Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa, della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS
Analisi e prevenzione

18 marzo 2025

Valutazione tecnologica

SCION

1 Introduzione

A partire dalla metà degli anni Sessanta una rete a commutazione di pacchetto originariamente concepita per scopi scientifici e non commerciali si è evoluta fino a diventare il mezzo che conosciamo oggi per tutti i tipi di comunicazione: Internet. Nonostante questa evoluzione, Internet utilizza ancora oggi le tecnologie di base sviluppate in origine, che hanno conosciuto perfezionamenti ma mai ripensamenti radicali per soddisfare le mutate esigenze di un'infrastruttura di comunicazione globale caratterizzata da una generale disponibilità e affidabilità. Tra queste tecnologie di base rientra il routing, ovvero la modalità con cui i dati (pacchetti) possono essere trasmessi da un mittente a uno o più destinatari all'interno di una rete a commutazione di pacchetto.

È qui che entra in gioco SCION. SCION è l'acronimo di «Scalability, Control, and Isolation On Next-Generation Networks» (ovvero scalabilità, controllo e isolamento in reti di prossima generazione). Al contempo, in inglese il termine «scion» significa «discendente» o «germoglio». SCION non rappresenta solo una tecnologia che promette maggiore sicurezza, affidabilità e controllo a livello di routing e quindi di trasmissione di dati, ma ha anche l'ambizione di fungere da base per una nuova architettura di Internet, diventando in un certo senso l'erede dell'attuale modalità di trasmissione di pacchetti su Internet.

La presente valutazione tecnologica intende illustrare brevemente il problema dell'architettura odierna e la misura in cui SCION può offrire una soluzione. Per ulteriori informazioni si rimanda a [1, 2] nonché a numerose risorse disponibili su Internet.[1]

2 Problema

I protocolli di routing in Internet sono responsabili dell'instradamento (routing) dei pacchetti IP, con una distinzione tra protocolli di routing interni ed esterni. Mentre i primi eseguono l'instradamento all'interno di sistemi autonomi (AS, autonomous system) assimilabili a domini, i secondi effettuano quest'operazione tra i domini. A causa della crescita esponenziale di Internet, negli anni Novanta è stato necessario sostituire il protocollo Gateway-to-Gateway (GGP) impiegato inizialmente, specificato nella RFC 823, con un protocollo di routing esterno più potente denominato Border Gateway Protokoll (BGP). La versione di BGP ancora in uso oggi e

[1] Molte di queste risorse sono disponibili su https://www.scion.org e https://scion-architecture.net.

specificata nella RFC 427 risale al 2006, sebbene da allora la funzionalità del protocollo sia stata ampliata e integrata costantemente in RFC complementari.

In quanto protocollo di routing esterno, BGP è pensato per la trasmissione quanto più efficiente di pacchetti IP tra domini e meno per la sicurezza. Di conseguenza in BGP emergono continuamente criticità e vulnerabilità che possono essere sfruttate in molti attacchi di rete, come ad esempio il «distributed denial of service» (DDoS) o il «BGP hijacking».[2] In entrambi i casi vi è un problema a monte, legato al fatto che i dati trasmessi nel quadro di BGP (ovvero informazioni di routing tra sistemi autonomi) non sono crittografati e sono quindi vulnerabili a manipolazioni e falsificazioni. Inoltre il BGP non offre nessuna possibilità di influire sul routing di pacchetti IP nella rete geografica (wide area network), un aspetto che si riflette negativamente anche sul controllo dei percorsi di trasmissione dei dati e quindi sulla relativa sovranità.

Per ovviare al primo problema nel 2017 è stata rilasciata un'estensione di sicurezza per BGP, nota come BGP Security (BGPsec) e specificata nelle RFC da 8205 a 8209. BGPsec offre un meccanismo per la validazione degli instradamenti avvalendosi di firme digitali. Questa accortezza permette di garantire l'autenticità degli annunci di route e la loro autorizzazione da parte dei domini competenti (AS). Tuttavia, per poter essere usato, BGPsec richiede un'infrastruttura a chiave pubblica (PKI, public key infrastructure) impostata come Resource PKI (RPKI). Sebbene anche la Federal Communications Commission (FCC), l'autorità di regolamentazione statunitense responsabile di Internet, si stia impegnando per sviluppare la RPKI[3], BGPsec non sarà in grado di risolvere tutti i problemi di sicurezza relativi al routing, soprattutto durante la fase di utilizzo incrementale.

3 SCION

Le carenze nonché le relative criticità e vulnerabilità di BGP (e dell'estensione BGPsec, allora in fase di sviluppo) hanno spinto i ricercatori del Politecnico federale di Zurigo a sviluppare, a partire dal 2009, un'alternativa a BGP che si distinguesse non solo per una maggiore sicurezza ma anche per le altre caratteristiche a cui rimanda l'acronimo SCION, ovvero scalabilità, controllo e isolamento. SCION va quindi oltre i requisiti di BGPsec e di RPKI.

L'architettura di SCION si fonda sui cosiddetti domini di isolamento (ISD, isolated domain), in cui sono riuniti uno o più domini logicamente correlati (AS) che condividono una base fiduciaria comune. Ciascun ISD deve disporre di un'autorità di certificazione (CA, certification authority) che funge da organo di autenticazione e di emissione di certificati digitali. Oltre a gestire certificati un ISD svolge un ulteriore compito importante: fornire informazioni sui percorsi disponibili. In questo modo i sistemi finali sono in grado di stabilire su quali percorsi occorre trasmettere i pacchetti di dati già al momento dell'invio. Analogamente al source routing dell'IP, alcuni dei compiti di instradamento vengono così trasferiti dai provider di servizi Internet (ISP, internet service provider) ai sistemi finali e alle applicazioni di un ISD. Si tratta di un vero e proprio cambiamento di paradigma che permette non solo di controllare i percorsi di trasmissione dei dati, ma anche di selezionarli secondo determinati criteri quali le larghezze di banda disponibili, i tempi di latenza o parametri di compatibilità ambientale e di sostenibilità come ad esempio le emissioni di CO_2 del router impiegato. Il controllo dei percorsi di trasmissione dei dati permette di utilizzare più percorsi contemporaneamente, consentendo il cosiddetto «multipathing» e quindi, in determinate circostanze, una rapida commutazione in caso di guasti ai singoli percorsi. L'impiego di firme digitali permette di autenticare non solo le informazioni di

[2] Già in occasione di un'audizione presso il Senato degli Stati Uniti nel maggio del 1998 i membri del collettivo di hacker L0pht Heavy Industries avevano messo in guardia dai pericoli derivanti tra l'altro dall'assenza di meccanismi di sicurezza in BGP (https://www.youtube.com/watch?v=VVJldn_MmMY).

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

routing (come nel caso di BGPsec e RPKI), ma anche quelle sul mittente dei pacchetti di dati, consentendo così di difendersi da attacchi DDoS e da relativi attacchi di amplificazione (amplification attack). Oltre alle funzioni principali, SCION offre anche numerosi servizi aggiuntivi, tra cui la connessione a ISD esistenti, funzioni di firewall e gateaway, possibilità di creare reti virtuali private e di riservare larghezze di bande. Sono inoltre in fase i sviluppo router compatibili con SCION con software verificato formalmente. Oltre al Politecnico federale di Zurigo, a questo progetto partecipano anche un'azienda spin-off[4] e partner industriali, alcuni dei quali membri della SCION Association[5]. Da ultimo i protocolli impiegati da SCION saranno incorporati nella standardizzazione di Internet.[6] Così anche i fornitori di terze parti potranno offrire prodotti e prestazioni compatibili con SCION.

In ultima analisi i nuovi approcci nel campo delle tecnologie di rete faticano a imporsi poiché esistono numerose interdipendenze in parte anche con sistemi di incentivi diversi. Ad esempio, da una parte gli operatori di rete potrebbero voler implementare un approccio solo in presenza di un numero sufficiente di applicazioni che ne fanno uso. Dall'altra parte, simili applicazioni vengono sviluppate solo se l'approccio in questione è sufficientemente diffuso e imposto nell'utilizzo. Simili dipendenze esistono tra tutte le parti coinvolte in SCION, complicandone il roll out. Mentre all'inizio si utilizzavano soprattutto reti «overlay» compatibili con SCION, oggi le capacità di SCION sono integrate direttamente nelle reti. Oggi molti ISP offrono servizi SCION, e in alcuni settori gli ISD operano come «gated community», come ad esempio il Secure Swiss Finance Network (SSFN) in ambito finanziario o il Secure Swiss Health Network (SSHN) in campo sanitario. Attualmente per collegare apparecchi terminali (non compatibili con SCION) possono essere utilizzati gateway offerti da varie aziende, mentre in futuro verrà stabilita una connessione «nativa» attraverso il sistema operativo o un software applicativo dedicato.[7] La connessione non deve necessariamente avere natura esclusiva, bensì può condividere l'allacciamento a reti IPv4 o IPv6 «convenzionali» basate su BGP, al fine ad esempio di massimizzare la disponibilità.

4 Conclusioni e prospettive future

Sotto il profilo tecnologico SCION offre notevoli vantaggi rispetto a BGP e alle successive estensioni di sicurezza (BGPsec e RPKI), che non si traducono solo in maggiore sicurezza in senso stretto, ma anche in termini di disponibilità, affidabilità, controllo e sovranità. In un contesto caratterizzato dal continuo inasprimento di conflitti geopolitici e/o economici, le tecnologie in grado di consolidare la sovranità di un Paese sono particolarmente importanti. Con l'impiego di ISD è possibile strutturare le relazioni di trust nel modo più utile a livello locale; rinunciando invece all'impiego di strutture di fiducia globali (come ad esempio Web-PKI). Infine i collaudi e le misurazioni dimostrano che l'allacciamento SCION è utile non solo sotto il profilo della sicurezza, ma anche della performance. Si tratta di una sorpresa positiva, poiché i vantaggi in termini di sicurezza sono spesso accompagnati da cali di prestazioni.

SCION presenta tuttavia anche degli svantaggi. Ogni nuova tecnologia deve fare i conti con la temporanea carenza capillare di conoscenze tecniche, che impiegano tempo per maturare. Questo problema si attenuerà con la graduale standardizzazione della tecnologia e la sua integrazione nei prodotti. In tal senso SCION, con le sue attività (per esempio negli ambiti di «community building» e standardizzazione), sta andando nella giusta direzione. Qualsiasi

[4] Anapaya Systems (https://www.anapaya.net)
[5] https://www.scion.org
[6] Il gruppo di ricerca competente si chiama Path Aware Networking Research Group (PANRG). I relativi documenti sono disponibili su https://datatracker.ietf.org/rg/panrg/.
[7] Questa possibilità viene attualmente testata da circa 250 mila utenti nel quadro della rete SCION Education, Research, and Academic (SCIERA).

tecnologia di sicurezza è accompagnata dalla speranza di poter risolvere tutti i problemi di sicurezza. Inutile dire che questo auspicio è mal riposto anche nel caso di SCION: anche se consente di mitigare molti attacchi (basati sulla rete), non può del tutto escludere la loro eventualità (in particolare a livelli più alti dello stack di protocollo). Si pensi ad attacchi contro applicazioni web quali «SQL injection» o «cross-site scripting», a procedure di autenticazione deboli, ad attacchi basati sui dati, come per esempio file Excel infettati da malware, o ad altre forme di attacchi di «phishing» e «social engineering». Sebbene SCION ne prometta una discreta mitigazione, anche grazie all'autenticazione delle informazioni di routing e al contrasto degli attacchi tramite indirizzi IP arbitrari, respingere tutti i possibili attacchi rimane una chimera. Pertanto è necessario dotare SCION di ulteriori tecnologie, meccanismi e servizi di sicurezza al fine di raggiungere un'adeguata protezione.

Abbreviazioni

AS	Autonomes System
BGP	Border Gateway Protokoll
BGPsec	BGP Security
CA	Certification Authority
DNS	Domain Name System
DNSSEC	DNS Security
PF	Politecnico federale
FCC	Federal Communications Commission
GGP	Gateway-to-Gateway Protokoll
IETF	Internet Engineering Task Force
ISD	Isolated Domain
ISP	Internet Service Provider
PANRG	Path Aware Networking Research Group
PKI	Public Key Infrastructure
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

Fonti bibliografiche

[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