Collaborative Security

An approach to tackling Internet Security issues

APRIL 2015

Internet Society™

Executive Summary

People are what ultimately hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration. Cooperation and collaboration remain the essential factors for the Internet's prosperity and potential.

Collaborative Security is an approach that is characterized by five key elements:

- **Fostering confidence and protecting opportunities**: The objective of security is to foster confidence in the Internet and to ensure the continued success of the Internet as a driver for economic and social innovation.
- **Collective Responsibility**: Internet participants share a responsibility towards the system as a whole.
- **Fundamental Properties and Values**: Security solutions should be compatible with fundamental human rights and preserve the fundamental properties of the Internet — the *Internet Invariants*.
- **Evolution and Consensus**: Effective security relies on agile evolutionary steps based on the expertise of a broad set of stakeholders.
- **Think Globally, act Locally**: It is through voluntary bottom-up self-organization that the most impactful solutions are likely to reached.

Introduction

Any cybersecurity framework needs to start with an understanding of the fundamental properties of the Internet (open standards, voluntary collaboration, reusable building blocks, integrity, permission-free innovation and global reach ("*the Internet Invariants*"[1])) and an appreciation of the complexity of the cybersecurity landscape. It should be premised on fostering trust and protecting opportunities for economic and social prosperity. Furthermore, real security on the Internet can only be realised within a broader context of trust and respect of fundamental human rights and values, such as privacy.

Achieving security objectives, while preserving these fundamental properties, rights and values is the real challenge of cybersecurity strategy. The design and implementation of security solutions should be undertaken with consideration as to the potential effect they might have these fundamentals.

Everyone has a collective responsibility for the security of the Internet: multistakeholder cross-border collaboration is an essential component.

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

Commercial competition, politics and personal motivation play a role in how well collaboration happens. But, as 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.

Informed by these reflections, we introduce the term "**Collaborative Security**" to describe our approach for tackling Internet security issues.

The Collaborative Security approach to Internet security

> ***People are what ultimately hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration. Cooperation and collaboration remain the essential factors for its prosperity and potential.***

Collaborative Security is an approach that is characterized by five key elements. These are described below.

1. Preserving opportunities and building confidence

The Internet enables **opportunities** for human, social and economic development on a global scale. Those opportunities will only be realized if Internet participants have **confidence**[2] that they can use the Internet for secure, reliable, private communication all across the world.

A security paradigm for the Internet should be premised on fostering confidence and protecting opportunities for economic and social prosperity, as opposed to a model that is based simply on preventing perceived harm. Moreover, security solutions should advance that objective in design, and in practice. Otherwise, security solutions may go too far, thereby jeopardizing the very infrastructure that ties together the global economy, and provides the engine for its growth.

2. Collective Responsibility

The Internet is a global interconnected network of networks. It is, in effect, a global common resource and a highly interdependent system. Participation on the Internet means **global interdependency**.

In an interconnected interdependent system, no one participant can achieve absolute security. And, no security solution exists in isolation. There will always be threats, so it is useful to consider security in terms of residual risks that are considered acceptable in a specific context.

---

[2] In this context, an Internet participant's "confidence" is formed, among other things, taking into account the degree of perceived security risk associated with using the Internet and whether that degree of risk is acceptable while protecting opportunities for economic and social prosperity. A better understanding of actual risks and how to reduce them to an acceptable level are two main factors that build confidence.

Internet security depends not only on how well participants manage security risks they face, but also, importantly, how they manage security risks that they may pose to others (whether through their action or inaction) – the "outward" risks.

These factors mean that Internet participants have:

- a common interest in the management of this resource to ensure its sustainability; and
- a collective responsibility to care for the Internet for the benefit of everyone.

Furthermore, if Internet participants act independently and solely in their own self-interest, not only will the security of the Internet be impacted: the overall pool of social and economic potential that the Internet offers the global community will also diminish. Therefore, Internet participants need to see this as a long-term investment for the benefit of everyone.

Note: The scope of collective responsibility extends to the system as a whole: it is not the same as asking everyone to be responsible for their part of the ecosystem. Therefore, collective responsibility requires a common understanding of the problem, shared solutions, common benefits, and open communication channels[3].

Multistakeholder cross-border collaboration is an important component of collective responsibility. Its success depends on trustful relationships – between nations, between citizens and their government, between operators, service providers, and across all stakeholders.

3. Security solutions should be fully integrated with rights and the open Internet

Security solutions should be fully **integrated** with the important objectives of preserving the fundamental properties of the Internet (open standards, voluntary collaboration, reusable building blocks, integrity, permission-free innovation and global reach (also known as the *Internet Invariants*[4])) and fundamental human rights, values and expectations (e.g. privacy, freedom of expression).

Any security solution is likely to have an effect on the Internet's operation and development, as well as user's rights and expectations. Such effects may be positive or negative. From our perspective, it is important to find solutions that support the *Internet Invariants* and fundamental rights and values.

[3] Please refer to Understanding Security and Resilience of the Internet http://www.internetsociety.org/sites/default/files/bp-securityandresilience-20130711.pdf

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

4. Security solutions need to be grounded in experience, developed by consensus and evolutionary in outlook

Security solutions need to be **flexible** enough to evolve over time. We know that technology is going to change and threats will adapt to take advantage of new platforms and protocols. Therefore, solutions need to be responsive to new challenges.

Like a human body that may suffer from viruses, but gets stronger and more resilient as a result, new technologies, solutions and cooperative efforts that build on "**lessons-learned**" make the Internet more resilient to threats.

Experience shows us that, in a quickly evolving system such as the Internet, an **open consensus-based participatory approach** is the most robust, flexible and agile.

Partial solutions and staged deployment are important and should be taken seriously. A collection of **incremental solutions** may be more effective in practice than a grand design. Even if an approach does not solve the problem completely, it might help to contain it, or to change the economic equation significantly enough, so as to make the vulnerability much less attractive to malicious actors.

The focus needs to be put on defining the agreed problem and finding the solution. We also need to make space for the new, the innovative and the odd. We need to be prepared to test disruptive or non-traditional ideas.

In the end a process, which draws upon the interests and expertise of a broad set of stakeholders is likely to be the surest path to success.

5. Targeting the point of maximum impact: think globally, act locally

Security is not achieved by a single treaty or piece of legislation; it is not solved by a single technical fix, nor can it come about because one company, government or actor decides security is important.

Creating security and trust in the Internet requires different players (within their different responsibilities and roles) to take action, closest to where the issues are occurring.

Typically, for greater effectiveness and efficiency, solutions should be defined and implemented by the smallest, lowest or least centralized competent community[5] at the point in the system where they can have the most impact.

[5] In politics, such approach is called a Subsidiarity principle: Solutions should be defined and implemented by smallest, lowest or least centralized competent authority. We feel that the word community better matches the sense of bottom-up development. http://en.wikipedia.org/wiki/Subsidiarity

Such communities are frequently spontaneously formed in a **bottom-up, self-organizing** fashion around specific issues (e.g. spam, or routing security) or a locality (e.g. protection of critical national infrastructure or security of an Internet exchange).

As much as possible, solutions should be based on **interoperable building-blocks** – e.g. industry-accepted standards, best practices and approaches.

Conclusion

We believe that this Collaborative Security approach for addressing Internet security issues is critical for ensuring the future of the open Internet as a driver for social and economic innovation. As a network of networks without centralized control, the security of the Internet cannot be maintained by any single entity or organization. It is important that these issues be addressed by all stakeholders in a spirit of collaboration and shared responsibility in ways that do not undermine the global architecture of the Internet or curtail human rights. The Internet is for everyone: let's work together to realize its full potential.

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

Version 1.0 updated 11 April 2015-english