- PDF
- Send to a friend

What Would a More Secure Future Look Like?

Essay by David Clark, June 10, 2008

Most users of the Internet today would probably say that they are concerned about the state of Internet security. And they would probably be more concerned if they understood the true state of affairs. While many technical improvements have been added to the network over the last decade, many new attacks have been invented as well. More importantly, the motivation for the attacks has changed. The early history of attacks was almost playful, with the computer hacker as a symbol of rebellious technical mastery. Today, attacks are the business of organized crime and cyber-warfare. Attacks originate in parts of the globe with weak laws, little appetite for enforcement and little chance of extradition. Or they originate at the hands of “patriotic hackers”, who launch attacks that may or may not have official state backing.

The recognition that Internet security (or lack thereof) is the backdrop for large illicit profits and cyber-skirmishes should suggest that security is not purely a technical problem. But it is still easy to hope that with enough technical intervention, these problems can be deflected, if not cured. This is a misguided hope. Some of the current problems with the Internet are indeed technical flaws that can be mitigated with a technical solution. But many problems result from the nature of the Internet, and some result from the fact that users of the Internet are only human, and make human mistakes.

First, it is important to recognize how the nature of the Internet has both made it a success and made it vulnerable to malicious behavior. The Internet was designed to be open—open to innovation, to new applications, and to open communication among all parties. This “open by default” design means that it is very easy to try a new application, or to connect to another party anywhere in the world. On the Internet, an inventor does not have to negotiate with the Internet Service Providers to trial a new application, they “just do it”. But this open nature also leaves the network open to attack. We could imagine a very different sort of Internet, with more controls and more regulation. It might be safer. It might feel more like the global equivalent of a police state, with governments and other third parties everywhere watching what their users do.

Here are two specific examples that illustrate the benefits and costs of the open Internet. Today, the data sent across the Internet (the packets), carry a source and a destination address; from the addresses it is possible to surmise where in the Internet the source and the destinations are located. But there is no way that is easy or consistently reliable to map these addresses to the identity of the persons at the ends. So it is very hard to hold people accountable for what their computers have done. We could demand that all packets carry some non-repudiatable mapping back to a person who can be held accountable, but is this the online world in which we want to live? For another example, consider email, which was designed to allow anyone to send a message to anyone. The design did not require that the sender get a permit or a registered identity in order to send, or that the sender first get the permission of the receiver. So we get an open medium of interaction, and we get spam. We could have designed a “Victorian” email system in which you cannot talk to someone unless you have first been introduced. This approach would have excluded the spammers (unless they were clever social climbers), but again, is this restricted world the one we want?

So the starting point for improving the state of Internet security must be a social dialog, not just a technical dialog, about what sort of Internet we want. The challenge to the technical

community is not to build a very secure Internet—that might be more of a price than we actually want to pay. The challenge is to find clever ways to give us more security without taking away our freedom of action. And finding these better solutions will require a design process that involves both technologists and social observers, because it will take both technical imagination and social imagination to conceive of a different Internet from what we have today, more secure but still suited to our desires for open, diverse access.

Here, to stimulate our critical thinking, is just one example of a different Internet that has been seriously put forward as a contribution to better security. Imagine that there is not one Internet, but several of them, each of which is accessible from all of the machines connected at the edge. (In technical terms, these would be called virtual networks.) Different activities would be carried out on the different Internets. On some of them, you would, as today, need no permits or authentication in order to connect, but on one of them, intended for ecommerce, you would not be allowed to connect unless you identify yourself by giving a credit card as a form of identification. This approach to identification would exclude that vast segment of the population who have no credit cards. But, perhaps, since folks without credit cards cannot purchase anything, there is no reason to worry about excluding them. Or perhaps there is. And if this slice of the Internet, because it was “safer”, attracted more and more activity, those who have no access to a credit card would be excluded from more and more of the Internet’s activity. So perhaps this would be a bad road to start down. Or perhaps the bad consequences could be mitigated. This sort of analysis, trying to look into the future and see the consequences of our design choices, is both necessary and difficult, since there are so many stakeholders and so many paths to the future.

It is not clear where the locus of leadership should center as we work through these options. The problems are trans-national, so no one government can easily take the lead. The deliberation cannot be just populated by technologists, as I note, but must have strong and creative participation from technologists, because creative technologists can help us to imagine the space of the possible. We must not take the present form of the Internet as a given.

In the U.S., the National Science Foundation has challenged the research community to envision what the Internet of 15 years from now should be, and has reached out beyond the networking community to other parts of CS, and beyond that into the social sciences and the humanities to try to start a multi-disciplinary dialog about the future. Other countries have contemplated similar undertaking, and NSF has reached out to engage them. Perhaps this endeavor, which has an emphasis on better security, can be successful. But it is a significant challenge to build a lasting, multi-disciplinary conversation around difficult issues such as this, no matter how important.

David Clark *is currently a Senior Research Scientist at the* MIT Computer Science and Artificial Intelligence Laboratory*. Since the mid 70s, Dr. Clark has been leading the development of the Internet; from 1981-1989 he acted as Chief Protocol Architect in this development, and chaired the* Internet Activities Board*. He has also served as chairman of the Computer Sciences and Telecommunications Board of the National Research Council.*

All Security Essays

Anonymity

- Anonymity on the Web
  by The Cheshire Cat

Privacy

- The Right to Privacy. Again.
  by Dembitz

- On Technology, Security, Personhood and Privacy: An Appeal
  by John Clippinger

Protection from Harm

- What Would a More Secure Future Look Like?
  by David Clark

- Malware: The Great Equalizer
  by Beau Brendler

View all thematic areas »

Source URL: http://publius.cc/what_would_more_secure_future_look#comment-0