Bruce Schneier
Resilient Systems

Cryptography Is Harder than It Looks

Writing a magazine column is always an exercise in time travel. I'm writing these words in early December. You're reading them in February. This means anything that's news as I write this will be old hat in two months, and anything that's news to you hasn't happened yet as I'm writing.

This past November, a group of researchers found some serious vulnerabilities in an encryption protocol that I, and probably most of you, use regularly. The group alerted the vendor, who is currently working to update the protocol and patch the vulnerabilities. The news will probably go public in the middle of February, unless the vendor successfully pleads for more time to finish their security patch. Until then, I've agreed not to talk about the specifics.

I'm writing about this now because these vulnerabilities illustrate two very important truisms about encryption and the current debate about adding back doors to security products:

1. Cryptography is harder than it looks.
2. Complexity is the worst enemy of security.

These aren't new truisms. I wrote about the first in 1997 and about the second in 1999. I've talked about them both in *Secrets and Lies* (2000) and *Practical Cryptography* (2003). They've been proven true again and again, as security vulnerabilities are discovered in cryptographic system after cryptographic system. They're both still true today.

Cryptography is harder than it looks, primarily because it looks like math. Both algorithms and protocols can be precisely defined and analyzed. This isn't easy, and there's a lot of insecure crypto out there, but we cryptographers have gotten pretty good at getting this part right. However, math has no agency; it can't actually secure anything. For cryptography to work, it needs to be written in software, embedded in a larger software system, managed by an operating system, run on hardware, connected to a network, and configured and operated by users. Each of these steps brings with it difficulties and vulnerabilities.

Although cryptography gives an inherent mathematical advantage to the defender, computer and network security are much more balanced. Again and again, we find vulnerabilities not in the underlying mathematics, but in all this other stuff. It's far easier for an attacker to bypass cryptography by exploiting a vulnerability in the system than it is to break the mathematics. This has been true for decades, and it's one of the lessons that Edward Snowden reiterated.

The second truism is that complexity is still the worst enemy of security. The more complex a system, the more lines of code, interactions with other systems, configuration options, and vulnerabilities there are. Implementing cryptography involves getting everything right, and the more complexity there is, the more there is to get wrong.

Vulnerabilities come from options within a system, interactions between systems, interfaces between users and systems—everywhere. If good security comes from careful analysis of specifications, source code, and systems, then a complex system is more difficult and more expensive to analyze. We simply don't know how to securely engineer anything but the simplest of systems.

I often refer to this quote, sometimes attributed to Albert Einstein and sometimes to Yogi Berra: "In theory, theory and practice are the same. In practice, they are not."

These truisms are directly relevant to the current debate about adding back doors to encryption products. Many governments—from China to the US and the UK—want the ability to decrypt data and communications without users' knowledge or consent. Almost all computer security experts have two arguments against this idea: first, adding this back door makes the system vulnerable

Copublished by the IEEE Computer and Reliability Societies
1540-7993/16/$33.00 © 2016 IEEE

to all attackers and doesn't just provide surreptitious access for the "good guys," and second, creating this sort of access greatly increases the underlying system's complexity, exponentially increasing the possibility of getting the security wrong and introducing new vulnerabilities.

Going back to the new vulnerability that you'll learn about in mid-February, the lead researcher wrote to me: "If anyone tells you that [the vendor] can just 'tweak' the system a little bit to add key escrow or to man-in-the-middle specific users, they need to spend a few days watching the authentication dance between [the client device/software] and the umpteen servers it talks to just to log into the network. I'm frankly amazed that any of it works at all, and you couldn't pay me enough to tamper with any of it." This is an important piece of wisdom.

The designers of this system aren't novices. They're an experienced team with some of the best security engineers in the field. If these guys can't get the security right, just imagine how much worse it is for smaller companies without this team's level of expertise and resources. Now imagine how much worse it would be if you add a government-mandated back door. There are more opportunities to get security wrong, and more engineering teams without the time and expertise necessary to get it right. It's not a recipe for security.

Unlike what much of today's political rhetoric says, strong cryptography is essential for our information security. It's how we protect our information and our networks from hackers, criminals, foreign governments, and terrorists. Security vulnerabilities, whether deliberate back door access mechanisms or accidental flaws, make us all less secure. Getting security right is harder than it looks, and our best chance is to make the cryptography as simple and public as possible. ■

Bruce Schneier is the CTO of Resilient Systems. His new book is *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World.* Contact him via www.schneier.com.