

We set up a poor Windows XP machine with no firewall or anti-virus software. Connecting it to the internet would be like throwing it into a lion pen with raw meat strapped to its hard drive.

How long would it be before we were hit by something nasty on the net? Hours, minutes?

As it turned out - eight seconds!

- BBC News, 8 April 2005

[http://news.bbc.co.uk/1/hi/programmes/click\\_online/4423733.stm](http://news.bbc.co.uk/1/hi/programmes/click_online/4423733.stm)

---

## Towards a More Secure Cyberspace

Steve Crocker

[steve@shinkuro.com](mailto:steve@shinkuro.com)

March 12, 2008

Revised very slightly for public dissemination March 18, 2008

I am here today presumably because I am one of the “old guys” who helped develop the Internet, or because I chair ICANN's Security and Stability Advisory Committee (SSAC), or possibly because I run a small company, Shinkuro, Inc. which has funding from the Department of Homeland Security to facilitate the deployment of DNSSEC, the security protocol for the domain name system. At the end of this short talk, I'll say a word or two about SSAC, but since this is an address to the Commission on Cybersecurity for the 44<sup>th</sup> President, I want to speak primarily about setting goals.

The largest portion of our nation's efforts to secure cyberspace are founded on two dismal assumptions:

1. Our systems are inherently insecure and there is nothing fundamental we can do about them, and
2. Therefore we must put all of our energy into band-aids, detection and reactive measures.

This is a failure of vision and will.

Modern computers and networks are large and complex, but they are nonetheless our

own technical creations. There is no fundamental reason they have to be so deeply flawed. Thus, the first step toward a more secure cyberspace is an adjustment of attitude and vision. It is possible to have a reasonably secure network where the bad guys do not have easy access to our systems and data.

This said, we have two major hurdles, one technical and one “organizational.”

The technical hurdle is the three way tussle between ease of use, speed to market and security. While it's possible to design systems which are both easy to use and secure, it's not always quick and easy to do so. Both the design and the implementation take a lot of work. Competitive pressures, combined with a tolerance in the market, generally result in ease of use and time to market winning out.

The organizational<sup>1</sup> hurdle is fragmentation of the market, with a relatively few large vendors controlling the standards and little pushback from the government or the users. As a consequence, each enterprise does what it can to protect itself – firewalls, configuration controls, intrusion detection systems, reporting and response systems – but there's no systemic improvements. The dominant vendors want to be paid to improve their systems. Small companies develop band-aid products and venture capitalists fund them because there's a market. People are making money with the current disorganization.

Is there a way forward? Yes, I believe so.

1. Set the right goals: Solutions which have it all: secure and fully functional and easy to use.
2. Fund research which leads in this direction. Limit funding for incremental improvements to the existing framework. Strive for significant improvements.
3. Take into account that introduction of new paradigms takes a lot of work and time. Fund transition and deployment efforts. Do the analysis and planning to create a virtuous cycle for adoption.
4. Work closely and cooperatively with other governments and organizations around the world. The U.S. cannot do everything by itself.

Let me translate these general statements into something specific in just one critical area. One of the biggest security problems in the Internet is distributed denial of service attacks. A flood of traffic directed at a specific site can effectively shut it down, even if the site is fully protected against penetration. These sorts of attacks take place quite

---

<sup>1</sup> I put “organizational” in quotes because it's not clear this is the right word. Perhaps a better term is socio-cultural or perhaps political-economic. In any case, we're clearly talking about a hurdle that requires the skills of social scientists and business leaders, not just computer scientists.

often. Only a few make the evening news. The attack last year in Estonia was one that did make the news, but most do not. Not uncommonly, attacks are threatened instead of actually carried out, and the victim is extorted. “Pay us or else we'll shut you down, perhaps at a particularly awkward time.”

Is it possible to change the game? I believe the answer is yes, although it will take some work. In terms of the four points I stated in general terms above, the agenda becomes:

1. Imagine – and set out to achieve – an Internet which does not provide an easy way to overwhelm a target site with unwanted traffic.
2. Fund research for the design of an Internet which meets this criterion. DDoS attacks either don't exist or don't have any impact.
3. Also fund research into the perhaps even harder problem of how to move from the existing operation to the improved system. The transition has to be incremental and not disruptive, even though the result will be “disruptively stronger.”
4. Work with other governments to establish a common set of goals in this area and cooperative mechanisms to combat DdoS attacks.

Since this talk is short, I won't try to lay out the available literature or the technical ideas that might lead to these results. For the purpose of this talk, it's sufficient to say there are reasonable ideas available.

Instead, let me return to my first point. Look at how the government is spending money on cybersecurity. In the Department of Homeland Security, there's work in two distinct components. In NCSD, a huge amount of money is being spent on industry coordination, computer emergency response centers, reporting, etc. An embarrassing pile of money was spent providing expensive T1 lines to each of the root servers. Very impressive, nearly useless, and utterly irrelevant in changing the game. Meanwhile, in the Science and Technology Directorate, the budget is small but the vision is much better. New technology and much stronger goals. The imbalance in funding and the imbalance in vision is telling. And the fix is reasonably simple: get people who believe it's possible to make a significant difference and that it's important to do so.

---

I promised to talk briefly about ICANN and SSAC. ICANN is a non-profit created to coordinate the domain name system and the addressing system for the Internet. The purview is limited and the authority even more so. That said, ICANN sits in a unique position because it functions as one of the few – perhaps the only – truly global organizations related to the operation of the Internet.

In our small, volunteer advisory committee on security and stability, we look at specific issues related to the domain name system and the addressing system, and we write reports, advisories and comments. One of our earliest and longest standing efforts is to assist in the adoption of the DNS security protocol, DNSSEC. We've been aided in recent years with funding from DHS S&T. It's slow going, which causes some to doubt its worth, but it's moving along step by step.

Let me close with a pointer to the committee's portion of the ICANN web site where the committee's work is documented <http://www.icann.org/committees/security/ssac-documents.htm> .