A Funny Thing Happened on the Way to the Marketplace

S.W. Smith
Dartmouth College

The security community tends to define problems and solutions in terms of technology. For example, giving your credit-card number to Amazon.com instead of an impostor is a problem, but clever use of public-key cryptography might be a solution; buffer overflow is a problem, but stack inspection tricks might be a solution.

However, real-world systems are more than just technology, and if we want to secure them, we also must consider their nontechnological aspects. In the May/June Secure Systems ("Humans in the Loop: Human–Computer Interaction and Security," p. 75), we considered human factors and usability issues. But before we can even get a chance to use technology, it must be in the systems that we use—it must succeed in the marketplace.

This installment of Secure Systems explores this marketplace dimension of building secure systems in the real world. Besides the technology, what else should we consider? Jothy Rosenberg, founder, CEO and CTO of Service Integrity, a Web-service monitoring and analysis software firm, and Adam Golodner, Associate Director for Policy at the Institute for Security Technology Studies, offered some insight into the subject.

Rosenberg departed early from the standard academic track to spend years in the trenches at several start-ups. Golodner has spent time in government and is now in academia examining public policy in relation to economic forces and security technology.

S.W. Smith: To start, we should consider what security technology is supposed to do. We must consider the trade-offs between the security goals we desire, the price we are willing to pay to achieve them, and the resources we expect adversaries to have.

Jothy Rosenberg: Too often, cryptographers and security developers keep working on something until they believe it is completely secure—forgetting along the way that they made it exceedingly complex and unusable. This is why people still use passwords—even though most people know passwords are not very secure, they are easy to use.

Secure sockets layer (SSL) is the only significant example of public key infrastructure (PKI) in use on the Internet because it is easy to use. Most of us who have analyzed SSL know that it is full of holes, but it is good enough. (Security technology always just has to be good enough to match the risk/cost of what might be lost/compromised.) Several things have been built with this in mind (such as limited liability on credit-card purchases) to make it work.

Smith: Adam, in your recent work, you've been looking at these issues from an economic perspective.

Adam Golodner: It is important to try to understand the way the marketplace works in security. Policy makers generally believe that if the market addresses a problem in sufficient time, the government should not intervene. Clearly, there are significant vulnerabilities and real costs to both individual firms and the economy, and we must identify current incentives for vendors, large users, and consumers to be either more or less secure.

If it appears that the market is working in a way that does not provide incentives to reduce vulnerabilities in a timely fashion, policy makers are likely to look at private-sector or public responses seeking to make us more secure. The bottom line is this: the way the marketplace and incentives work matters when deciding the proper course to address the security issue.

Smith: Jothy brought up SSL. Let's review what's happening when Alice directs her browser to https://www.foo.com/, and her browser's SSL icon indicates that it's a secure connection. Alice's browser and the server have carried out a "handshake" in which the server has proven knowledge of a private key and presented a certificate for the corresponding public key, correctly signed by one of Alice's browser's trusted roots.

But how do you get to be a trusted root? (Users can always add new ones, but that doesn't work for the mass market.)

Rosenberg: The entire SSL industry is about avoiding a nasty browser dialog that warns you not to trust a site.

That dialog is avoided if that site has a certificate from someone whose key is embedded in the browser. Because it takes three years from when a new browser version is released with a new key in its root store until that version is ubiquitous enough to cover 95 percent of the world's browsers, this is a significant issue.

In the early days, one or two "certificate authorities" (CA) issued SSL certificates. Browser manufacturers Netscape and Microsoft both wanted to promote more Web use, e-commerce, and browser downloads, so they were motivated to get the root keys of any CAs issuing SSL certificates into the browsers. This root key is the cryptographic magic needed to accept an e-commerce site's digital certificate credentials and not display the "lack of trust" dialog. But quickly, as more folks wanted to issue SSL certificates, it became clear that if browser vendors let weak CAs with poor authentication practices into the browsers, they could hurt overall trust in the Internet, and therefore hurt their own business goals. So both Microsoft and Netscape decided to tighten up the entry rules.

Netscape's approach was to charge money. If you as a CA could afford to pay the large amount of money to get your root pre-installed in the browser, you were probably serious enough to care about trust in the process; therefore, you're a good guy that should have a root in the browser.

Microsoft never charged money for pre-installed roots but tried to create barriers to ensure those roots' high standards for authentication of e-commerce sites applying for credentials. This proved too ad hoc of a process for Microsoft to manage fairly so they decided to find a third party to be the "bad guy"—to make the rules for those who qualified and those who did not. The third party, the American Institute of Certified Public Accountants (AICPA), represents over 300,000 auditors. They have standards for how financial (and other) audits, should be performed. So they started to come up with a CA audit. This created a new revenue opportunity for the AICPA and the auditors they represented because these audits cost at least US $100K and must be done annually. It got Microsoft out of the business of deciding who gets their root in the browser because they just required passing the AICPA audit. But politics still got the better of things because the stakes were so high. Some CAs tried to thwart the AICPA and control the rule-setting process until the US Federal Trade Commission and the US Justice Department started making inquiries about whether this standards process was open and fair.

Smith: Of course, a site that has a certificate doesn't necessarily mean it's the site users thought it was. A wonderful example of this was the https://palmstore.com site, which used to have a certificate that belonged to Modus Media, prompting those users who examined the certificate to wonder whether Palm had delegated to Modus Media (they had).

Rosenberg: If you go to ual.com, it is United Airlines' site. At least, we sure think so. It has United's logo and users can shop for flights. Once users find an itinerary they like and go to purchase it, the site continues to look like United with the same logos and design touches, but the browser's lock symbol lights up to remind us that the page is now secure to enter personal information. If you look at the certificate behind that lock symbol, you might be very surprised to find out that it is a certificate for ITN.net, and not United Airlines.

Does this weaken the very idea of SSL? Does it make people begin not to trust sites even when they use SSL? Why didn't United notify users that one of their trusted business partners managed the rest of the transaction?

Smith: We've both looked at ways of trying to make it easier for users to make a more reasonable trust decision. My efforts were in academia, but you were trying to sell a product (in a previous start-up). Can you tell us a bit more about TrustWatch?

Rosenberg: TrustWatch is an application implemented like a Google toolbar that users can download and install into their browser. It then tracks the sites that users browse. Each time the browser goes to a new domain, TrustWatch checks with a trusted third party to see if the domain is really what it purports to be. Now, when a site uses SSL—but especially when it does not—users have a higher assurance that this is the site they think it is. The browser designers could have done this in the United case, but chose not to.

If you mistyped a site name, TrustWatch would alert you that you were not where you thought. If someone tries to spoof a site—say AOL—and trick you into entering credit-card information, TrustWatch would alert you that you were not at AOL's site.

Smith: It's safe to say that we don't see TrustWatch in browsers. Why not?

Of course, a site that has a certificate doesn't necessarily mean it's the site users thought it was.

S.W. Smith

Jothy Rosenberg

The major players have a house of cards built up around SSL, the lock symbol, and people's trust.

Rosenberg: This is where the "catch-22" realities of the market come into play. Site owners need to see it in lots of browsers for it to be effective but people don't want to download it into their browsers until a lot of sites support it.

Smith: We had our own problems there, with our trusted-path patch to Mozilla to defend against Web spoofing. The student who led that work told me that it spanned too many modules, which required too many people to buy in. Jothy, you also had some other technology to address Web spoofing.

Rosenberg: Because the download is so hard to make happen, is there something "good enough" that is worth getting sites to use instead? TrueSite was an attempt to solve the "good enough" problem; it's a smart icon that might not be totally secure from purists' standpoint, but it might go a long way toward improving trust. When a site puts this smart icon on a page, browsers visiting the page must process an <IMG> tag that requires visiting another URL, which is an SSL trusted third party. Whenever this happens, the browser notifies this new site it is visiting via a "referring address" what address it came from.

The referring address is the URL of the site the browser was originally trying to visit. Referring addresses are important because they help companies such as Doubleclick determine whose ad it should display and who has clicked on one of its ads.

The referring address tells the trusted third party which smart icon is supposed to be displayed on the original page. It constructs that icon on the fly. (It's actually cached about every 10 minutes, so it can be rendered really fast.) The icon has embedded in it the site's name and its time of creation to prevent fraud of the icon itself.

If people learn to look for the icon on certain sites, the fact that it's not there should be an alert that this is not the right site (this, of course, requires that it have broad acceptance so that people look for it). If someone copies the page and displays it on a new domain, the icon will not display (or it will display a big "this site is pirated" icon) so simple site spoofing won't work.

Smith: Initially, you and I held different views here. I felt that this approach was sufficiently spoofable that widespread adoption would make users more susceptible to attack—and I'm sure you feel that's just another case of an academic looking at the wrong part of the trade-off curve. However, here again, surprising forces hindered market penetration, rendering this debate moot. What happened?

Rosenberg: Many site owners worried that getting the icon from a third party site would slow down page rendering. In fact, it didn't, because it was cached on very fast servers. Perception can be reality, and this was an uphill battle.

A worse problem was that TrueSite maintained the brand of a trusted third-party's name, logo, and color scheme, not that of the site owners. That made it less attractive to site owners. Many, if not most, sites worry about the color schemes and layout on their pages, and because they did not prepare for TrueSite's scheme, it didn't fit. In the end, the main reason for not putting the icon on site pages was that the color scheme did not fit with the site's look.

Smith: I don't think we teach students the importance of good color schemes when designing security technology! This reminds me of Carl Turner's study (cited in the May/June issue) showing that customer perceptions of how secure a Web site is correlated with how good its graphical design is. Cynically, we could suggest that the solution to this security problem is to fire the security staff and hire some good graphic designers. Of course, I think your cynicism here trumps mine.

Rosenberg: From the cynic's view, we can boil this down to an industry designed just to make sure one warning dialog in the browser is not displayed to average Web consumers. We are talking about the dialog stating that the site you're visiting is not trusted. The dialog is not displayed only if the root key that decrypts the signature on the SSL server certificate is pre-installed in the browser. Certificate authorities certify a site and issue them a signed certificate. These certificate authorities also must get the keys that sign those certificates pre-installed in the browsers.

The user interface could be more expressive, but we wonder if the major players want this. They have a house of cards built up around SSL, the lock symbol, and people's trust. They don't want to upset site *x* by making it clear that site *x* outsources to site *y*. Hundreds of sites do what United is doing; it would confuse consumers and confused consumers do not trust consumers or buying consumers.

Additionally, scaring people with statements about the prevalence of spoofing does not help get more people to spend more money over the Internet. No one wants to even talk about this topic, much less promote a download that helps people spot it. This is a true uphill battle until someone—either a major software vendor or e-commerce site—with a big name and strong brand decides to push it.

Smith: Is there any hope?

Rosenberg: When powerful vendors think nightly news stories decrease people's trust in the Internet as it exists today, they will finally change things. Browsers can change their user interfaces dramatically to improve understanding and trust but will only do so based on market pressure.

On a different note, Web services are a fairly new thing added to the equation. In the past, security focused on our networks and our "perimeters," as if our systems somehow mirrored our physical buildings. But Web services might force us to see that it was always about keeping information secure, not machines.

We must ensure that information only goes to whom it is supposed to and that it's kept safe and secure along the way. We know how to do that, but we have to make sure we are smart about how approachable we make our cryptography. Let's learn a lesson from the Web and make things secure enough with technology that people will really be able to use.

Smith: Adam, what do you see as the necessary next steps?

Golodner: We need to do a serious, fact-based analysis of the marketplace, and then draw conclusions about current incentives to ensure security. My initial read is that structural issues could help explain why the market has not addressed all vulnerabilities. I also think, however, that market-based incentives, if there, give some belief that the market's power might help reduce vulnerabilities over time.

From the big-picture perspective, this marketplace seems to have nontrivial externalities, free-rider problems, and coordination issues. These types of markets tend to leave a certain amount of consumer welfare unaddressed.

Smith: Can you explain some of these issues for the layman?

Golodner: Sure. An *externality* is something that happens to somebody else. So, although we might spend to protect ourselves, we might not spend so readily to protect others. If we believe it's in our interest to internalize this cost, or if we have to, then the incentives will change. For example, coal-fired plants in the Midwest will not readily stop emissions unless they have to, because acid rain is a harm that happens to someone else.

The *free rider problem* is people not pitching in but still getting the benefit because others have paid the tab. If one tier-one Internet backbone provider that peers traffic thought it could be more secure by investing another $2 billion dollars, the other providers would say "thank you very much," ride on that safer network, then try to win the investing companies' clients, using its lower-cost competitive advantage.

We need to do a serious, fact-based analysis of the marketplace, and then draw conclusions about current incentives to ensure security.

Adam Golodner

For coordination issues, think of creating a new public park. Try coordinating the thousands or millions of us it would take to sort out our contributions, particularly in a way reflecting the value to each of us, and the transaction costs of doing that.

So, even if we thought there was a way of increasing the level of security across information infrastructure, there might be existing structural conditions that indicate impediments to getting it done.

Smith: So, from the economic perspective, how do we get security into real systems?

Golodner: One way is to examine if there is competitive advantage in security. Vendors can and do compete on security. Users might gain a similar competitive advantage from security in their markets, whether autos, financial services, movies, or widgets. To the extent that being more secure gives you a competitive advantage over your market rivals—whether increasing productivity, avoiding catastrophe, reducing costs, or creating a new business model—you will have the incentive to get more secure. To the extent there is competitive advantage, it could alter behavior, lead to investing in security, and help require vendors to ensure security. Increasing the transparency of costs and effects on firms and systems might also help.

Smith: What if that doesn't work?

Golodner: Private-sector responses include contracts between parties, insurance, voluntary standard setting, competition, innovation, best practices, more transparency about harms, good corporate citizenship, and the bully pulpit. Others have discussed possible public responses that include regulation, new liability rules, mandatory standards, tax credits, more research and development funding, procurement policy, and, of course, the bully pulpit.

Each of these possible responses will have its own likelihood of efficacy, its own set of costs and benefits, and the intended and unintended consequences. We don't have the time to go through each one here, but I will say my own sense is that market responses are generally the most powerful, efficient, and efficacious way to address the issue. As a general matter, we still need to examine and set out more finely the way the market is working, along with some factual predicates on vulnerabilities and consequences before policy makers can feel confident that they would understand the effects of the possible public and private responses. We all have a lot of work to do.

Smith: Agreed! □

Jothy Rosenberg *is founder, CEO, and CTO of Service Integrity. Previously, he was employee 12 at MasPar Computer (Massively Parallel Supercomputers); VP of development at Borland Languages (Delphi, C++, and JBuilder boss); founder of Webspective (Web server monitoring and management); CEO of Factpoint (content security and fraud prevention); and founder, COO, and CTO of GeoTrust. He earned a PhD in computer science from Duke University, where he served as a research assistant professor. Contact him at jothy@acm.org.*

Adam Golodner *is currently Associate Director for Policy at the Institute for Security Technology Studies. Before coming to ISTS, he served in several policy positions in government. He also served on a number of technology policy boards such as the White House E-Commerce Working Group and the National Information Infrastructure Task Force. After working on technology, Internet, telecoms, and competition policy matters in government, he now tries to approach the security issue through the lens a policy maker who has to make some real policy choices. Contact him at adam.golodnder@dartmouth.edu.*

S.W. Smith *is an assistant professor of computer science at Dartmouth College. Previously, he was a research staff member at the IBM T.J. Watson Research Center, working on secure coprocessor design and validation, and a staff member at Los Alamos National Laboratory, doing security reviews and designs oratory for public-sector clients. He received his BA in mathematics from Princeton University and his MSc and PhD in computer science from Carnegie Mellon University. He is a member of ACM, Usenix, and the IEEE Computer Society. Contact him at sws@cs.dartmouth.edu or www.cs.dartmouth.edu/~sws/.*