Silver Bullet Talks with Steven Kent

Gary McGraw: What’s it been like to work on Internet security for so long?

Kent: Well, it’s certainly been a learning experience, for me and for many of the other folks who you’ve talked to in this series, as we’ve seen the environment evolve considerably. The problems we were trying to solve in the later part of the ’70s and into the early ’80s are much, much simpler conceptually than the challenges we face today. We had trouble even back in simpler times getting suitable mechanisms developed and engineered, and tremendous difficulty trying to deploy them. So that part has remained constant, unfortunately, but the challenges have grown immensely.

McGraw: The notion of secure transport is not exactly a new one. And even in the base protocols, we’re still having trouble getting adoption.

Kent: Yes, I’m proud, in some respects, of the kind of work that I was part of many years ago because we did a lot of this stuff in the early days. We did it under funding from DARPA, typically back in the early days at BBN. I was working on end-to-end encryption as an overlay, as something that you could slip in between IP and the TCP layers, much the way we do with IPsec today, and we had hardware to do this—and the first DES chips that were ever certified by what was then the NBS [National Bureau of Standards], now NIST.

[We also had] a system with key distribution centers and access controllers. I wrapped up performance measurements on that project in my first full year at BBN as an employee. Several years before project Athena at MIT started and Kerberos came along.

In those days, we were doing really cutting-edge stuff, and yet we couldn’t get it out into the mainstream, which has always been a disappointment.

McGraw: So I guess that leads to my next question, which you can dodge if you want. What role has politics played in accelerating or slowing down real security on the Internet?

Kent: Oh, I think in various ways, politics does enter into that as it intrudes into all aspects of our lives. Certainly, the export control regimes that were in place not only in the US but through a collection of countries—Western Europe as well as the US in the ’80s and into the first part of the ’90s—did have real effects on what we did. It had effects on the standards that we were developing in the IETF at the time. It impeded the progress and the deployment of the technology; however, we’ve seen all those Cold-War-era controls diminished very, very dramatically, and it hasn’t caused encryption to become a normal part of all the stuff that we do, with the exception of people using SSL for protecting credit-card numbers as they’re sent across the Internet. At the time, they’re probably the least vulnerable to the threat you should be worrying about. I mean, they’re in danger when they get to the other end.

McGraw: Exactly. And you know the risk management aspects of
About Steven Kent

Stephen Kent is the chief scientist of BBN Communications, a division of Bolt Beranek and Newman, where he’s been engaged in network security research and development activities for more than a decade. His work has included the design and development of user authentication and access control systems, end-to-end encryption and access control systems for packet networks, performance analysis of security mechanisms, and the design of secure transport layer and electronic message protocols. Kent has an SMEE and a PhD in computer science from the Massachusetts Institute of Technology. He’s the chair of the Internet Privacy and Security Research Group and a member of the Internet Activities Board.

Interview

credit-card stuff are almost all back end, yet we spend all this time worrying about the transport level for that stuff.

Kent: Right. I think what happened there is that the technology was applied at the one place in the system where it was easiest to deploy through browsers and by selling service certificates to people to give a perception to the consumer of security so that they would be more comfortable doing online purchases or online banking.

It’s been reasonably successful as a perception Band-Aid, but as you certainly know and you’ve told your readers about, this isn’t getting at the area where the real problems exist; that’s a lot harder. So, it’s unfortunate, but true.

McGraw: Do you think that the diminishing influence of the Cold War export controls, now that they’re gone, I mean—what is holding IPsec back? Even in the last two or three years, there seemed to be kind of a new groundswell, and then it disappeared.

Kent: Of course I have an emotional attachment to [IPsec] as the principle author of those standards. The good news is that it’s very widely available because it ships in every operating system out there and has for several years, but the bad news is, people almost never turn it on.

There are several very legitimate reasons for that. One is that IPsec, unlike TLS, isn’t just a protocol that provides you with confidentiality and integrity and authentication. It provides access control and that’s its fundamental feature. Access control requires management, and doing that management well requires discipline. Users are short on discipline.

McGraw: There you go. So, it’s a human nature problem.

Kent: It’s a human nature problem in terms of home use, let’s say. In a corporate environment, my perception is that today, despite what we know, most corporate IT security folks believe and focus heavily on perimeter security—firewalls, IPS, et cetera. The notion of encrypting traffic internally within their network strikes them as a lot of work and not worth the benefit in terms of encountering any perceived threats, even though, of course, it’s not just encrypting the traffic, it’s providing that access control, which would help prevent the spread of malware under the right management controls.

It’s similar in some regards to the use of secure email. When we did the early work for Privacy Enhanced Mail at the end of the ’80s and into the early ’90s, it took us a while, but we did a reasonable job of working our way through the technical issues, and what we didn’t really appreciate in terms of a barrier to deployment is that if you issued certificates to people, you had to make them available to other folks in order to allow encrypted—not just digitally signed—messages to flow freely. That directory problem of making that information available prevented widespread deployment because organizations didn’t want to have those directories externally available to the rest of the world because of spam and because of providing tremendous input to headhunters.

Those things that are part of the overall system for deployment and success tend to be significant road blocks, and IPsec encountered some of that. S/MIME has certainly encountered that. It’s been an issue.

McGraw: Yep, there’s a new barrier for S/MIME because Thawte disappeared last month, and now if you want to get a certificate, you’ve got to buy one from VeriSign.

Kent: Well, you can make up your own certificates.

It’s all a question of who you want to talk to and how you’re going to bootstrap. But you’re right, the folks at VeriSign have essentially cornered the market—tremendous amount of mindshare there, even though you can go to Go Daddy and get a certificate for your website for not much more than you’re paying for your website. But yes, the thing that we’ve missed is a tremendous opportunity to tie certificates into Domain Name System management.

McGraw: I agree with that completely.

Kent: If we had just done that, it would be a distributed system. We wouldn’t have a monopoly player in the marketplace, and because most of what we want in the way of certificates are the ones that on an everyday basis are tied to their domain names, it would be an ideal match up, but we didn’t do that.
**McGraw:** Alas.

When you began your work in Internet and applied security in 1978, I guess you were an intern back then. Did you anticipate making a career out of it?

**Kent:** The way I got involved is I showed up at MIT in the fall of '74 as a graduate student, and I wanted to do operating system stuff. I wound up being connected with the research group at what was then Project MAC [the Project on Mathematics and Computation]. Historically, the Multics group, although I hadn't realized at the time, was very heavily focused on operating system security issues. While I was attached to that group, I began to look for a master's thesis topic, and the head of that group, Jerry Saltzer, pointed me to work that was happening in that time frame—the early days of cryptography coming out from behind the door and appearing in the public literature, the IBM work on Lucifer, the call for the development of a data encryption standard before the specific algorithm was chosen that became DES.

He said, “Gee, people are saying that as soon as this becomes public, and we have a standard for the people who make chips, this will solve a whole bunch of problems,” and he suggested that there might be a little more to it than that and that there would be a thesis topic lurking in there.

**McGraw:** Just one?

**Kent:** I said, “Okay, boss, sure.”

So I started looking into the area and published my master's thesis a couple of years later, which was, to the best of my knowledge, the first public treatment of the issue of how to integrate crypto into operating system environments. It explored lots of the issues that I went into in more detail and later worked on in the '80s and '90s.

**McGraw:** So you just never got done with your thesis is the real answer.

**Kent:** I never did what I thought I was setting out to do, but the things that I've done instead have all turned out to be enjoyable and exciting and certainly a learning experience.

**McGraw:** I want to talk about applied cryptography a little bit more because we all know it can be difficult and really challenging to do properly. We talked about the commercial space a bit, but I wondered if you could talk about the major differences in fielding reasonable crypto in a military setting versus a corporate setting.

**Kent:** There are a lot of big differences. Historically, the military, whether it's US or others, has relied on hardware crypto. Even today, that's the major focus if you're serious about protecting classified information. The motivation for that is that you can have confidence if you build a box and engineer it very carefully and vet it very thoroughly so that it's going to do what you thought it was going to do, and you don't have to worry about all the software on somebody's server or their laptop or their desktop machine undermining your confidence in the crypto doing its job properly.

The commercial sector, to the extent that it does cryptography (with a few exceptions), focuses almost exclusively on software-based crypto, and that means that there is enormous difference in terms of the assurance that you can have that the crypto that you're using is doing what you expect it to do, is not being bypassed.

Now, there are exceptions. The folks at NIST have done a fabulous job in my opinion with the FIPS [Federal Information-Processing Standard] 140 series of evaluation criteria for crypto modules, which can apply to both software and hardware, and certain sectors of industry do emphasize using FIPS-evaluated hardware modules. I think that's been a very successful program.

I was able to learn about how well it works when I served as an external reviewer for the security lab at NIST on a few occasions over the years. They have great statistics showing that, of the products that are brought to them for review—and, presumably, a company that's bringing the products to a laboratory that's certified by NIST to do this review thinks they're going to pass, because otherwise you're wasting your money—a very high percentage of those products have security-significant errors in the documentation associated with the product. Even if you never think anyone reads the user's manual, it's not quite so big a deal, but, still, it's worrisome. A significant percentage, maybe 30, 40 percent, have security flaws that are detected in the course of the evaluation procedure and thus are remedied before they get the seal of approval. Those are all products that would have been out on the market touting that they provided good security, when in fact they didn't.

**Historically, the military, whether it’s US or others, has relied on hardware crypto. Even today, that’s the major focus if you’re serious about protecting classified information.**

One of the things that we did at BBN in the '90s was to build a crypto module specifically for use with public-key certification au-
thorities. It was the first module evaluated under FIPS 140-1 level 3. It was a little difficult being a pioneer, getting the errors, but it didn’t cost an arm and a leg.

It was reasonable for what we were doing. Even in our stuff, they found some bugs that we were able to remedy very easily and quickly, but it was an excellent process, so that’s one of the few examples that we can point to in the security community of a product evaluation process that has been extremely successful. It’s not overly long. It’s not unduly expensive or burdensome, and the results are very, very good.

**McGraw:** So, one might argue that that’s because of the limited nature of the target of evaluation, and when it comes to modern software—like these ridiculously massive distributed systems we’re building—that even the same very reasonable approach just doesn’t scale, and that’s the challenge we all face when it comes to trying to make software work, for example.

**Kent:** Absolutely. I agree that it’s successful because it has modest, though important, goals and well-defined boundaries. An individual operating system, even on my laptop, is so dramatically more complex that it’s qualitatively different, not just quantitatively different. Then when you expand that, as you were saying, to distributed system environments, we don’t even know what we’re doing, and so trying to achieve a reasonable level of assurance in those environments is a tremendous challenge. We’re not up to it yet.

**McGraw:** Let’s talk about another aspect of a system that doesn’t seem that complicated, but it’s super critical—BGP [Border Gateway Protocol], which has been lambasted for years as sort of the Achille’s Heel of the Internet—both via Black Hat presentations and the famous L0pht claims regarding taking down the Net in 30 minutes. Are things getting any better?

I know you worked on S-BGP and PKI and Attestation for BGP; what’s the deal?

**Kent:** Well, we’re making real progress there, although it has been a very, very slow process. The S-BGP work that we did not quite a decade ago was useful in terms of exploring what sorts of security assurances one could try to provide in that environment and was guided by a very old principle, the principle of least privilege. [There’s] a saying, “On the Internet, nobody is in charge.” Each autonomous system is being operated by an entity who takes that word “autonomous” very seriously, so the best you can do when they make announcements about routes on the Internet is that you can verify that the announcements they’re making are ones that they have transitively been authorized to make.

That’s about it. We come nowhere close to it in today’s system, and this allows things like the Pakistani YouTube hijacking [in 2008] to occur.

**McGraw:** Or BGP eavesdropping, which is something that I guess you anticipated far before the Black Hat guys.

**Kent:** We had anticipated that would be an issue, because for the S-BGP work, we said, sure you could do this, and at one point, somebody said, “Are you sure?” And I said, “Yeah, we could show you,” and we did a very brief demo with part of our own address base just to show people that it could be done.

The trickier part is not getting the traffic to come to you but getting it to go through you and then to the real destination.

**McGraw:** Exactly. The pre-pending things was very clever.

**Kent:** If you have to convince somebody of that—by showing them, by doing an experiment—you do it, but we’re not looking to point out vulnerabilities to the world in general. This was just trying to convince people that it’s a serious problem, and they should fund it, so we presented it to people and showed them it was a serious problem.

**McGraw:** I have a question about that, about your view of sharing ideas inside of, say, the DoD [US Department of Defense] and the national security establishment versus publicizing things. What causes better security results in your decades of experience?

**Kent:** I think that’s a tough one. I have some sympathy for researchers who have discovered vulnerabilities, bring them to the attention of vendors, quietly saying, “Hey, this is an issue, and you really ought to fix it,” and then become frustrated by what they see as complete inaction on the part of the vendors to fix the problems. Once you get to that point, then the question is, what do you do to try to make sure this is fixed?

I don’t want to comment on the “Is it appropriate to go public with this to force the hand of the vendor to do it?” question. Should you be going to the CERT and trying to hit them to enter the fray and put pressure on the vendor? I really don’t often find myself in that position. I am usually looking at issues on behalf of government clients and saying, hey, there is a concern here, and you guys really need to either tell the vendor that you aren’t going to buy more of this if they don’t fix the problem, or you have to put in some remedial measure to deal with it because you can’t get the vendor to fix it, or it’s just going to take too long or whatever. I don’t tend to find myself in those positions and, since I don’t, I don’t think it’s fair
for me to talk about what’s a good or bad way to do this.

McGraw: Well, you know, I think that’s a very rational response, and frankly the one that almost all research scientists like you have, so it’s an important opinion for some of the other guys, the so-called “researchers,” to have a view of.

Kent: Getting back to the BGP stuff, the one thing I would like to say is that we are making very big progress in the following sense: we have gotten the IETF to establish a working group that’s establishing standards for securing BGP and, in particular, is focusing initially on creating a public-key infrastructure that will issue certificates to the holders of address space throughout the worldwide Internet. Of course, it’s nice to have standards for this, but if the people who are responsible don’t do it, then you’re losing; fortunately, all of the regional Internet registries, all five of them around the world and the IANA [Internet Assigned Numbers Authority], have all signed onto this. In fact, they published a declaration to say that they would have operational capability by the beginning of 2011.

McGraw: Oh, that’s great!

Kent: Some of them are already doing this on a prototype or testbed basis. Some of the regional registries are doing it, so it’s taken a lot of work. You’re getting these people to devote their resources to this, so they have to believe it’s a reasonable thing to do with the funds that their members—ISPs—give them, so that’s encouraging.

It’s just going to be a first step, if people do this. If ISPs make use of the data, then the simple kinds of hijacks, which may be purely benign even though they have terrible effects, could be prevented just by doing this first step. It doesn’t deal with the more insidious kinds of attacks that we’ve talked about, but it would get rid of all of the “Oh, I fat-fingered this, and that’s why I’m sucking down all this traffic that I shouldn’t be” issues.

If you can get rid of that, it does tend to emphasize that anything else that’s still happening is more likely to be malicious, and that in itself is beneficial.

McGraw: What are your feelings and thoughts about security and individual liberty? I know you testified in Congress on behalf of the NRC [US National Research Council] about ID systems and the challenges technically posed by those, but as a person who has thought about this very carefully, I’m interested in how you come down on that issue.

Kent: I think that people should have the ability to control when they’re disclosing identity information in the various kinds of transactions in which they engage. We wind up having to demonstrate who we are a lot more today than we used to, say, pre-9/11. That’s a fact of life on a worldwide basis. I do a lot of travel—as you do—so you just recognize that you have to do that.

But in the online environment, we need to give individuals appropriate controls, things that are understandable and manageable for them to decide—when they’re going to disclose identifying information, credit-card numbers, things of that sort. It’s easier in many cases for the consumers of the information (not the users as consumers but the companies, merchants, and so on) to want to request all sorts of stuff that they don’t really need.

McGraw: The marketing people love it.

Kent: The marketing people love it, absolutely … the numerati, the data mining folks. But I think that the problem we face here is that we can come up with lots of technical means of doing it, but people have a natural tendency to go for what is most convenient and easiest for them to use, not surprisingly.

McGraw: Right.

Kent: We fail to provide controls that make it easy for people to behave in a privacy-preserving fashion. That is, so far, the exception rather than the norm. But we lose personal privacy unnecessarily as a result.

McGraw: My view is that the Europeans are doing a better job with that, and, in fact, a recent study we did about the European software security initiatives versus the US shows a larger emphasis on privacy, just because it’s part of the culture over there [BSIMM Europe; http://bsimm2.com].

Kent: Absolutely, European privacy controls are much more stringent that those in the US. The US is pretty good in terms of personal liability for electronic transactions than you are in many European contexts (and certainly in the UK from what I’ve read), but on the privacy front, I agree with you entirely that the European Commission has done a much better job. People are more serious about it. They pay a lot of attention to it, which we don’t tend to do over here.

See the full text of this interview at www.computer.org/cms/Computer.org/dl/mags/sp/2010/03/extras/msp2010030005s.pdf.

Gary McGraw is Cigital’s chief technology officer. He’s the author of Exploiting Online Games (Addison-Wesley, 2007), Software Security: Building Security In (Addison-Wesley, 2006), and seven other books. McGraw has a BA in philosophy from the University of Virginia and a dual PhD in computer science and cognitive science from Indiana University. Contact him at gem@cigital.com.