Trusting Bad Code from Day One

Vint Cerf is often called the “father of the Internet.” Together with Bob Kahn, he created TCP/IP, the protocol that routes Internet traffic, in 1973. When interviewed several years ago about TCP/IP, Cerf admitted: “We never got to do the production engineering.” In software design language, this essentially means: “We never got out of beta.” That is, some crucial features that were needed did not make it into the protocol that the world runs on now. Cerf explained: “My thought at the time, thirty-five years ago, was not to build an ultra-secure system, because I couldn’t even tell if the basic ideas would work.”

The focus at the time, since it was an ARPANET Defense project, was on fault tolerance, not security. The message was supposed to automatically reroute network packets around atomic bomb blast sites, not protect a user against identity theft or keep hackers out of a user’s network.

Cerf has stated many times over that the only way the Internet is going to be truly secure is to rebuild it from the ground up. That is difficult, but can it be done? Absolutely. But doing so will take worldwide agreement, then a lot of time, and then a lot of money. Looking at the state of the planet, I’m doubtful this will ever be done—especially since some powerful players would prefer for things to stay as is, because they have access to everything now.

Still, there are security technologies that are far superior to what is being used today. Why are they not being deployed? The answer has to do with people, not technology. Hackers and the U.S. National Security Agency (NSA) are far ahead in their offensive technology; they can essentially break into any piece of code. And then there is that pesky end-user. Machine-to-machine communications are easy, but once you throw in hundreds of workstations, dozens of servers, and thousands of devices and apps that are being driven by humans, things get very messy, very quickly. Fancy mathematical security algorithms start to break down or become overwhelmed.

NSA Monitoring

CafePress is featuring T-shirts with the following text: “NSA, the only part of government that actually listens.” As Cerf stated, the basic transmission protocols were not built with security in mind. This allows organizations with access to centralized Internet traffic hubs—organizations such as the NSA—to hoover up whatever data they deem to be critical. The problem is that if one organization can do this, others might follow soon after, and then the genie is totally out of the bottle. The NSA claims that it “touches” only 1.6 percent of daily Internet traffic.

If the net carries 1,826 petabytes of information per day, then the NSA “touches” about 29 petabytes a day. IT pros are very interested in what “touches” actually means. Analyzes? Stores (for how long)?

Let’s dig a little bit deeper into that 1.6 percent that the NSA claims to touch. First of all, most data traffic is not e-mail or web pages: 62 percent of North American traffic is real-time entertainment; another 10.5 percent is P2P file-sharing. So the NSA is not looking at 72.5 percent of the data. Web browsing is only 11.8 percent of aggregated upstream and downstream traffic. Communications make up just 2.9 percent. Thus the 1.6 percent of net traffic that the NSA touches would be roughly half of the actual e-mail traffic on the net. But if we consider that according to some estimates, about 80 percent of e-mail traffic is spam, which the NSA surely filters out, it is highly likely the organization touches all e-mail traffic in North America.

Potential Threats

With the NSA building a huge facility in Utah, where it can store this type of information indefinitely, we can imagine the risks. Government organizations simply have a bad record regarding data breaches: an abundance of records have been stolen by a variety of hackers in the last few years. The hacking of millions of tax-payer records in South Carolina is a good example. Not surprisingly, many U.S. citizens are very concerned about their financial stability and about government records falling into the wrong hands. If one’s personal confidential records are freely bought and sold in a flourishing criminal underground economy, there is possible exposure for many years into the future.

But that is not all. Once a government agency has ten, fifteen, or twenty years of personal e-mail stored, it can run algorithms that reveal a wealth of private information. For instance, Artificial Intelligence software applications can look at e-mail and closely approximate political convictions, sexual orientation, degree of agreement with current political administrations, potential for violence, potential for anti-social behavior, and any other specific trait.

The potential for abuse is horrifying. The recent scandals of the IRS seeking out specific organizations and treating them differently based on their political orientation are child’s play compared with what the NSA could potentially come up with based on personal e-mail stored for decades. Even sending everything with strong open-source encryption is not safe. The NSA has already broken most encryption, and if not, it can simply store encrypted data until it has broken the encryption.
and then go back and decrypt the “safe” communication. Moreover, encrypted data stands out like a sore thumb, meaning that encrypted e-mail paints a bright red target from the get-go.

The Old Way and the New Way
Remember the old days when security standards were created by a large body of experts? Government, in cooperation with large companies, threw a lot of resources at the efforts, and two to three years later, we had a new standard. But now, with large amounts of money being paid for 0-day vulnerabilities, hackers make security standards obsolete even before the standards come out. The game has changed completely. There are dozens, if not hundreds, of 0-day vulnerabilities in almost all applications.

There is a fundamental difference between cybersecurity and almost any other technology. The more people know about cybersecurity, the less secure we are. People have a choice to become a white hat or a black hat, and at the moment the dark side pays a lot more. In some Eastern European countries, the dark side is the only game in town. Continuing to fix vulnerabilities with regular patching is at best a Band-Aid—and an expensive one at that. There is always the risk that a hacker will get into a network before the patch can be applied. And of course, there simply is no patch for 0-day vulnerabilities.

The time has arrived to pay the piper. For forty years, we have trusted code that was never designed to be secure. It is time for higher education institutions to start using defensive technology that will truly keep out attackers. Doing so begins with taking a good look at the institution’s defense-in-depth and, at the very least, becoming a hard target to penetrate. I would also advise that institutions consider using Application Control (a.k.a. whitelisting), which is a technology that turns the antivirus strategy on its head. Whereas antivirus keeps the bad guys out, Application Control allows only known good code to run and denies everything else by default. It’s a bit more work, but it’s a lot safer. Last but not least, institutions need to realize that end-users are the low-hanging fruit that criminal hackers use to break into a network via social engineering tactics. Institutions should thus start immediately with effective security awareness training.

Notes

Stu Sjouwerman (stu.sjouwerman@knowbe4.com) is the founder and CEO of KnowBe4 (http://www.knowbe4.com/), which provides web-based Internet Security Awareness Training (ISAT) to small and medium-sized enterprises.

© 2013 Stu Sjouwerman