Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Département fédéral de la défense,
de la protection de la population et des sports DDPS

Office fédéral de la cybersécurité OFCS
Analyse et prévention

18 mars 2025

Considérations technologiques

SCION

1 Introduction

Depuis le milieu des années 1960, l'internet a évolué : réseau à commutation par paquets utilisé à des fins scientifiques et non commerciales à l'origine, il est progressivement devenu l'outil de communication par excellence que l'on connaît aujourd'hui. Malgré cette évolution, on recourt toujours aux mêmes mécanismes de base sur Internet. Ils ont certes été perfectionnés, mais ils n'ont jamais été repensés en profondeur pour répondre aux nouvelles exigences, c'est-à-dire une infrastructure de communication mondiale, fiable et accessible à tout le monde. Le routage est l'un de ces mécanismes. Il consiste à sélectionner, au sein d'un réseau, les chemins par lesquels les paquets de données d'un expéditeur seront transmis à un ou plusieurs destinataires.

C'est là qu'intervient SCION. Acronyme de *Scalability*, *Control* et *Isolation On Next-Generation Networks* (extensibilité, contrôle et isolation sur des réseaux de nouvelle génération), ce terme anglais signifie aussi « jeune pousse » ou « successeur ». En effet, cette technologie promet non seulement davantage de sécurité, de fiabilité et de contrôle lors du routage et, donc, lors de la transmission de données sur internet, mais elle concrétise aussi une ambition, celle de servir de base à une nouvelle architecture internet et d'être, en quelque sorte, le successeur de la méthode actuelle pour transmettre des paquets de données.

Dans les considérations technologiques d'aujourd'hui, nous abordons le problème de l'architecture actuelle et montrons dans quelle mesure SCION peut constituer une solution. Les ouvrages cités en référence et les nombreuses sources internet disponibles fournissent de plus amples informations à ce sujet[1].

2 Problème

Sur internet, les protocoles de routage s'appliquent aux paquets IP. Une distinction peut être opérée entre protocoles de routage internes et protocoles de routage externes. Dans le premier cas, il s'agit d'un routage au sein de systèmes autonomes (SA) que l'on peut considérer comme des domaines, tandis que, dans le deuxième, il s'agit d'un routage entre domaines.

[1] Bon nombre de ces sources sont disponibles sur les sites https://www.scion.org et https://scion-architecture.net.

En raison de l'expansion d'internet, il a fallu remplacer, dans les années 1990, le protocole de base en vigueur, à savoir le GGP (détaillé dans le RFC 823), par un protocole de routage externe plus performant appelé BGP. Le BGP que l'on utilise encore de nos jours (RFC 4271) date de 2006, même si, depuis, des spécifications pour ce protocole ont été régulièrement ajoutées ou élargies dans des RFC complémentaires.

En tant que protocole de routage externe, le BGP est conçu pour transmettre aussi efficacement que possible des paquets IP entre les domaines, mais il est moins axé sur la sécurité. Par conséquent, des failles et des vulnérabilités sont régulièrement observées. Elles peuvent être exploitées pour lancer de nombreuses attaques contre le réseau. Il peut s'agir par exemple d'une attaque par déni de service ou d'un détournement de BGP[2]. Dans les deux cas, le problème vient du fait que les données échangées lors du BGP (échange d'informations de routage entre SA) ne sont pas cryptées. Elles peuvent donc être facilement manipulées ou falsifiées. En outre, le BGP n'offre pas la possibilité d'influer sur le routage de paquets IP dans un réseau étendu, ce qui a bien sûr des répercussions négatives sur le contrôle des chemins de transmission et sur la souveraineté des données.

Pour revenir au problème de sécurité du BGP, il existe depuis 2017 une extension connue sous le nom de BGPsec et détaillée dans les RFC 8205 à 8209. Elle permet de vérifier l'intégrité d'un chemin à l'aide de signatures numériques, garantissant ainsi que les annonces de routes sont authentiques et qu'elles ont été aussi autorisées par les domaines compétents (SA). Pour utiliser l'extension BGPsec, il faut toutefois une infrastructure à clés publiques globale, développée en tant qu'infrastructure à clés publiques de ressources (RPKI). Bien que la FCC, autorité de régulation américaine responsable d'internet, s'efforce de développer la RPKI[3], l'extension BGPsec ne peut pas résoudre tous les problèmes de sécurité liés au routage, en particulier durant le processus incrémental.

3 SCION

En 2009, en raison des points faibles du BGP (et de l'extension BGPsec, en cours de développement à ce moment-là), l'EPFZ a commencé à élaborer une solution alternative : le but n'était pas seulement d'améliorer les mécanismes de sécurité, mais aussi d'intégrer les autres propriétés contenues dans l'acronyme SCION, c'est-à-dire l'extensibilité, le contrôle et l'isolation. SCION va donc au-delà des exigences fixées pour l'extension BGPsec et la RPKI.

L'architecture de SCION repose sur ce qu'on appelle des ISD, utilisés pour regrouper de façon logique un ou plusieurs SA et créer un espace de confiance commun. Dans chaque ISD, il faut une autorité qui délivre et authentifie des certificats numériques. Outre la gestion des certifications, une autre tâche essentielle consiste à fournir des informations sur les chemins disponibles. Ainsi, dès l'envoi de paquets de données, les systèmes d'extrémité (*end systems*) peuvent déterminer les chemins à emprunter. À l'instar du routage à la source (*source routing*) des IP, une partie des tâches de routage passe des fournisseurs d'accès à internet (FAI) aux systèmes d'extrémité et aux applications d'un ISD. Il s'agit d'un vrai changement de paradigme qui ne permet pas seulement de contrôler les chemins de transmission des données, mais aussi de les choisir en fonction de critères précis tels que la disponibilité des bandes passantes, la latence, la compatibilité environnementale ou encore la durabilité (p. ex. émissions de CO_2 des routeurs utilisés).

---

[2] Déjà en mai 1998, lors d'une audience devant le Sénat, le groupe de hackers L0pht Heavy Industries a alerté l'État américain sur les risques liés, entre autres, à l'absence de mécanismes de sécurité pour le BGP (https://www.youtube.com/watch?v=VVJldn_MmMY).

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

En contrôlant les chemins de transmission des données, il est possible d'utiliser plusieurs chemins simultanément (*multipathing*) de manière à pouvoir changer rapidement de chemins si certains sont défaillants.

Les signatures numériques sont utilisées pour authentifier des informations de routage (comme pour l'extension BGPsec et la RPKI) et des informations sur l'expéditeur de paquets de données, permettant ainsi de repousser certaines attaques (attaques par déni de service et attaques par amplification). En plus de ses fonctions principales, SCION offre de nombreuses autres possibilités telles que la connexion à des ISD existants, des dispositifs de pare-feu et de passerelle (*gateway*), la création de réseaux privés virtuels et la réservation de bandes passantes. Des routeurs compatibles avec SCION et dont le logiciel est formellement vérifié sont aussi développés. Outre l'EPFZ, une entreprise issue d'une scission[4] et des partenaires, dont certains sont membres de la SCION Association[5], travaillent également sur le sujet. Les protocoles SCION seront intégrés dans la normalisation d'internet[6]. Ainsi, des tiers seront également en mesure de proposer des produits et des services conformes à SCION.

En définitive, les nouvelles approches dans le domaine des réseaux ont toujours de la peine à s'imposer, car il y a de nombreuses interdépendances avec, parfois, des systèmes d'incitation différents. D'un côté, les opérateurs de réseau ne vont privilégier une approche que s'il y a suffisamment d'applications qui sont utilisées. De l'autre, ces applications ne seront développées que si l'approche est suffisamment répandue. Les parties prenantes de SCION font face au même problème, ce qui complique le déploiement de cette architecture internet. Alors que l'idée initiale était de travailler surtout avec des réseaux superposés compatibles avec SCION, on intègre aujourd'hui directement les capacités de SCION aux réseaux. Ainsi, de nombreux FAI offrent des services SCION. Dans certains secteurs, les ISD sont utilisés comme des réseaux fermés, par exemple le SSFN dans le domaine de la finance ou le SSHN dans le domaine de la santé. Pour connecter des terminaux incompatibles avec SCION, il existe à l'heure actuelle la possibilité de recourir aux passerelles proposées par différentes entreprises. Mais à l'avenir, une connexion « native » sera établie via le système d'exploitation ou via une application dédiée[7]. Pour ce faire, il faut que la connexion ne soit pas exclusive : elle doit être complémentaire à une connexion aux réseaux « classiques » IPv4 ou IPv6, basés sur le BGP, par exemple pour avoir une disponibilité maximale.

4 Conclusions et perspectives

D'un point de vue technologique, SCION présente de gros avantages par rapport au BGP et à ses solutions pour améliorer la sécurité (BGPsec et RPKI). Ses atouts ne résident pas seulement dans la sécurité au sens strict, mais aussi dans la disponibilité, la fiabilité, le contrôle et la souveraineté. Dans un contexte où les tensions géopolitiques et économiques ne cessent de monter, les technologies importantes sont justement celles qui permettent d'améliorer la souveraineté d'un pays. En utilisant des ISD, il est possible de créer un climat de confiance à l'échelle local et de renoncer aux structures globales (p. ex. web PKI). Les tests et les mesures ont finalement révélé qu'une connexion SCION est judicieuse au regard de la sécurité et de la performance. C'est d'autant plus une bonne surprise que les gains de sécurité vont normalement de pair avec des baisses de performance.

---

[4] Anapaya Systems (https://www.anapaya.net)
[5] https://www.scion.org
[6] Le groupe de recherche s'appelle PANRG. Ses documents sont disponibles à l'adresse https://datatracker.ietf.org/rg/panrg/.
[7] Cette option est actuellement testée dans le cadre du réseau SCIERA. 250 000 utilisateurs participent au test.

L'architecture de réseau SCION présente toutefois aussi des inconvénients. Comme toute nouvelle technologie, elle se heurte à une difficulté : les connaissances sont encore fragmentaires. Il faut donc d'abord développer un savoir. Plus une technologie se normalise et s'intègre à des produits, plus ce problème s'atténue. Sur ce point, SCION est sur la bonne voie (p. ex. avec ses activités dans les domaines du *community building* et de la normalisation). Toute nouvelle technologie sécuritaire peut en outre faire naître l'espoir que tous les problèmes de sécurité vont être résolus, ce qui n'est bien sûr pas le cas, y compris pour SCION. En effet, même si cette architecture permet de réduire un grand nombre d'attaques réseau, celles-ci restent toujours possibles (en général sur les couches supérieures dans la pile de protocoles). On pense ici à des attaques contre des applications web : injection SQL ou *cross-site scripting*, exploitation d'un processus d'authentification faible, logiciel malveillant (pouvant par exemple infecter des fichiers Excel) ou toute forme d'hameçonnage et d'ingénierie sociale. Bien que SCION se veuille assez rassurant sur ce point, par exemple en authentifiant les informations de routage et en rendant les attaques sur n'importe quelle adresse IP plus difficiles, toutes les attaques ne peuvent pas être repoussées. Il faut donc compléter l'architecture SCION avec d'autres technologies, mécanismes ou services de sécurité pour atteindre un niveau de protection adéquat.

Abréviations

BGP	*Border Gateway Protocol*
BGPsec	BGP *Security*
EPFZ	École polytechnique fédérale de Zurich
FAI	Fournisseur d'accès à internet
FCC	Federal Communications Commission
GGP	*Gateway-to-Gateway Protocol*
ISD	*Isolation domain*
PANRG	Path Aware Networking Research Group
RFC	*Request for Comments*
RPKI	*Resource Public Key Infrastructure*
SA	Système autonome
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*

Références

[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