

Trust and the Future of the Internet

Summary

To be trusted, the Internet must provide channels for secure, reliable, private communication between entities, which can be clearly authenticated in a mutually understood manner. The Internet Society (ISOC) Board of Trustees has determined that the issue of trust is both important and crucial for the long-term growth and success of the Internet. After a review of current literature and of emerging research efforts as well as consultations with subject experts, the following areas were deemed to be of special importance:

- **Advancing Internet architecture** by supporting the implementation of open trust mechanisms throughout the full cycle of research, standardization, development, and deployment
- **Strengthening the current Internet model** by focusing on the mitigation of social, policy, and economic drivers that could hinder development and deployment of trust-enabling technologies
- **Facilitating end users' ability to manage personal data and ensure personal security** by elevating identity to a position as a core issue in network research and standards development

The ISOC Board of Trustees conducted a three-day retreat in October 2007 in Toronto to focus on the subject of trust within the context of network-enabled relationships. The retreat was part of the Board's discovery process to define a long-term Major Strategic Initiative (MSI). The ISOC Board chair's stated aim was to "achieve a common understanding of the subject area and form an initial opinion whether we [ISOC] can make unique and useful contributions in this area."

A nonprofit organisation, the Internet Society was founded in 1992 as a leader in promoting the evolution and growth of the Internet. Through our members, chapters, and partners, we are the hub of the largest international network of people and organisations that work with the Internet. We work on many levels to address the development, availability, and technology of the Internet.

The Internet is critical to advancing economic growth, community self-reliance, and social justice throughout the world. Become a member of the Internet Society, and share this vision. For more information, visit <http://www.isoc.org>.

1775 Wiehle Avenue, Suite 102
Reston, VA 20190-5108, U.S.A.
+1 703 439 2120

4, rue des Falaises
CH-1205 Geneva, Switzerland
+41 22 807 1444

Retreat Agenda, Structure, and Attendees

Agenda

The agenda was designed around the following high-level goals:

- To develop a shared language for talking about trust, to come to a shared understanding of current architectural and operational practices, and to create a set of trust-related questions worthy of further exploration
- To determine how trust issues might be included in strategic planning for the future of the Internet and how, where, and whether ISOC should begin to address the topic of trust issues
- To achieve an understanding of the breadth of trust-related issues and to brainstorm ideas for ways ISOC could most productively involve itself with those issues

Structure

The workshop was structured to have three unique days. On day one, participants explored the problem space and developed a shared language and understanding. Day two focused participants on key issues, with participation by invited subject experts. And on day three, participants developed an ISOC-centered approach to trust and began to formulate next steps.

Attendees

ISOC Board of Trustees/Officers: Fred Baker, Scott Bradner (remote), Hiroshi Esaki, Patrik Fältström, Ted Hardie, Daniel Karrenberg, Franck Martin, Desirée Miloshevic, Alejandro Pisanty (remote), Glenn Ricart, Stephen Squires (past BoT member and instigator), Lynn St. Amour, Bill St. Arnaud, Patrick Vande Walle

ISOC Staff: Leslie Daigle (remote), Frederic Donck, Lucy Lynch, Karen Rose

Internet Technical Community Representatives: Russ Housley (Internet Engineering Task Force chair), Olaf Kolkman (Internet Architecture Board chair), Danny McPherson (Internet Architecture Board)

Subject Experts: Levi Gundert (Team Cymru), Dick Hardt (Sxip Identity), RL “Bob” Morgan (Internet 2, University of Washington), Mikko Särelä (Nomadic-Lab)

Day One: Exploring the problem space and developing a shared language and understanding

Exploring the Problem Space

The retreat opened with a series of roundtable discussions based on reading material provided in advance. This review served to frame some of the important issues and enabled participants to communicate experiences and concerns. It also generated a number of questions and assertions to be explored further with subject experts.

Developing a Shared Language and Understanding

Defining Trust

Following the review, the group moved on to a set of questions about trust:

- What do we mean when we say *trust*, *trusted*, or *trustworthy*?
- Where and how is trust established?
- How are conflicting goals managed?

Those questions were explored via a list of four key words drawn from a presentation by Stephen Squires on the historical development of network security:

- Reliability
- Security
- Privacy
- Liberty

This exercise led to an extended group discussion that sought to identify some of the key elements of trust, and then explored how those elements might be incorporated into both Internet architecture and the end-user experience. Many raised concerns about the tussles between openness, security, and privacy as well as about where and how trust could be implemented in the existing layered architectural model. There was also a discussion of “behaves as expected in a given context” as a formulation for what it meant to be trustworthy.

Throughout the discussion there was strong support for addressing the concerns of the end user and for finding ways to ensure trustworthiness across all the layers of the current Internet model.

What does trust mean for ISOC?

The group next considered ISOC's core principles and the nature of ISOC's role in this area: to promote the stand that everyone have a fundamental level of network access and to ensure that the common networks to which individuals have access possess the key attributes of the Internet. One of the key characteristics that ISOC deems is critical to preserve is the any-to-any nature of the Internet, which allows unfettered data flows without prior coordination and with every network over which such data flows will pass. ISOC's role in the trust programme falls within this category.

Some of ISOC's concerns were also discussed in terms of the current and potential threats to the any-to-any paradigm and whether those issues can be resolved in a cohesive manner. Additional questions were raised about how trust issues might affect ISOC constituents—namely, end users (identity/privacy/access), IAB/IETF/IRTF (architecture/standards/research), and core ISOC programmes (support for standards/policy/education) and their interests.

The areas where ISOC could have maximum impact—primarily at the policy and technical levels—were discussed.

Questions for the Subject Experts

The various concerns and issues raised were crystallized into the following list of questions to be raised with the subject experts on day two. The questions were framed to deliberately encourage participants to look beyond any single problem or proposed change and instead focus on the long-term implications of incorporating trust as a core element of the Internet design and deployment process.

- What are the alternative futures for trust and the Internet? Does that future still include the any-to-any Internet?
- How do proposed changes align with economic reality? Can those changes be deployed?
- Where do you see the boundaries between technology and policy? What are the potential showstoppers?
- What solutions would you propose? Would they facilitate wider deployment of the Internet?

Day Two: Focusing on key issues with the participation by invited subject experts

Using the list of questions as a basis for the discussion, the second day had the group and invited subject experts considering three major tussle spaces corresponding to the goals stated on the retreat agenda.

- Internet architecture both old and new
- Current problems and emerging solutions
- Identification of the conflicting expectations of end users, including privacy, security, active user management, and ease of use

The subject experts' presentations and the group discussions exposed certain recurring points of conflict such as the difficulties of designing for both security and openness, the ways human factors influence both design and adoption, how changing uses of the Internet affect existing systems, and the need for better coordination across all of the layers and players.

These sessions opened up some additional concerns about both the continued viability of the any-to-any nature of the Internet and ISOC's ability to address the issues effectively. It was decided that participants would split into two small groups to focus on (1) what ISOC's strategic goals would be for a trust initiative and (2) the opportunities ISOC has for engaging and proactively working on these issues.

Breakout Session One: What are ISOC's strategic goals for a trust initiative?

Discussion of ISOC's goals was framed as a single question: What would the Internet we're building with this programme be like, and what is our role there?

Ted Hardie shaped the further discussion by telling about some experiences from his days as a cultural anthropologist. When analysing a large number of requests for migration from one country to another, he found that successful migrants were trained to focus less on the reasons for leaving the country of origin than on the vision of the country of destination. With that focus, migrants were able to help the destination country see why it should welcome each specific immigrant as a new citizen.

Ted suggested the discussion should aim the same way: by focusing on the Internet we'd like to create rather than on problems with current conditions. Thus, the discussion on trust focused mostly on what an In-

Internet that preserves the any-to-any principle would be like if it also enabled the highest, most relevant level of trust among its many users, builders, and providers.

Responses were then captured into the following set of characteristics describing what could constitute and inform a trust-based Internet:

- **Appropriateness:** facilitate trust or identity mechanisms appropriate to users' needs
- **Stability:** reachability—consistently available and predictable
- **Common law and the metric system:** a shared set of rules including open protocols and interoperability among implementations
- **Criminality:** We expect that there will continue to be criminals, different types of crime, and ways to address crime.
- **Abundant shared resources** that all are able to access
- **Opportunities:** providing a field for innovation

Breakout Session Two: What are the opportunities for engagement?

The second group held a brainstorming session to identify current and new capacities that ISOC could use to tackle some of these issues and effect positive change.

The group concluded that some immediate short-term projects could be effectively handled within existing core ISOC programmes (such as support of standards, education, and policy) but that ISOC needed to reach out to new partners and build up internal technology efforts in order to achieve some of the longer-term goals of the trust initiative.

Day Three: Developing an ISOC-centric approach to trust and formulating next steps

Synthesis

Day three began with the participants of both breakout sessions sharing results with each other, followed by the opportunity for the wider group to comment. Highlights included a statement from Board chair Daniel Karrenberg on his envisioned ideal end-user

experience; a technical proposal by Fred Baker that explored the problem of persistent identity and privacy; and final remarks by subject experts and departing guests.

Many speakers took the opportunity to emphasize key issues one last time. Concerns ranged from the technical (improve the security of the end devices) to the operational (influence the economic drivers currently tipped against deployment), to long-term ideals (elevate identity to a position as a core issue in standards development and research).

Participants also returned to core concerns: What are the threats to the Internet model if the Internet technical community doesn't act to provide solutions beforehand? What are the overall architectural constraints on realizing our end goals? The group acknowledged that taking on some of the major trust-related issues could carry a certain amount of risk both for ISOC and for the current multistakeholder model.

The general consensus was that the problem of trust was both serious and important and that ISOC could have a major role in effecting changes that improve Internet technologies, strengthen the Internet model, and improve the end-user experience.

ISOC's Seven Directives for the Trust Initiative

In the final session, key takeaways and agreements were discussed, and seven directives were created:

1. Promote the stand that trustworthiness is crucial for the long-term growth and success of the Internet.
2. Formulate ambitious goals for a long-term effort that are driven by the larger vision of an Internet that is good for everyone.
3. Investigate, be conscious of, and explain the economic drivers that achieve and sustain trustworthiness within the Internet.
4. Clearly articulate the purposes and end goals of the initiative; support this with a well-designed communications campaign.
5. Chart the problem/solution space in a holistic manner. Define the ISOC vision without being constrained; look both inside and outside ISOC. Extend ISOC's reach to new communities and partnerships. Develop and maintain a map of activities—both ISOC's own and those of others.

6. Develop plans and a framework for what the bigger picture looks like over the long term and how project proposals fit within that.

7. Take some short-term action in order to get going and gain momentum.

There was broad agreement that ISOC staff should move forward to develop and plan this work as a major effort. The Board emphasized the need for long-term vision but also expects to see progress in the form of smaller, short-term projects in the interim. Staff was urged to prioritize on areas where ISOC can make the greatest impact and to invite participants from all parts of the ISOC community, including chapters.

There was a strong sense that early efforts may need to focus on technology and education but also that there would be a natural expansion into governance work and the policy space as efforts matured.

The group then listed some major work items for ISOC, including:

- Identification of key stakeholders needed to work on these issues
- Engagement with civil society on issues related to liberties
- Elevation of issues related to trust in the enterprise sphere
- Support of deployment of emerging technical solutions (for example, Domain Keys Identified Mail)
- Pulling together of stakeholders across multiple layers to define problem scope

The retreat closed with the staff's confirmation to the Board that the staff had the direction and information needed to move forward. It was proposed that a summary report and detailed proposal for undertaking a trust initiative based on this new direction would be discussed at the December 2007 trustees' meeting.

Recommended Reading List

Tussle in Cyberspace: Defining Tomorrow's Internet

<http://www.sigcomm.org/sigcomm2002/papers/tussle.pdf>

Computer Security Technology Planning Study, Volume I, ESD-TR-73-51 Vol. I

<http://seclab.cs.ucdavis.edu/projects/history/CD/ande72a.pdf>

RFC 1281. Guidelines for the Secure Operation of the Internet

<http://tools.ietf.org/html/rfc1281>

Information Security: Science, Pseudoscience, and Flying Pigs

<http://www.acsac.org/invited-essay/essays/2001-schell.pdf>

IETF Security Tutorial

<http://www.ietf.org/proceedings/07mar/slides/sectut-0.pdf>

RFC 4948. Report from the IAB Workshop on Unwanted Traffic, March 9–10, 2006

<http://tools.ietf.org/html/rfc4948>

Report: The IAB Workshop on Unwanted Traffic

<http://www.ietf.org/proceedings/06nov/slides/plenaryt-3.pdf>

The Underground Economy: Priceless

<http://www.usenix.com/publications/login/2006-12/openpdfs/cymru.pdf>

Why The Internet Only Just Works

<http://www.cs.ucl.ac.uk/staff/M.Handley/papers/only-just-works.pdf>

Experimenting with TCPA/TCG Hardware, or How I learned to Stop Worrying and Love the Bear

<http://www.ists.dartmouth.edu/library/263.pdf>

The 4th Annual PKI R&D Workshop: Summary

http://middleware.internet2.edu/pki05/proceedings/workshop_summary.html

Trusted Network Connect: Frequently Asked Questions

https://www.trustedcomputinggroup.org/groups/network/TNC_FAQ_updated_may_18_2

Privacy Principles for Identity in the Digital Age

http://www.aotalliance.org/summit2007/2007_presents/202_ID%20Principlesx.pdf

Personal Internet Security

<http://www.parliament.the-stationery-office.com/pa/ld200607/ldselect/ldsctech/165/165i.pdf>

New Arch: Future Generation Internet Architecture

<http://lucan.ddns.comp.nus.edu.sg/Readinglist/newarch-final.finalreport.pdf>

Defining a Future Network: An International Research Agenda

<http://cfp.mit.edu/events/may07/Slides/CLARK%20Defining%20a%20future%20network.ppt>

The EIFFEL Initiative

http://dalore.net/DOT/wp-content/uploads/ETSI_presentation.ppt

Social and Economic Factors Shaping the Future of the Internet

http://www.oecd.org/document/4/0,3343,de_2649_201185_39046340_1_1_1_1,00.html

RFC 4949. Internet Security Glossary, Version 2

<http://tools.ietf.org/html/rfc4949>

Rethinking the Design of the Internet

<http://portal.acm.org/citation.cfm?doid=383034.383037>

RFC 3724. The Rise of the Middle and the Future of End-to-End: Reflections on the Evolution of the Internet Architecture

<http://tools.ietf.org/html/rfc3724>

End-to-End Arguments in System Design

<http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.pdf>