Die Neuerfindung des Internets

Forscher der ETH Zürich haben eine alternative Internet-Architektur entwickelt. Sie verspricht nicht nur eine Verbesserung der Sicherheit, sondern soll auch die Verfügbarkeit erhöhen. VON STEFAN BETSCHON

«Beschäftige dich nicht mit Informationssicherheit», bekam Adrian Perrig am Anfang seiner wissenschaftlichen Karriere zu hören. Perrig ist heute Professor an der ETH Zürich, wo er die Network Security Group leitet. Sein Informatikstudium begann er an der ETH Lausanne; ein Zufall hatte ihn in die Westschweiz verschlagen, eigentlich hatte er vorgehabt, sich an der ETH Zürich einzuschreiben. «Beschäftige dich nicht mit Informationssicherheit», so habe ihm ein Mentor geraten. Die mathematischen Grundlagen der Informationssicherheit waren gut erforscht, es schien damals, als ob es hier für einen jungen Wissenschafter nichts mehr zu holen gäbe. Doch Perrig hörte nicht auf den Rat des älteren Wissenschafters. Nach dem Ingenieurdiplom in der Schweiz setzte er seine computerwissenschaftlichen Studien in den USA fort, um sich an der Carnegie Mellon University und an der UC Berkeley vertieft mit Sicherheitsfragen zu beschäftigen. Und jetzt ist Perrig nicht nur als Forscher und Universitätsdozent, sondern auch als Berater, Interviewpartner und Vortragsredner überaus gefragt: Alle wollen von ihm wissen, wie man das Internet sicherer machen kann.

Im Internet der Zukunft sollen sich Datenströme präziser steuern lassen. SIMON TANNER / NZZ

Ein Netz der Netze der Netze

Es vergeht kaum eine Woche, ohne dass nicht eine grössere Sicherheitslücke weltweit für Schlagzeilen sorgt. Mitte Juni wies das Computer Emergency Readiness Team der USA (US-CERT) warnend darauf hin, dass Nordkorea ein Botnet in Stellung gebracht habe, um mit Überlastungsangriffen amerikanische Banken, Medienunternehmen und Rüstungsbetriebe zu schädigen. Wenige Tage zuvor hatten amerikanische Zeitungen über eine Malware russischer Provenienz berichtet, die in der Lage sein soll, die Stromversorgung lahmzulegen.

Als die technischen Grundlagen des Internets in den 1970er Jahren ausgearbeitet wurden, ging es darum, ein paar computerwissenschaftliche Forschungsinstitute amerikanischer Eliteuniversitäten miteinander zu verbinden. Niemand dachte an ein globales Netz, niemand beschäftigte sich mit Sicherheitsfragen. Heute verbindet das Internet rund um die Welt Milliarden von Computern, gibt es kaum eine gesellschaftliche Aktivität, die nicht vom Internet abhängig wäre.

Schon oft ertönte in jüngster Zeit der Ruf, das Internet grundlegend zu überarbeiten, den Neustartknopf zu drücken, ein «Internet 2.0» zu schaffen. Die EU etwa gab zwischen 2007 und 2013 mehrere Milliarden Euro aus, um europäische Wissenschafter bei der Neuerfindung des Internets zu unterstützen.

Ein Netz der Netze der Netze

Wie kann man das Internet sicherer machen? Wie kann es gelingen, diese komplexe Maschinerie im laufenden Betrieb zu revidieren? Adrian Perrig glaubt zu wissen, wie sich das bewerkstelligen lässt. Er möchte nicht nur das eine oder andere Rädchen neu schmieren, dieses eine oder dieses andere Übertragungsprotokoll kryptologisch ein bisschen aufpolieren – er möchte in das innerste Getriebe dieser Maschine eingreifen und ihre Funktionsweise grundlegend verändern; er möchte eine neue Internet-Architektur etablieren. Diese Architektur wird Scion genannt, ein Akronym: «Scalability, Control, and Isolation On Next-Generation Networks».

Ein zentrales Element der neuen Architektur ist Isolation.

Ein zentrales Element der neuen Architektur ist Isolation. Dem Prinzip «Teile und herrsche» folgend, sollen sich Sicherheitsprobleme bewältigen lassen, indem das Internet in sogenannte Isolation-Domains zerlegt wird. Das Internet wird auch «Netz der Netze» genannt, es verbindet viele eigenständige Netzwerke, sogenannte autonome Systeme. Bei Scion verwandelt sich das Internet in ein Netz der Netze der Netze. Mehrere Netze – autonome Systeme – bilden zusammen eine Isolation-Domain, und viele Isolation-Domains bilden zusammen das Internet. Ein autonomes System kann Teil von mehreren Isolation-Domains sein. Die Grenzen von Isolation-Domains könnten sich mit denen von Rechtsräumen oder politischen Einheiten decken, so dass es für eine Gruppe von autonomen Systemen juristische oder politische Anreize gibt, näher zusammenzurücken, sich gegen andere Isolation-Domains abzugrenzen. Gefährdet die Bildung von Isolation-Domains nicht das «offene Internet», wird dadurch nicht einer Balkanisierung Vorschub geleistet? Nein: Die Grenzen einer Isolation-Domain sollen die Verwaltung von Datenflüssen erleichtern, ohne die Kommunikation zu behindern.

Bei einem herkömmlichen Telefonnetz sitzt die Intelligenz im Zentrum des Netzes, in der Telefonzentrale. Fällt die Zentrale aus, ist das gesamte Netzwerk futsch. Im Internet gibt es kein Zentrum und keine Zentrale. Die Intelligenz, die es braucht, um Datenpakete von einem Sender zu einem Empfänger zu leiten, befindet sich, über das ganze Netzwerk verteilt, in Millionen von kleinen «Telefonzentralen», die Router genannt werden. Die Router wissen aufgrund von Routing-Tabellen im Hauptspeicher, was sie tun müssen, um ein Datenpaket auf seiner Reise ein Stück weiterzubringen. Weil sich das Netzwerk dauernd ändert, müssen die Routing-Tabellen laufend nachgeführt werden. Für den Austausch dieser Informationen ist das Border-Gateway-Protokoll zuständig. Die Datenmengen, die über diesen Mechanismus ausgetauscht werden, nehmen mit dem Wachstum des Internets rasch zu, viele Router arbeiten an der Grenze zur Überforderung.

Das Border Gateway Protocol (BGP) ist auch als «Two-Napkin Protocol» bekannt. Es wurde 1989 von zwei Netzwerkspezialisten – der eine arbeitete für Cisco, der andere für IBM – während eines Mittagessens auf zwei Papierservietten skizziert. Die beiden Papierservietten sind im Computer History Museum in Mountain View aufbewahrt. Man wünschte sich, die beiden Ingenieure hätten sich mehr Zeit genommen für das Mittagessen und hätten einen grösseren Vorrat an Servietten zur Verfügung gehabt. Denn BGP ist nicht nur ineffizient, sondern auch unsicher.

Bei Scion wird die Intelligenz an den Rand des Netzwerks verlagert. Die Informationen über die Struktur des Internets, die verstreut in den Hauptspeichern vieler Router abgelegt sind, werden nun in der Nähe des Senders oder Empfängers konzentriert. Im Rahmen eines Prozesses, der Beaconing genannt wird, besorgen sich die Isolation-Domains Informationen über die Struktur des Netzwerks. Dank diesen Informationen hat ein Sender nun die Möglichkeit, den Pfad, auf dem ein Datenpaket durch das Internet transportiert wird, vorzugeben. Er hat also die Möglichkeit, etwa einen Pfad zu wählen, der kurz und schnell ist, oder einen anderen, der unerwünschtes Territorium vermeidet. Die Vorgaben für die Reiseroute werden innerhalb des Datenpakets gespeichert. Am Ziel kann überprüft werden, ob das Paket tatsächlich dem vorgegebenen Weg gefolgt ist. Die auf den Beaconing-Servern gespeicherte Routing-Informationen sind auch beim Empfang von Daten nützlich: Sie können die Kommunikation auf bestimmte Zugänge einschränken; so lassen sich Überlastungsangriffe abwehren.

Um den Datenverkehr gemäss den Wünschen des Senders oder des Empfängers verlässlich abzuwickeln, braucht es kryptologische Sicherheitsmechanismen, die die Authentizität und die Integrität der Daten gewährleisten. Diese Sicherheitsmechanismen sind auf ein System angewiesen, das digitale Zertifikate und Schlüssel verwaltet. Dieses System kann verschieden ausgestaltet werden, je nachdem, welche Ansprüche an die Sicherheit gestellt werden. Die Aufteilung des Internets in verschiedene Isolation-Domains macht es möglich, dass hier verschiedene Sicherheitskulturen nebeneinander bestehen können.

Reparaturen im Getriebe des Internets sind schwierig durchzuführen.

Nochmals von vorne anfangen

Die Arbeit an Scion begann 2009. Zusammen mit Mitarbeitern an der Carnegie Mellon University machte sich Adrian Perrig daran, die grundlegenden Protokolle zu überarbeiten mit dem Ziel, die Sicherheit und die Verfügbarkeit zu verbessern. Wie würde man diese Protokolle gestalten, wenn man bei der Entwicklung das Internet noch einmal ganz von vorne anfangen könnte?

2012 wurde Perrig an die ETH berufen, die Weiterentwicklung von Scion wird seither am Institut für Informationssicherheit in Zürich vorangetrieben. Rund 80 verschiedene Wissenschafter, so schätzt Perrig, haben zu Scion beigetragen. 2016 begannen Praxistests mit auswärtigen Partnern, Swisscom und Switch testen das neue Internet. 2017 wurde in Zürich die Firma Anapaya Systems AG gegründet, die Hardware und Software für ein sicheres Internet verkaufen will. Nach wie vor ist aber die Software, die Scion ausmacht, im Quelltext als Linux-Anwendung gratis und frei erhältlich.

Wie lange wird es dauern, bis Scion die Welt erobert hat, bis Warnungen vor gravierenden Sicherheitsproblemen im Internet eine Seltenheit darstellen? Wenn man den «Erfolg» des Mitte der 1990er Jahre eingeführten neuesten Internet-Protokolls (IPv6) zum Massstab nimmt, wird man sich noch lange gedulden müssen. Die Ablösung von IPv4, die seit 20 Jahren nicht vorankommt, zeigt, dass Reparaturen im innersten Getriebe des Internets schwierig durchzuführen sind.