Schneier on Security

The Security Mindset

Uncle Milton Industries has been selling ant farms to children since 1956. Some years ago, I remember opening one up with a friend. There were no actual ants included in the box. Instead, there was a card that you filled in with your address, and the company would mail you some ants. My friend expressed surprise that you could get ants sent to you in the mail.

I replied: "What's really interesting is that these people will send a tube of live ants to anyone you tell them to."

Security requires a particular mindset. Security professionals -- at least the good ones -- see the world differently. They can't walk into a store without noticing how they might shoplift. They can't use a computer without wondering about the security vulnerabilities. They can't vote without trying to figure out how to vote twice. They just can't help it.

SmartWater is a liquid with a unique identifier linked to a particular owner. "The idea is for me to paint this stuff on my valuables as proof of ownership," I wrote when I first learned about the idea. "I think a better idea would be for me to paint it on *your* valuables, and then call the police."

Really, we can't help it.

This kind of thinking is not natural for most people. It's not natural for engineers. Good engineering involves thinking about how things can be made to work; the security mindset involves thinking about how things can be made to fail. It involves thinking like an attacker, an adversary or a criminal. You don't have to exploit the vulnerabilities you find, but if you don't see the world that way, you'll never notice most security problems.

I've often speculated about how much of this is innate, and how much is teachable. In general, I think it's a particular way of looking at the world, and that it's far easier to teach someone domain expertise -- cryptography or software security or safecracking or document forgery -- than it is to teach someone a security mindset.

Which is why CSE 484, an undergraduate computer-security course taught this quarter at the University of Washington, is so interesting to watch. Professor Tadayoshi Kohno is trying to teach a security mindset.

You can see the results in the blog the students are keeping. They're encouraged to post security reviews about random things: smart pill boxes, Quiet Care Elder Care monitors, Apple's Time Capsule, GM's OnStar, traffic lights, safe deposit boxes, and dorm room security.

One recent one is about an automobile dealership. The poster described how she was able to retrieve her car after service just by giving the attendant her last name. Now any normal car owner would be happy about how easy it was to get her car back, but someone with a security mindset immediately thinks: "Can I really get a car just by knowing the last name of someone whose car is being serviced?"

The rest of the blog post speculates on how someone could steal a car by exploiting this security vulnerability, and whether it makes sense for the dealership to have this lax security. You can quibble with the analysis -- I'm curious about the liability that the dealership has, and whether their insurance would cover any losses -- but that's all domain expertise. The important point is to notice, and then question, the security in the first place.

The lack of a security mindset explains a lot of bad security out there: voting machines, electronic payment cards, medical devices, ID cards, internet protocols. The designers are so busy making these systems work that they don't stop to notice how they might fail or be made to fail, and then how those failures might be exploited. Teaching designers a security mindset will go a long way toward making future technological systems more secure.

That part's obvious, but I think the security mindset is beneficial in many more ways. If people can learn how to think outside their narrow focus and see a bigger picture, whether in technology or politics or their everyday lives, they'll be more sophisticated consumers, more skeptical citizens, less gullible people.

If more people had a security mindset, services that compromise privacy wouldn't have such a sizable market share -- and Facebook would be totally different. Laptops wouldn't be lost with millions of unencrypted Social Security numbers on them, and we'd all learn a lot fewer security lessons the hard way. The power grid would be more secure. Identity theft would go way down. Medical records would be more private. If people had the security mindset, they wouldn't have tried to look at Britney Spears' medical records, since they would have realized that they would be caught.

There's nothing magical about this particular university class; anyone can exercise his security mindset simply by trying to look at the world from an attacker's perspective. If I wanted to evade this particular security device, how would I do it? Could I follow the letter of this law but get around the spirit? If the person who wrote this advertisement, essay, article or television documentary were unscrupulous, what could he have done? And then, how can I protect myself from these attacks?

The security mindset is a valuable skill that everyone can benefit from, regardless of career path.

This essay originally appeared on Wired.com.

EDITED TO ADD (3/31): Comments from Ed Felten. And another comment.

EDITED TO ADD (4/30): Another comment.

Tags: essays, schools, security education, security mindset

Posted on March 25, 2008 at 5:27 AM • 90 Comments

Comments