Understanding Security and Resilience of the Internet

Cybersecurity is a rather vague overarching term that is used in different contexts to mean anything from: "information and computer security"; security of the Internet infrastructure; security of anything connected to the Internet (including "essential services" such as electricity distribution); security of data; applications and communications; safety of Internet users (particularly children), and frequently encompasses notions of "national" security as well as "private" security. Indeed, there is no consensus on what the term means.

Without trying to better define the term "cybersecurity" or proposing solutions for all aspects that might fall within its ambit, this paper explores the essential components for the security and resilience of the Internet ecosystem (a cornerstone for a sound cybersecurity strategy). These components are: technical and policy solutions aligned with Internet invariants; individual and collective responsibility for risk; and collaboration.

The Internet Invariants

The Internet has undergone immense change since its inception and continues to evolve. It is important to understand what is actually unchanging *about the Internet – the key properties, or invariants, "which have enabled the Internet to serve as a platform for seemingly limitless innovation, outline not only its technology, but also its shape in terms of global impact and social structures"*[1].

Any strategy for tackling cybersecurity needs to start with an understanding of the fundamental properties of the Internet that really make this global communication medium what it is – a tool for creativity, collaboration, ingenuity, expression of ideas, cultural and social identity, commercial activity, etc. We describe these fundamental properties as the "**Internet invariants**" because the continued widespread success of the Internet depends upon these properties enduring.

The first two properties are **global reach and integrity**.

The Internet is global because any endpoint connected to it can address any other endpoint. An endpoint could be a laptop, a smartphone, an Internet-enabled car navigation system, etc.

The integrity of the Internet means that an endpoint receives the information that was intended by the sender wherever the receiver connects to the Internet. For example, no matter where a user is located, he or she should receive the same Web content when accessing the Internet Society home page at **www.internetsociety.org**. Of course, a user may decide to limit the content he or she receives on his or her device (e.g. by using a browser plug-in (e.g. Ghostery) to block tracking elements such as tags, web bugs, pixels and beacons that are included in web pages to observe users online behaviour such as the websites they visit). This does not affect the integrity of the communication. However, if an ISP were to block a user's access to **www.internetsociety.org** that would be interfering with the integrity of the Internet because the information is diverted or dropped by the ISP before it reaches the endpoint. Significantly, that action is not taken by an endpoint, but rather, by an intermediary in the network.

The third key property is its **support for innovation without requiring permission.** Put another way, this is the ability for anyone to create a new application on the Internet without having to get special approval from anyone. The history of the Internet is full of examples of amazing technologies and services made possible by the freedom to introduce a new application or service without asking permission from the government, the ISP or anyone else. Perhaps, the best-known example is HTML (HyperText Markup Language), which gave rise to the World Wide Web. It was developed by a researcher at CERN in Switzerland and made available for others to run. If Tim Berners-Lee had needed to ask for permission, would the World Wide Web exist? Would the idea of providing links to data have been rejected, cutting off the development of Internet search services such as Google? Would Facebook have one billion monthly active users[2]? Would crowd-sourced data collection and visualisation services such as Ushahidi[3] exist? What about Wikipedia, Twitter, YouTube, apps, mapping software, streamed music and hundreds of other things we take for granted in our daily lives?

The fourth property is **open** – openly developed and open for anyone to use. The Internet is built on technical standards that are developed openly by consensus and then put out to the world to use. Examples of such standards include HTTP (for accessing web content), SMTP (for email), SIP and RTP (for voice and audio communications).

A fifth property that we must preserve is the **accessibility of the Internet**. This goes farther than people being able to access information and online services. It extends to their ability to: contribute content; interact with others all around the world; add an "app" or service; attach a server or a new network as long as they follow the Internet's technical standards.

The sixth key property that we need to safeguard is the Internet's **spirit of collaboration**. In addressing Internet security issues, we must find a way to get all stakeholders involved – from users, to the Internet research community, to commercial companies, to policymakers and beyond. Solutions developed in isolation either don't solve the problem or cause more harm than good. In some cases, they can even create significant problems that undermine the stability of the Internet.

The complexity of the security landscape

> *Achieving security objectives, while preserving the key Internet properties, is a fine balance and the real challenge of a cybersecurity strategy. It is essential that solutions are compatible with the Internet invariants.*

Achieving security requirements in a closed system operating in a constrained environment is relatively easy and, in many cases, a simple strategy of “security by obscurity” (a strategy that relies on the attacker's ignorance of the system design) may work well. By contrast, securing an open system, like the Internet, presents several different challenges.

First, the very same properties of the Internet that underpin its success and its value for users, open up new opportunities for various types of malicious activity. For example:

- The Internet is accessible.
    - *But, it means it is also accessible for attacks and intrusion.*
- The Internet is flourishing because of permission-free innovation.
    - *But, this also allows development and deployment of malware of different types.*
- We value the global reach of the Internet.
    - *But, in cybersecurity terms, it means that transborder cybercrime may be easier to commit and attacks could have far reaching effects.*
- Internet standards are voluntary, as is their adoption. They are the result of collaboration – the collaboration that is an integral part of the Internet’s operation.
    - *But, at the same time, it makes it hard to assign responsibility and prescribe solutions.*

When addressing cybersecurity issues, it is important to appreciate that while malicious actors will exploit any opportunity, the Internet invariants themselves are neither the origin nor the cause of malicious activity. Achieving security objectives, while preserving these properties, is a fine balance and the real challenge of cybersecurity strategy. This means that design and implementation of security solutions should be undertaken with consideration as to the potential effect they might have on the fundamental Internet properties. As noted above, it is important that security solutions are based on, or at least consistent, with the Internet invariants to ensure the continued success of the Internet as a driver for economic and social prosperity.

Technology building blocks for security

At the technical layer, the Internet technical community has a long track record of developing such solutions (which include technical protocols and technologies, as well as best operational practices) and making them available to the world to help build a more trusted and secure Internet. These solutions are developed in different standards organisations and fora openly, collaboratively, and by consensus.

Some examples of technical standards developed by the Internet Engineering Task Force (IETF) to improve the security of Internet infrastructure include:

- IPsec (Internet Protocol Security) – provides the end-to-end security at the Internet layer
- TLS (Transport Layer security) – provides communications security over the Internet and is widely used, for example, in securing web communications
- Kerberos Network Authentication System – provides a means of verifying the identities of entities on an open (unprotected) network
- DNSSEC (Domain Name System Security Extensions) – securing integrity and authenticity of DNS responses
- DANE (DNS-based Authentication of Named Entities) – leveraging DNSSEC to enable the administrators of a domain name to specify the keys used to establish a cryptographically secured connection to a server with this name.

Some examples of technical standards work under development and consideration at the World Wide Web Consortium (W3C) to improve the security of the Web and the Internet include:

- Content Security Policy
- Cross-Origin Resource Sharing
- XML Signature, XML Encryption and related specifications
- Cryptographic APIs for JavaScript

Examples of Organization for the Advancement of Structured Information Standards (OASIS) data security standards include:

- Digital Signature Services (DSS) - digital signature services standards for XML
- Key Management Interoperability Protocol (KMIP) – provides extended functionality to asymmetric encrypted key technologies
- Security Assertion Markup Language (SAML) – XML-based framework for creating and exchanging security information between online partners
- eXtensible Access Control Markup Language (XACML) – representing and evaluating access control policies

Secondly, there is no absolute security. There will always be threats and vulnerabilities, so "secure" simply means that residual risks are acceptable in a specific context. That is why "**resilience**" is an important metric when defining the goal of cybersecurity efforts. Like a human body that may suffer from viruses, but gets stronger and more resilient as a result, new technologies, solutions and collaborative efforts make the Internet more resilient to malicious activity.

Culture of shared and collective responsibility for risk

> *A high degree of interconnection and interdependency in the Internet ecosystem brings a new important requirement for achieving effective security: managing "inward" and "outward" risks collaboratively.*

Traditional approaches to security were principally concerned with external and internal threats, and the impact they may have on one's own assets. There is, however, a growing recognition that a security paradigm for the Internet ecosystem should be premised on protecting opportunities for economic and social prosperity, as opposed to a model that is based simply on preventing perceived harm. Furthermore, security needs to be approached from the perspective of managing risk – an approach that takes into account threats and vulnerabilities as well as their likelihood and impact.

The Internet, with its high degree of interconnection and dependencies, brings another dimension to the assessment of risks. Security and resilience of the Internet depends not only on how well risks to an organisation and its assets are managed, but also, importantly, on the recognition and management of risks that the organisation itself (by its action or its inaction) presents to the Internet ecosystem – the "outward" risks. For example: the existence and poor maintenance of so-called "open DNS resolvers" that are commonly used for reflector DDoS attacks[4]; poor security policies and practices that allow compromised computers to join long-lived botnets; a PKI Certification Authority (CA) with insufficient protection and inadequate security breach detection capability leading to a compromise and a delayed announcement of a security incident[5].

This particular aspect of risk management is not necessarily self-evident, especially since there is often no obviously identifiable immediate harm to the organisation or its assets and, therefore, no direct business case that can be immediately associated with reducing the "outward" risks. At the same time, neglecting it leads to a decrease in the overall security of the ecosystem.

Additionally, some risks need to be managed by more than one actor. This is the notion of shared risk management. This is especially important where the security of the global Internet infrastructure is concerned. As networks are interconnected and interdependent, one network acting alone can make little difference, even in protecting its own resources. Collective responsibility, therefore, plays a particularly crucial role in the security and resilience of the global Internet routing system. For example, mitigating the risk of reflection DDoS attacks requires wide adoption of ingress filtering practices to prevent IP addresses spoofing[6]. While a resource (e.g. a web server) can still be attacked even though the network hosting it uses ingress filtering, if other connected networks do not deploy ingress filtering, this network's action benefits the Internet as a whole because this network would not be a launch pad for such attacks.

The culture of shared and collective responsibility is well aligned with the "public interest" nature of the Internet. In the cybersecurity context, this means that the implementation of security solutions is a long-term investment in the Internet ecosystem from which everyone benefits, and that all stakeholders have a shared interest in the management of these resources.

Collaboration as an essential component of effective security

> *Ultimately, it is people that hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration and we believe that is still one of the essential factors for its prosperity and potential.*

Security, in general, is a difficult area when it comes to identifying incentives. The security of the global Internet infrastructure, whether it is DNS or routing, brings additional challenges: the utility of security measures is heavily dependent on the actions of many other parties.

Further, if participants in the Internet ecosystem act independently and solely in their own self-interest, not only will it impact the security of the ecosystem, but it will also diminish the overall pool of social and economic potential that the Internet offers. Such a situation is often described as the "tragedy of the commons" – a term coined by Garrett Hardin[7] in his paper with the same title. Indeed, the analogy of the commons can be applied to the Internet ecosystem, powerfully highlighting some of the challenges, especially in the area of cybersecurity.

It is not easy to overcome the "tragedy of the commons" in the area of Internet security and resilience because it is human nature to seek outcomes that further our individual self-interest. However, that approach is counter-productive and, in the long-term, harmful to everyone's interests.

Technology solutions are an essential element here, but technology alone is not sufficient. To realise visible improvements in this area, there must first be a better articulation of the problem space in terms of risks, based on metrics and trends, and, more importantly, a cultural change promoting collective responsibility across all fields of endeavour: policy, legal, technical, economic, social.

Internet development has been based on voluntary cooperation and collaboration. Internet history contains many examples of such cooperation and its efficacy. A prime example is the Conficker Working Group[8], created to fight the Internet borne attack carried out by malicious software known as Conficker. Regional and national network operators groups (NOGs), and their role in resolving operational problems (often spanning multiple networks), is another example.

The issues, the associated challenges of and opportunities for collaboration, together with the cultural change that is needed can be grouped into four main areas. In our opinion, making progress in each of these areas is a prerequisite for a positive impact on the security and resilience of the Internet:

1. **Common understanding of the problem**. The more aligned all the stakeholders are with regard to the problems, their severity and the priority of their resolution, the more focused the dialogue is, and the more coherent various efforts aimed at improving security and resiliency will be.

2. **Common understanding of solutions**. The challenge here is that there is a whole array of possible solutions (technical, policy, economic, social) and each of them solves only part or one set of the problems at a particular point in time. It is important to understand that there is no "silver bullet", but rather, evolving building blocks that can be used in constructing a security solution.
3. **Understanding of common and individual costs/benefits**. The technology building blocks vary in the costs and the benefits they bring to an individual participant and to the common good of the global infrastructure. Understanding these factors and how they are aligned with the business objectives of network operators and others is crucial for sustained improvements in security and resilience.
4. **Ability to assess risks**. The adequate selection of tools and approaches is dependent on the ability to properly assess risks, both "inward" as well as "outward". This requires agreement on metrics and factual data, and on the trends associated with them. This data is also important to measure the effectiveness and impact of such tools once they are deployed, and to monitor the changing dynamics of the environment.

It is not realistic to assume that there will be universal agreement on the underlying issues, or that a coherent plan of action will be adopted globally in the foreseeable future. Commercial competition, politics and personal motivation also play a role in how well collaboration happens. But, as several collaborative efforts have demonstrated, differences can be overcome to cooperate against a threat. Such voluntary as-needed "working for the benefit of everyone" collaboration is remarkable for its scalability and its ability to adapt to changing conditions and evolving threats, yielding unprecedented efficacy.

Endnotes

[1] "Internet Invariants: What Really Matters", http://www.internetsociety.org/internet-invariants-what-really-matters

[2] http://news.cnet.com/8301-1023_3-57525797-93/facebook-hits-1-billion-active-user-milestone/

[3] Ushahidi is an open source project which allows users to crowdsource crisis information to be sent via mobile, www.ushahidi.com/

[4] For example, a technique used in the attack against www.spamhaus.org in March 2013.

[5] For example, a compromise of a Dutch Certificate Authority Diginotar, full report http://www.rijksoverheid.nl/bestanden/documenten-en-publicaties/rapporten/2012/08/13/black-tulip-update/black-tulip-update.pdf

[6] For more information see RFC 2827 Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing (http://tools.ietf.org/html/rfc2827)

[7] Hardin, G. "The Tragedy of the Commons". Science 162 (3859): 1243–1248, 1968.

[8] Conficker Working group, http://www.confickerworkinggroup.org/wiki/

Internet Society
Galerie Jean-Malbuisson, 15
CH-1204 Geneva
Switzerland
Tel: +41 22 807 1444
Fax: +41 22 807 1445
www.internetsociety.org

1775 Wiehle Ave.
Suite 201
Reston, VA 20190
USA
Tel: +1 703 439 2120
Fax: +1 703 326 9881
Email: info@isoc.org