglich entwickelten Basistechnologien eingesetzt, die zwar seither weiterentwickelt aber nie grundlegend neu überdacht worden sind, um den veränderten Anforderungen an eine allgemein verfügbare und zuverlässige globale Kommunikationsinfrastruktur gerecht zu werden. Eine dieser Basistechnologien betrifft das Routing, bzw. die Art und Weise, wie in einem paketvermittelten Netzwerk Daten(pakete) von einem Sender zu einem oder mehreren Empfängern weitergeleitet werden können.

Hier kommt SCION ins Spiel. Auf der einen Seite ist SCION ein Akronym für «Scalability, Control, and Isolation On Next-Generation Networks» (dt. Skalierbarkeit, Kontrolle und Isolierung in Netzwerken der nächsten Generation). Auf der anderen Seite bedeutet der englische Begriff «scion» auch «Nachkomme» oder «Spross». In diesem Sinne steht SCION nicht nur für eine Technologie, die mehr Sicherheit, Zuverlässigkeit und Kontrolle beim Routing und damit bei der Datenübertragung im Internet verspricht, sondern auch und gerade für den Anspruch dieser Technologie, als Grundlage für eine neue Internetarchitektur zu dienen und damit gewissermassen der Nachkomme der heutigen Art und Weise zu werden, wie im Internet Datenpakete übertragen werden.

Im Rahmen dieser Technologiebetrachtung wird kurz aufgezeigt, was das Problem der heutigen Architektur ist und inwiefern SCION hier eine Lösung bieten kann. Für weitergehende Informationen wird auf [1, 2] und viele im Internet verfügbare Ressourcen verwiesen.[1]

2 Problem

Im Internet sind Routing-Protokolle für das Routing von IP-Paketen zuständig, wobei zwischen internen und externen Routing-Protokollen unterschieden werden kann. Während interne Routing-Protokolle das Routing innerhalb von autonomen Systemen (AS) leisten, die als Domänen betrachtet werden können, übernehmen externe Routing-Protokolle das Routing zwischen den Domänen. Aufgrund des exponentiellen Wachstums des Internets musste in den

[1] Viele dieser Ressourcen sind unter https://www.scion.org und https://scion-architecture.net verfügbar.

1990er-Jahren das ursprünglich eingesetzte und in RFC 823 spezifizierte Gateway-to-Gateway Protokoll (GGP) durch ein leistungsstärkeres externes Routing-Protokoll mit dem Namen Border Gateway Protokoll (BGP) ersetzt werden. Die heute immer noch im Einsatz stehende und in RFC 4271 spezifizierte Version von BGP datiert auf das Jahr 2006, auch wenn seither die Funktionalität des Protokolls in komplementären RFCs immer wieder erweitert und ergänzt worden ist.

Als externes Routing-Protokoll ist BGP auf eine möglichst effiziente Übertragung von IP-Paketen zwischen Domänen und weniger auf Sicherheit ausgelegt. Entsprechend werden immer wieder Schwachstellen und Verwundbarkeiten im BGP bekannt, die für viele Netzwerk-basierte Angriffe, wie z. B. «Distributed Denial of Service» (DDoS)- oder «BGP-Hijacking»-Angriffe, ausgenutzt werden können.[2] In beiden Fällen besteht ein ursächliches Problem darin, dass die im Rahmen von BGP ausgetauschten Daten (d. h. Inter-AS-Routinginformationen) nicht kryptografisch abgesichert sind und deshalb einfach manipuliert oder gefälscht werden können. Zudem bietet BGP keine Möglichkeit, das Routing von IP-Paketen im Weitverkehrsbereich zu beeinflussen, was sich natürlich auch negativ auf die Kontrolle der Datenübertragungspfade und damit auch auf die Souveränität bei der Datenübertragung auswirkt.

Im Hinblick auf das erste Problem gibt es seit 2017 eine Sicherheitserweiterung von BGP, die unter der Bezeichnung BGP Security (BGPsec) bekannt ist und in den RFCs 8205 bis 8209 spezifiziert ist. BGPsec bietet einen Mechanismus zur Validierung von Routen mit Hilfe von digitalen Signaturen. Damit kann sichergestellt werden, dass Routenankündigungen authentisch und von den zuständigen Domänen (AS) auch autorisiert worden sind. Allerdings braucht es für den Einsatz von BGPsec eine globale Public Key Infrastruktur (PKI), die als Ressource PKI (RPKI) aufgebaut wird. Obwohl sich auch die für das Internet zuständige U.S. amerikanische Regulierungsbehörde Federal Communications Commission (FCC) um den Aufbau der RPKI bemüht,[3] wird BGPsec – besonders während der Phase der inkrementalen Nutzung – nicht alle Routing-bezogenen Sicherheitsprobleme lösen können.

3 SCION

Aufgrund der Unzulänglichkeiten und damit verbundenen Schwachstellen und Verwundbarkeiten von BGP (und der sich damals in Entwicklung befindlichen BGPsec-Erweiterung) haben Forschende der ETH Zürich 2009 begonnen, eine Alternative zu BGP zu entwerfen, die sich nicht nur durch bessere Sicherheitseigenschaften auszeichnen soll, sondern auch durch die anderen Eigenschaften, die im Akronym SCION enthalten sind, d. h. Skalierbarkeit, Kontrolle und Isolation. Damit geht SCION über die Ansprüche von BGPsec und RPKI hinaus.

Die Architektur von SCION basiert auf sogenannten Isolationsdomänen (ISDs), in denen eine oder mehrere logisch zusammengehörige Domänen (AS) mit gemeinsamer Vertrauensbasis vereint sind. In jeder ISD muss eine Certification Authority (CA) betrieben werden, die als Beglaubigungs- und Ausgabestelle für digitale Zertifikate agiert. Neben dem Zertifikatsmanagement besteht eine weitere wesentliche Aufgabe einer ISD darin, Informationen über verfügbare Pfade bereitzustellen. Damit können Endsysteme bereits beim Versenden von Datenpaketen festlegen, auf welchen Pfaden die Pakete ausgeliefert werden sollen. Ähnlich wie beim Source Routing von IP verschieben sich damit Teile der Routing-Aufgaben von den Internet Service Providern (ISPs) auf die Endsysteme und Anwendungen einer ISD. Das ist ein eigentlicher Paradigmenwechsel, der es nicht nur erlaubt, die Datenübertragungspfade zu

---

[2] Bereits im Mai 1998 haben die Mitglieder des Hackerkollektivs L0pht Heavy Industries im Rahmen einer Anhörung im U.S. Senat vor den Risiken gewarnt, die unter anderem von den nicht vorhandenen Sicherheitsmechanismen in BGP ausgehen (https://www.youtube.com/watch?v=VVJldn_MmMY).

[3] https://docs.fcc.gov/public/attachments/DOC-402579A1.pdf

kontrollieren, sondern diese auch gemäss bestimmten Kriterien auszuwählen, wie z. B. verfügbare Bandbreiten, Latenzzeiten oder Umweltverträglichkeits- und Nachhaltigkeitskriterien, wie z. B. der CO_2-Ausstosss der eingesetzten Router. Durch die Kontrolle der Datenübertragungspfade können mehrere Pfade gleichzeitig benutzt werden, so dass ein «Multipathing» und damit ein unter Umständen schnelles Umschalten bei Ausfällen einzelner Pfade möglich wird. Der Einsatz von digitalen Signaturen erlaubt nicht nur eine Authentifizierung von Routinginformationen (wie bei BGPsec und RPKI), sondern auch eine Authentifizierung der Absenderinformationen von Datenpaketen. Damit können bestimmte «Distributed Denial of Service»- und entsprechende «Amplification»-Angriffe abgewehrt werden. Neben seinen Kernfunktionen bietet SCION auch viele Zusatzfunktionen an, wie z. B. die Anbindung an bestehende ISDs, Firewall- und Gateway-Funktionen bzw. Möglichkeiten zum Aufbau virtuell privater Netze, sowie die Möglichkeit zur Reservation von Bandbreiten. Zudem werden SCION-fähige Router entwickelt, deren Software formal verifiziert ist. Neben der ETH Zürich sind an diesen Arbeiten auch eine Spin-off-Firma[4] und industrielle Partner beteiligt, die teilweise in der SCION Association[5] zusammengeschlossen sind. Schliesslich werden die von SCION eingesetzten Protokolle in die Internet-Standardisierung eingebracht.[6] Damit werden auch Drittanbieter SCION-konforme Produkte und Dienstleistungen anbieten können.

Letztlich haben es neue Ansätze im Bereich der Netzwerktechnik immer schwer sich durchzusetzen, weil es viele gegenseitige Abhängigkeiten mit zum Teil auch unterschiedlichen Anreizsystemen gibt. So werden Netzwerkbetreiber einen Ansatz z. B. erst dann einsetzen, wenn es genügend viele Anwendungen gibt, die davon Gebrauch machen. Auf der anderen Seite werden solche Anwendungen erst entwickelt, wenn der Ansatz hinreichend breit zur Verfügung steht und auch genutzt wird. Ähnliche Abhängigkeiten gibt es zwischen allen an SCION interessierten Parteien, so dass das Ausrollen von SCION nicht einfach ist. Während man anfänglich primär mit SCION-fähigen «Overlay»-Netzwerken gearbeitet hat, werden heute SCION-Fähigkeiten direkt in den Netzwerken auf- und eingebaut. So bieten heute viele ISPs SCION-Dienste an, und in einzelnen Branchen werden ISDs als «Gated Communities» betrieben, wie z. B. das Secure Swiss Finance Network (SSFN) im Finanzbereich oder das Secure Swiss Health Network (SSHN) im Gesundheitswesen. Für den Anschluss (nicht SCION-fähiger) Endgeräte können heute zwar Gateways genutzt werden, die von verschiedenen Firmen angeboten werden, aber in Zukunft wird eine «Native»-Anbindung über das Betriebssystem oder eine dedizierte Anwendungssoftware erfolgen.[7] Dabei muss die Anbindung nicht exklusiv sein, sondern kann auch mit einer Anbindung an «konventionelle» BGP-basierte IPv4- oder IPv6-Netzwerke komplementär erfolgen, um z. B. eine möglichst grosse Verfügbarkeit zu erreichen.

4 Schlussfolgerungen und Ausblick

Aus technologischer Sicht bietet SCION grosse Vorteile gegenüber BGP und seinen sicherheitstechnischen Erweiterungen (d. h. BGPsec und RPKI). Diese Vorteile betreffen nicht nur die Sicherheit im engen Sinne, sondern auch die Verfügbarkeit, Zuverlässigkeit, Kontrolle und Souveränität. Vor dem Hintergrund der sich laufend verschärfenden geopolitischen und/oder wirtschaftlichen Konflikte sind gerade Technologien wichtig, die die Souveränität eines Landes verbessern können. Mit dem Einsatz von ISDs können die Vertrauensverhältnisse so gestaltet werden, wie sie lokal sinnvoll sind; auf den Einsatz von globalen Vertrauensstrukturen (wie z.

[4] Anapaya Systems (https://www.anapaya.net)
[5] https://www.scion.org
[6] Die zuständige Forschungsgruppe heisst Path Aware Networking Research Group (PANRG) und ist mit ihren Dokumenten im Internet unter https://datatracker.ietf.org/rg/panrg/ verfügbar.
[7] Diese Möglichkeit wird zurzeit im Rahmen des SCION Education, Research, and Academic (SCIERA) Netzwerks mit einer Viertelmillion Benutzern ausgetestet.

B. Web-PKI) kann verzichtet werden. Schliesslich ist aus Versuchen und Messungen bekannt, dass eine SCION-Anbindung nicht nur aus der Sicht der Sicherheit sinnvoll ist, sondern auch aus der Sicht der Performanz. Das ist insofern überraschend positiv, weil Sicherheitsvorteile sonst normalerweise mit Performanzeinbussen einher gehen.

Auf der anderen Seite gibt es bei SCION auch Nachteile zu vermerken. So hat jede neue Technologie mit der Schwierigkeit zu kämpfen, dass das Fachwissen dazu (noch) nicht flächendeckend vorhanden ist, und dass dieses Fachwissen zuerst aufgebaut werden muss. Je mehr die Technologie zum Standard wird und in den Produkten verbaut ist, umso mehr wird sich dieses Problem entschärfen. Insofern ist SCION mit seinen Aktivitäten (z. B. in den Bereichen «Community Building» und Standardisierung) auf dem richtigen Weg. Zudem kann jede Sicherheitstechnologie die Hoffnung wecken, dass damit alle Sicherheitsprobleme gelöst werden können. Natürlich ist das auch bei SCION nicht der Fall. Auch wenn damit viele (netzwerkbasierte) Angriffe mitigiert werden können, bleiben Angriffsmöglichkeiten übrig (typischerweise auf höheren Schichten im Protokollstack). Man denke hier an Angriffe gegen Web-Anwendungen, wie z. B. «SQL Injection»- oder «Cross-Site Scripting»-Angriffe, schwache Authentifikationsverfahren, datengetriebene Angriffe, wie z. B. mit Malware infizierte Excel-Dateien, oder auch andere Formen von «Phishing»- und «Social Engineering»-Angriffe. Obwohl SCION hier eine gewisse Milderung verspricht, weil z. B. Routinginformationen authentifiziert und Angriffe über beliebige IP-Adressen erschwert werden, können nicht alle Angriffe abgewehrt werden. Entsprechend wird SCION mit anderen Sicherheitstechnologien, -mechanismen und -diensten ergänzt werden müssen, um einen adäquaten Schutz zu erreichen.

Abkürzungen

AS	Autonomes System
BGP	Border Gateway Protokoll
BGPsec	BGP Security
CA	Certification Authority
DNS	Domain Name System
DNSSEC	DNS Security
ETH	Eidgenössische Technische Hochschule
FCC	Federal Communications Commission
GGP	Gateway-to-Gateway Protokoll
IETF	Internet Engineering Task Force
ISD	Isolationsdomäne
ISP	Internet Service Provider
PANRG	Path Aware Networking Research Group
PKI	Public Key Infrastruktur
RFC	Request for Comments
RPKI	Resource PKI
SCIERA	SCION Education, Research, and Academic
SCION	Scalability, Control, and Isolation On Next-Generation Networks
SSHN	Secure Swiss Health Network
SSFN	Secure Swiss Finance Network

Referenzen

[1] Adrian Perrig, et al., SCION: A Secure Internet Architecture, Springer, 2017
[2] Laurent Chuat, et al., The Complete Guide to SCION: From Design Principles to Formal Verification, Springer, 2022