Schneier on Security

← DVD Encryption Broken The 1999 Crypto Year-in-Review →

A Plea for Simplicity

You can't secure what you don't understand.

Bruce Schneier
Information Security
November 19, 1999

Ask any 21 experts to predict the future, and they're likely to point in 21 different directions. But whatever the future holds--IP everywhere, smart cards everywhere, video everywhere, Internet commerce everywhere, wireless everywhere, agents everywhere, AI everywhere, *everything* everywhere--the one thing you can be sure of is that it will be complex. For consumers, this is great. For security professionals, this is terrifying. The worst enemy of security is complexity. This has been true since the beginning of computers, and it's likely to be true for the foreseeable future.

We all know the amount of testing that goes into any major software product, and we all know the number of bugs that still slip through. The testing process--implement, test, fix, test, repeat--is imperfect, but it's the best we've found. Security doesn't lend itself to this process, because security properties cannot be "tested" in the same way as functional properties. Products are useful for what they do, while security products are useful solely because of what they *prevent* from being done. A security product may work fine, but you have no idea if it is secure. No amount of beta testing can uncover a security flaw. Ever.

The only way to evaluate the security of a system is to analyze it. This is a time-consuming and expensive process, and almost no one bothers to go through it. If they did, they would quickly realize that most systems are far more complex to analyze, and that there are security flaws everywhere.

We've seen security bugs in almost everything: operating systems, applications programs, network hardware and software, and

security products themselves. This is a direct result of the complexity of these systems. The more complex a system is--the more options it has, the more functionality it has, the more interfaces it has, the more interactions it has--the harder it is to analyze. Everything is more complicated: the specification, the design, the implementation, the use. And everything is relevant to security analysis.

This complexity isn't limited to single systems, but includes interactions *between* systems as well. For years we knew that Internet applications like sendmail and rlogin had to be secure, but the recent epidemic of macro viruses shows that Microsoft Word and Excel need to be secure too. Rogue printer drivers can compromise Windows NT. Malicious attachments can tunnel through firewalls. Maintenance ports on routers can compromise networks, as can random modems. DSL and satellite modems can completely compromise security. So can Java or Microsoft Outlook. Or your recycling bin.

The networks of the future will be necessarily more complex, and therefore less secure. The technology industry is driven by the demand for features, for options, for speed. There are no standards for quality or security, and there is no liability for insecure software. Hence, there is no economic incentive to build in high quality. In fact, it's just the opposite. There is an economic incentive to create the lowest quality the market will bear. Unless customers demand higher quality and better security, this will never change.

I see two alternatives. The first is to recognize that the digital world will be one of ever-expanding features and options, of ever-faster product releases, of ever-increasing complexity and of ever-decreasing security. This is the world we have today, and we can decide to embrace it knowingly.

The other choice is to slow down, simplify and try to add security. Customers won't demand this--the issues are too complex for them to understand--so a consumer advocacy group is required. This solution might not be economically viable for the Internet, but it is the only way to get security.

BRUCE SCHNEIER*is CTO of Counterpane Internet Security Inc., a company trying to bring managed security solutions to complex networks. He writes the CryptoRhythms column for* Information Security*, and is the author of* Applied Cryptography *and the Blowfish and Twofish encryption algorithms.*

Predictions

- As systems get more complex, security will get worse.
- As systems become more interconnected, security will get worse.
- Unless manufacturers are held liable for security failures, security will get worse.
- The only long-term solutions are to either embrace insecurity or eschew "Internet-years" style complexity.
- In the short term, the best course of action for enterprises is to outsource security to companies that have the expertise to understand the systems being secured.

Categories: Business of Security, Computer and Information Security

Tags: Information Security
