A Time for Choosing

As the Internet becomes more important, the claims on it increase. Those claims cannot all be met. Now is the time for choosing.

Daniel E. Geer Jr.
In-Q-Tel

The Internet was built by academics, researchers, and hackers—meaning that it embodies the liberal cum libertarian cultural interpretation of "American values," namely that it is open, nonhierarchial, self-organizing, and leaves essentially no opportunities for governance beyond protocol definition. Anywhere the Internet appears, it brings those values with it (treating censorship as a routing failure, say). Other cultures, other governments, know that these are America's strengths and that we are dependent upon them, hence as they adopt the Internet they become dependent on those strengths and thus on our values. A greater challenge to sovereignty does not exist.

Most world governments have a very different relationship with their citizens than does the US; our prioritization of free speech above competing values being a strikingly clear example. If the definition of freedom is simply "that which is not forbidden is permitted," then there is little room to argue whether free speech is or is not built into the design of the Internet. It is, per se.

Most governments see formal standards as a tool of national policy, and for that precise reason most governments prefer the International Telecommunications Union (ITU) where it is governments that have standing. By contrast, the founders of the Internet Engineering Task Force (IETF) had a fundamentally American view and took a fundamentally American approach, as when David Clark said, "We reject kings, presidents, and voting. We believe in rough consensus and running code."

To my mind, the most important technical decision ever made was that the security of the Internet was to be end-to-end. Nothing else comes close. 50 vs. 60 Hz for alternating current? Who cares? It's all fungible. But end-to-end security, not security in the fabric of the Internet itself, is American values personified. It is the idea that accountability, not permission seeking, is the way a government curbs the misuse of freedoms, and, as accountability scales where permission seeking does not, accountability wins.

End-to-end is the digital manifestation of the right of association and, in any case, is what enabled the Internet to become relevant in the first place. End-to-end does precisely what Peter Drucker told us to do: "Don't solve problems, create opportunities." The provision of content from anywhere to anywhere, which is the value statement in Metcalfe's law, is a challenge to sovereignty. America's founders wanted no sovereign at all, and they devised a government that made the center all but powerless and the periphery fully able to thumb its nose at whatever it felt like. Much ink has been spilled on the frontier ethic versus the wishful policies favored by the comfortable urbanity of the welfare state, but the Internet's protocols have everything in common with the former and nothing in common with the latter.

US Supreme Court Justice Louis Brandeis, writing in 1928, defined privacy in this same American spirit, calling it, "The right to be left alone—the most comprehensive of rights, and the right most valued by civilized men." Not even governments threaten that definition as much as does consolidation in the telecommunications market: anti-freedom regulation and anti-privacy surveillance become easier the fewer the number of entities to regulate and/or deputize. Of course, for those countries that choose a government monopoly in telecommunications, freedom in the American sense cannot be lost as it never existed in the first place. The Internet's protocols presume many paths, not The One True Path leading to the only door in a Great Firewall.

On security as viewed by governments, many of them act consistently with a belief that all American Internet technology must somehow have been rigged to appear benign and open but actually to be a tool of American espionage—though, as everyone

cont. on p. 95

1540-7993/11/$26.00 © 2011 IEEE

cont. from p. 96

who cares to know knows, it is the US that is the preferred and predominate target of Internet-enabled espionage.

Countries seeking sovereignty in the Internet at large are thwarted by the Internet's structure, by the very protocols that carry American values. Countries wanting sovereignty in some piece of the Internet are asking that the Internet be fragmented. The realist knows that global agreement on what policy to embed in the Internet fabric simply will never happen. Take cybercrime: cybersecurity failure is always involved and so one might imagine that the global community could agree on it. BRIC countries (Brazil, Russia, India, China) dismiss the Council of Europe's Convention on Cybercrime as "unenforceable" and the US will sign only the Convention and not the Protocol forbidding free speech.

Benjamin Franklin voiced American values when he said "They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." The Internet, for all its slop, delivers liberty in a way that Franklin would immediately call his own. All despots consolidate their power in the name of security. We, you and I, are at an inflection point in history. We have an Internet that has American values built in. There are many who want it otherwise, including the anti-American faction of the permanent American bureaucracy.

I write this literally staring at a broken fortune cookie on my dining room table: "Do not pray for safety; it is the most dangerous thing in the world." I ask you to do your part to keep policy—everyone's policy—out of Internet protocols. Speak as security people and remind all that there comes a point where safety is not safe, a point one passes as soon as one concludes that personal responsibility for Internet security is irrelevant or quaint. Had American values not been embedded in Internet protocols, we would not be having this conversation. If these protocols fall, many future conversations will never happen. Time is short, and the water rises. □

***Daniel E. Geer Jr.** is CISO for In-Q-Tel and past president of the Usenix Association. Contact him at dan@geer.org.*

cn *Selected CS articles and columns are also available for free at http://ComputingNow.computer.org.*

Call for Papers:

Developments in Authentication Technologies

IEEE SECURITY & PRIVACY

Guest editors: Richard Chow (richard.chow@parc.com),
Markus Jakobsson, and Jesus Molina

Final submissions due 15 May 2011

With a constantly increasing number of devices and situations requiring authentication, there's a need for improved authentication methods—and for an improved understanding of the properties of the methods in use. We seek articles on developments in authentication technologies. Potential submission topics include (but are not limited to) the following:

- Authentication methods and implementations; evaluations of these, including experimental assessments of their security, usability, and attacks on them
- Techniques to detect and manage exceptions; to broker trust; to authenticate and yet preserve privacy; and to share and evaluate data for authentication purposes in ways that minimize the negative impacts of sharing.
- Practical cryptographic protocols; innovative constructs, their performance and implementation issues.
- The possible role of embedded devices, mobile communications devices, and personal computers to support authentication decisions.
- Risk assessments, including risk associated with data mining, social engineering, and of false positives.
- Attribution methods in general, that is, methods for associating characteristics with an entity

We welcome articles that address innovative conceptual, implementation, and experimental results relevant to authentication as well as articles addressing requirements, especially from potential users of authentication technology, are encouraged as well. Articles describing products or narrow/specific applications as well as largely theoretical articles are discouraged.

Submissions will be subject to peer-review. Articles should be 6,000 words, maximum, with a maximum of 15 references. Articles should be understandable to a broad audience of people interested in security and privacy. The writing should be down to earth, practical, and original. Authors should not assume that the audience will have specialized experience in a particular subfield. All accepted articles will be edited according to the IEEE Computer Society style guide.

www.computer.org/security/cfp

To submit a manuscript, please log on to Manuscript Central (https://mc.manuscriptcentral.com/cs-ieee) to create or access an account, which you can use to log on to *S&P*'s Author Center and upload your submission.