A National Goal for Cyberspace: Create an Open, Accountable Internet

Today's Internet has proven to be such a valuable resource, so useful in enabling creative new forms of communication and commerce, that it has become a critical infrastructure underlying much of our economy and society. Unfortunately, today's Internet and the machines it connects have also become easy targets for economically and politically motivated attacks that exploit vulnerabilities in computer software and network protocols that were designed without security as a primary consideration.

Hand-wringing over computer and network insecurity today is common. To manage the problem, we've grown entire industries that seem to depend on providing regular patches and system updates. Recently, the CERT-CC at Carnegie Mellon University celebrated its 20th anniversary; its creation was a response to the original Internet worm episode of 1988. Without deprecating in any way the good work of this organization and its cooperators over the past 20 years, it was set up to deal with "emergencies." By now, shouldn't we see fewer such emergencies rather than more? Must we be satisfied to live with a cyberspace in which simply browsing a Web site or reading an email can turn our personal computers into slaves of organized crime or a foreign government?

In our last issue, Fred Schneider argued that, in a world of imperfect systems and malicious attacks, accountability can provide a force to improve systems and deter attackers.[1] Unfortunately, as he also noted, today's systems are not only imperfect, they are not designed to provide very good accountability. It remains difficult to hold developers, users, or system components accountable for actions and traffic on the Internet and in systems connected to it. To preserve its creative force, the Internet must remain open to the development of innovative services and applications, but its infrastructure must evolve to provide an increased level of accountability.

Holding people accountable will require a sound infrastructure for identification and authentication, which immediately raises concerns about privacy and anonymity. Accountability can actually help assure privacy, by making it possible to hold accountable those who improperly expose or transmit private information, for example. Perhaps "accountable anonymity" is an oxymoron, but degrees of anonymity are possible. Scott Charney, while strongly asserting the need for soundly based mechanisms for identification and authentication (and indeed a diverse collection of such mechanisms), calls equally for the preservation of mechanisms that enable anonymous expression (see www.microsoft.com/mscorp/twc/endtoendtrust). Our paper or "snail" mail systems today permit both anonymous letters and certified mail to flow through the same infrastructure. Electronic bank transactions demand a high standard of authentication, but we must also provide for anonymous retrieval of information about sensitive diseases from public healthcare databases.

Accountability can be provided in many ways: forensically, after the fact, or before the approval of a communication or transaction. It can apply to different kinds of principals—to network users but also to software developers, ISPs, routers, and other infrastructure components. To be accountable, the individual, company, or system component must pledge something of value—money, reputation, friendship—that can be forfeited in case of improper actions.

What capabilities should we expect of an accountable Internet? They might include the ability to know with confidence the source of an arriving packet; the ability to hold a user (or a machine) accountable for the traffic it originates, thereby enabling the recipient to have the network reject traffic from specified sources a priori; the

Carl E. Landwehr
Editor in Chief

ability to determine what path an arriving packet has taken; and the ability to know the provenance of software updates arriving from the network and then authorize (or at least detect) any changes to software caused by arriving packets. This list doesn't capture all that's either necessary or sufficient for an accountable Internet, but such a list is certainly needed.

Many design choices are possible for introducing accountable behaviors, and many trade-offs in function, cost, and dependability must be considered. We need to propose, debate, and study those choices. But much of the technology required to provide these properties in the network infrastructure is available in some form today. Unfortunately, based on the Internet's past evolution, it seems unlikely that an open, accountable Internet will emerge on its own.

The lack of accountability in the cyberinfrastructure is truly a global problem: it would seem to be in the interest of virtually every responsible country, citizen, and company to solve it. But it might be most practical to begin to address accountability at the national level. The US government stimulated the original development of Internet technology, so perhaps it's the right entity to begin to renew it. It has already inaugurated a significant program to deal with the alligators in our current swamp of deployed technology, as we reported last year in an interview with Melissa Hathaway.[2] This program includes a thrust to develop "leap ahead" technologies that should help drain that swamp. Embracing the goal of creating an open, accountable Internet within, say, 10 years, could help focus many diverse research and deployment efforts. It could also help structure international cooperation.

This isn't a call for specific government funding or control (although some might be warranted), but for government leadership. The Internet infrastructure is largely privately owned, but simply defining the goal and publicizing it can do much to stimulate and catalyze needed development. Without improved accountability in the Internet, we can only expect attacks and damage to escalate. We should set a goal of achieving an open, accountable Internet by 2020. □

References

1. F.B. Schneider, "Accountability for Perfection," *IEEE Security & Privacy*, vol. 7, no. 2, 2009, pp. 3–4.
2. S. Saydjari, "Launching into the Cyberspace Race: An Interview with Melissa Hathaway," *IEEE Security & Privacy*, vol. 6, no. 6, 2008, pp. 11–17.