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

David • **March 25, 2008 5:55 AM**

Bruce, can I use you as a reference when my wife looks at me strangely when I voice simlar thoughts?

Lynoure Braakman • **March 25, 2008 6:13 AM**

I think this way all the time. Hotels do a similar thing a lot: they ask you to leave your key at the reception, then give it, it the worst case, based on the room number alone. And the cleaning ladies often with hold a room door open for you if you approach it confidently.

Dave Walker • **March 25, 2008 6:25 AM**

Interesting that you've just posted this, especially since I've just read another article on the perceived parallels between the thinking processes required in security and the thinking processes required in formal mathematical analysis. You might like to have a look at it, at http://www.daemonology.net/blog/2008-03-21-security-is-mathematics.html .

Nick Lancaster • **March 25, 2008 6:48 AM**

Is it just security professionals, or can this apply to aspects of the beta-test/programmer community?

What little coding I did when working on an online game, I always beta tested from the perspective of 'how can I break this?' or 'how can I exploit this?'

As for the 'hotel cleaning ladies holding open the door,' that's simply deferring to authority. Unless they've seen you come out of another room, they really have no means of verifying your identity, and are responding to your manner. This plays out in other places, as well - you're likely to be the one people approach in a store, no matter how you're dressed, and asked, "Do you work here?" Or, in a crowded environment, people part to let you pass, because you are moving with intent. (That last drives my wife nuts, since she has to scramble to keep up with me - any gap closes behind me.)

Anonymous • **March 25, 2008 7:05 AM**

@David

"Bruce, can I use you as a reference when my wife looks at me strangely when I voice simlar thoughts?"

I've tried this and it doesn't work. Being security conscious means being a criminal, if only in one's head, and this spooks people.

John • **March 25, 2008 7:32 AM**

While not directly related to security, I would love to see this mindset applied to legislation.

All bills are just absolutely wonderful according to proponents. The question that is ignored is "how will this bill be misused?"

---

clvrmnky • **March 25, 2008 7:36 AM**

Case in point: http://www.boingboing.net/2008/03/25/fake-craigslist-ever.html

---

Fred P • **March 25, 2008 7:55 AM**

"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."

-I tend to disagree; good engineering requires one to think about various failures (intentional or non-intentional), and how to cope with those failures.

---

sooth sayer • **March 25, 2008 7:55 AM**

@Bruce .. it explains some of your diatribe against things that "normal" people won't think twice about. And frankly I will never think about sending a a tube of ants to someone I care or don't care about.

There is always Zprexa .. used to be that Prozac did the trick .. but the world has gotten to be a lot nuttier.

Nick Lancaster • **March 25, 2008 8:12 AM**

@John:

Is the tradeoff of such legislative design a restrictive environment where individuals are not trusted to decide or accept responsibility? I'm not sure that laws which assume you're not smart enough or honest enough to comply are an improvement.

YWo • **March 25, 2008 8:38 AM**

Fred P is correct. Petroski had a book about this (forget the title) that said engineering is about foreseeing failures in the engineering process.

So the premise fails. Everytime I hear the wornout line of "ooooh security guys and hackers see the worlds weaknesses" I think that is the equivalent of security-porn. Heaps of people in different jobs think this way, engineers, police officers to catch crooks, intelligence analysts, accountants doing your tax. Each of them think about failures in their particular domain, and probably take those failure-perceptions into other areas.

So please, the only reason the security guy/hacker world view is continued on blogs like this and others is to make you guys think that you are special and unique. You arn't.

DLL • March 25, 2008 8:46 AM

@YWo: I don't know where you hang out, but most of the people I know do NOT think this way. If engineers, police officers, intelligence analysts, and tax accountants really did think this way, the world would be a very different place. Who would the TV reporter interview at the airport security check if everybody was in on the joke?

Anonymous • March 25, 2008 8:56 AM

RE: Hotels

I've stayed at quite a few hotels and have had different experiences, when I walked in my room when the cleaning lady was there (door was open) she asked for my room key and made sure it worked in the door. This hotel also required your roomkey to use the elevators.

At another hotel when I've lost my roomkey, a photo ID was required to retrieve it. These were upper class chain hotels acustom to business travellers tho, not sure how it would be for other hotels.

---

jayh • March 25, 2008 9:03 AM

There is the human factor too. We are social animals, we respond to cooperation, and, at least within our own group, do not want to be constantly 'on guard', thinking the worst. We seek out environments and people where we can trust, can let our guard down. (how often have you heard people yearning for a place where you 'don't need to lock your doors')

It starts to come down to tradeoffs. How much risk are you willing to take. Do you really want steel bars on your home? I don't always lock my car (hell during the summer it has neither roof nor windows), thought I will usually pop off the radio face plate and lock that up. To view every possible security threat at every possible time would result in paranoid, crippling life style.

Albatross • March 25, 2008 9:12 AM

My very first experience programming, well aside from toggling in the boot sequence on a PDP 8L (IIRC), was discovering that I could alter the BASIC code of the Lunar Lander program on the mainframe shared by all the schools in my state. Remember Lunar Lander?

M--------L

The first thing I discovered was I could change the lander symbols

)----->

Then I discovered I could alter the If-then statements for landing conditions, and (being 15) I quickly coded all sorts of horrific disasters as consequence for different landing velocities.

The 110-baud dial-up modem connection I was using kept disconnecting, which inspired me to add a randomly accessed subroutine that simulated a disconnection, then simulated a login sequence, and wrote the entered usernames and passwords into a file. After that the program ended, dropping you at the OS prompt where you would expect to be after login.

I collected a LOT of usernames and passwords...

Then there was the time that I worked for an energy-management firm, responsible for heating and cooling public and private buildings. I noticed that anyone could phone the 300-baud modem connected to the mainframe and immediately connect, with no password. I pointed out to my boss that one could disable the alarms on a school boiler, shut off the pressure valves, and then start the boiler. Someone could blow up a school!

I nagged and nagged that the modem should be kept turned off, and if a building engineer wanted to use it that they would phone in, identify themselves, and ask for the modem to be activated. Nothing happened.

Then the movie "War Games" came out, with its plot about kids accidentally dialing into a mainframe and starting a nuclear war. Suddenly my boss developed a new security procedure wherein the modem was kept shut off...

Ronald van den Heetkamp • **March 25, 2008 9:20 AM**

@YWo who said:

"Fred P is correct. Petroski had a book about this (forget the title) that said engineering is about foreseeing failures in the engineering process. So the premise fails."

My comment:

you obviously lack the skill to read between the lines, which proves Schneier's whole point he was making.

Skippern • **March 25, 2008 9:23 AM**

When engineers look at weaknesses and failure they look at the consequences of a failure, not how to make the system fail.

In many offshore systems a "safe fail" is often desired over a "fail safe" system. In other words, a system that fails without consequences.

The security mindset goes in the way of seeing how you can make the system fail.

BTW: I see many ways of having airport security fail, specially in the US. First you take away all weapons by security check, than place armed people on the other side. Overman one, and you have a weapon.

Niyaz PK • **March 25, 2008 9:30 AM**

Great article Bruce.

Anonymous • **March 25, 2008 9:37 AM**

I am reminded of some of the flim flam that James "the Amazing" Randi exposes. Even more than the exposes, what is really impressive is how he sets up the experiments to avoid security breaches. Conditions that seem absolutely watertight at first glance turn out upon inspection to have damning vulnerabilities which are invariably the vector for the Uri Gellers of the world to exploit. Randi finds them, plugs the leaks, and poof, the paranormal abilities disappear. It takes a very special mindset to think like that. I have always envied it, and despite a reseach education that actively encourages questioning your results, don't quite have it.

May I ask a question here that may be relevant? It has always puzzled me. Mr. Schneier, how do you avoid spambots in the comments?

RickS • **March 25, 2008 9:52 AM**

The book was "To Engineer is Human", by Petroski. Required reading my freshman year.

---

shoobe01 • **March 25, 2008 9:55 AM**

Agree totally with Fred P. GOOD engineers (and designers of all stripes) pay attention to all sorts of failure modes, whether security or not.

Plenty of bad or lax engineering abounds, however. And now that I think back to e-school, it seems that maybe they need to add a class on critical design thinking, and predicting failures before they happen.

Frank Wilhoit • **March 25, 2008 10:07 AM**

The "security mindset" and the "criminal mindset" have some obvious similarities. What do you say to those people who are inclined to take those similarities as being deeper and more essential than they actually are?

Sofa • **March 25, 2008 10:13 AM**

Fred P. is not totally correct. Bruce has said it many times you want to see how things fail and as a designer you want failures to be predictable and of minimal impact. You don't want large catastrophic failures and knowing how it fails helps with code execution and overflow behavior I would suspect. Sure you can try and design it to never fail, but designing to fail in predictable safe ways is far more realistic and advantageous. The way the twin towers went down is a perfect example, they took the heat for approximately 2 hours as designed and then collapsed in a way that probably saved as many lives as it cost because of the design by the engineer originally.

Rich Wilson • **March 25, 2008 10:17 AM**

@sooth sayer

Some people think about sending ants, other people actually do it. I'd like the thinkers to think about it before the doers get a chance to do it.

---

vvpete • **March 25, 2008 10:26 AM**

Engineers have got to consider failure to be any good. For example, a lazy engineer might specify the strongest bolt of a given size to hold together two halves of an assembly. But if the two halves are complicated, expensive castings, perhaps you'd rather have the bolt break under stress than a corner of the casting.

Such considerations are much more straightforward though than those surrounding most security situations where inexact sciences like economics and psychology come into play.

---

supersnail • **March 25, 2008 10:50 AM**

@john "The question that is ignored is "how will this bill be misused?""

I think you will find the related question "How can I be sure I can misuse this bill" is uppermost in the minds of many legislators.

Bruce Schneier • **March 25, 2008 10:57 AM**

"The 'security mindset' and the 'criminal mindset' have some obvious similarities. What do you say to those people who are inclined to take those similarities as being deeper and more essential than they actually are?"

I think the similarities are pretty deep and essential. The difference is how you act on it: making things more secure vs exploiting the insecurities for personal gain.

---

rai • **March 25, 2008 10:59 AM**

I must have that mindset. the first time I read about FACS (facial action coding system) I immediatly realized that botox would eliminate its effectiveness.
There are now computer facial recognition systems that read FACS.

Watt? • **March 25, 2008 11:06 AM**

The power grid would be more secure?

Maybe if they could find a safe and inexpensive way to bury transmission lines and substations a hundred feet down.

Petréa Mitchell • **March 25, 2008 11:15 AM**

@Nick Lancaster:

Yes, absolutely! In an ideal world, every programmer would be trained in the security mindset.

It also helps because there's a lot of overlap in security and usability problems. Usabilty issues also often spring from never questioning the assumption that people will only use a program in a certain way-- for security, the assumption is you'll only get authorized users, and for usability, it's that you'll only have expert users who instinctively understand the programmers' mental model of the program.

"How could somebody inadvertently do something they didn't want to?" is nearly equivalent to "How could someone intentionally break this?" for many programs, and the first question may be received better than the suggestion that your users are criminals.

---

pohart • **March 25, 2008 11:16 AM**

@Nick
When people refer to laws being abused, they are generally referring to laws that give more power to government officials.

---

obscurenough • **March 25, 2008 12:25 PM**

The Jason Bourne books by Robert Ludlum contain much of this pattern of thinking. I recommend them to anyone in this discussion who has not yet read them.

Pat Cahalan • **March 25, 2008 12:33 PM**

@ vvpete

> Engineers have got to consider failure to be any good.

Certainly. However, for most engineering applications, failure modes examined are unintelligent failure modes. What happens if the lateral force on this building design exceeds N? What happens if the soil density under this building is affected by a flood? If lightning strikes this power line, how much damage will the surge do to whatever is connected to it?

Security professionals, on the other hand, consider a different type of failure: the intelligent failure or the engineered failure - failure modes that aren't due to natural occurrences (or even freak occurrences), but the intentional gaming of the system by an intelligent entity.

Engineering is close to security... in fact, in practical terms often times it's better to listen to the engineer than the security guy because those natural or freak occurrences are often times orders of magnitude more likely than malicious misuse.

@ Dave Walker

re: Percival's blog

That's an interesting post. I don't know that I buy it, entirely. Mathematics can certainly teach you rigor, but mathematical systems are usually closed, and real world security systems are usually not. I do think that many mathematicians can be good security guys, but I'm reminded of one of my favorite of Bruce's anecdotes from his Applied Cryptography days. He's at a conference, and involved in some discussion when an FBI (?) guy is describing a side-channel attack, and Bruce says, "But that's cheating", and the lightbulb comes on.

Classically trained mathematicians can easily wind up being stuck in a box. Axiomatic systems can do that to you. :)

Tony H. • **March 25, 2008 12:47 PM**

>>"The 'security mindset' and the 'criminal mindset' have some obvious similarities. What do you say to those people who are inclined to take those similarities as being deeper and more essential than they actually are?"

>I think the similarities are pretty deep and essential. The difference is how you act on it: making things more secure vs exploiting the insecurities for personal gain.

Two non-technical writers I can think of have used "criminal mind" in the sense of "security mindset", and clearly understood its usefulness.

Roald Dahl, in one of his short stories, Parson's Pleasure, talks about the local petty-crook farm boys taking great interest when an antique dealer purports to show them that their piece of furniture is a modern replica, because it has machine-made screws. They are fooled (he has palmed the actual and very old screw), but they clearly have the right idea.

And more recently, Anthony Bourdain, in The Nasty Bits, uses the phrase in reference to his restaurant line cooks, who he seems to think need this attribute to be great at what they do.

Nick Lancaster • **March 25, 2008 1:00 PM**

@pohart

So are we better served by having unethical thugs restricted by carefully-worded laws, or by elected representatives who can be trusted to follow the spirit of the law? Would we even want public servants who *need* to be limited in such a manner (yes, I understand we've got more than a few people in D.C. playing the 'that which is not explicitly forbidden is legal' game)?

Can overly restrictive laws also work against the populace, in the sense that a healthcare law, focused on making sure hospitals and employers aren't defrauded, end up burning the citizen?

Emmett Shear • **March 25, 2008 1:03 PM**

I'm a programmer, so I build things for a living. I founded my own company, so I wind up in charge of security and building things at the same time.

One thing I've noticed is that I can't do them on the same day. Either I'm thinking about how to make things work and building them, or I'm thinking about how things are exploited and breaking them. Trying to do both gives me a headache and never works.

Splendidly Sailing Sliver • **March 25, 2008 1:09 PM**

I think the hardest thing to deal with is the reaction of people who do not think this way. I find that they sometimes react negatively to my analysis ("only a criminal would think like that") as opposed to reacting negatively to the crummy security.

---

old guy • **March 25, 2008 1:40 PM**

This really relates to Bruce's previous post of Adam Shostacks's Security Development Lifecycle blog, which I found to be an excellent resource as backing for process improvement where I work. There are people who are good at breaking things. There are people who are good at creating things. Sometimes traits co-exist in those extremely talented individuals you come across. That definitely hasn't been my experience. I've been carrying the 1-ton "paranoid" gorilla on my back for many years now. (My posture is pretty bad because of it- can't blame age for everything.) The developement process has to include us paranoid types to make it work. Judging the continuing state of infosec, this hasn't been accomplished. I'm confident that the pieces are coming together though, especially seeing posts like Mr. Shostack's.

False Data • **March 25, 2008 2:23 PM**

I've noticed several elements to the security mindset, both here and in previous posts.

1. A tendency to notice the way things might fail and how someone might exploit those failures.

2. A tendency to point out or explain those security flaws.

3. A tendency to place a stronger value than most people place on addressing security flaws, such as addressing flaws that others might regard as uneconomical to fix or as economic externalities.

Are all three necessary for a security mindset? Is any one of them sufficient?

Anonymous • **March 25, 2008 2:26 PM**

This mindset is really no different from that of people who work in areas such as product safety, aviation safety, construction safety, fire prevention, etc.

---

wyrdling • **March 25, 2008 2:41 PM**

i grew up around engineers who thought this way. they mostly spent their time doing failure analysis, so i guess it makes sense.

it's eminently disturbing that this sort of thinking isn't more common. people take too much for granted. seems a foundational element of critical thinking- "when will this idea _not_ work as intended? is that acceptable?"

---

xd0s • **March 25, 2008 3:14 PM**

@ Petrea
""How could somebody inadvertently do something they didn't want to?" is nearly equivalent to "How could someone intentionally break this?" "

Hmm, I'm not convinced. While both seem to cover the immediate issue (domain) failure, the second contains a factor not in the first, and that is intent. Implied in that is a reasonable assumption (ok I'm a security mindset sort) that the intent would be followed by further explaoitation, and that requires a security person to drive solutions deeper and provide more systemic, robust answers than just the immediate issue.

They are certainly close, but the quantum leap from "every job looks for failures" and "Security Mindset" is the extension from the immediate domain to the overall system IMO.

Colin M • **March 25, 2008 3:25 PM**

You can send someone 1500 live ladybugs for $10 via Amazon:

http://www.amazon.com/1500-Live-LadyBugs-GOOD-BUGS/dp/B000MR6WRG/ref=pd_bbs_sr_2

It doesn't take much imagination to think of the practical jokes you could play when armed with $1000 worth of ladybugs.

John • **March 25, 2008 3:43 PM**

Lancaster:

"Is the tradeoff of such legislative design a restrictive environment where individuals are not trusted to decide or accept responsibility? I'm not sure that laws which assume you're not smart enough or honest enough to comply are an improvement."

It looks like we aren't talking about the same thing.

I'm not talking about the citizen exploiting a law. I'm talking about officials exploiting laws that were apparently well intended.

Especially in criminal law, it is extremely important to consider the potential for official misuse.

James • **March 25, 2008 3:44 PM**

The link to the 'smart pillbox' security review at UW is broken, here's the correct link:
http://cubist.cs.washington.edu/Security/2008/02/10/security-review-smart-pillboxes-maybe-too-smart/

---

wkwillis • **March 25, 2008 4:47 PM**

Westlake is a mystery writer. He writes about characters that think like that.
Shouldn't cops think like that? Except I never read police procedural novels that have characters that think about security.

Urox • **March 25, 2008 5:03 PM**

I also have to object about the engineers not thinking about how to make things fail. How else does the term 'social engineering' come about? You find out how something works or doesn't work. Then you use that to your end for good or evil.

Henning Makholm • **March 25, 2008 5:29 PM**

I think Colin Percival's blog post overstates the connection between mathematics and the "security mindset" by implying, implicitly, that all the security mindset takes is rigorous attention to detail. As Pat says, attention to details, in and of itself, does not prevent you from missing the big picture.

However, if we limit ourselves to mathematical research (and not merely passing classroom courses) a much better argument for the proposition comes from the observation that the best way to devise proofs of interesting theorems is often to try to construct a counterexample.

Once a proof is arrived at, mere rigor is all that is needed to check it. But finding it in the first place (and, just as important, finding out what to prove!) often demands a more creative outlook.

You start by hypothesizing that conditions A, B, and C are sufficient to guarantee the desired result R. Right after this you mentally switch to being "the adversary" and try to figure out a way to achieve not-R while still satisfying A, B, and C. If you're in luck, you fail to find any counterexample, but do manage to convince yourself that your search for counterexamples was exhaustive. The narrative of your search then becomes the first draft proof, which if you're a good mathematician you will probably be able to massage into something more direct and elegant.

Another way to be in luck is to actually find a counterexample. The counterexample shows that your hypothesis was not good enough; you system could be broken. But in most cases the counterexample will also point towards additional assumptions you need to add to your conjecture. So you still achieve progress.

The only way not to make progress is not to find any counterexamples, and also not to be sure that one looked closely enough for them.

Thus, in order to be a successful mathematician, one needs the ability to look at some complex system (the assumptions) and try to find a way to beat it - probably by guesswork and hunches at first (because

that is quicker), but hard and systematic if that does not work. This appears to me to be very close to the "security mindset" that Schneier describes.

I acknowledge that not all mathematics is done in this way - it depends on the subdiscipline how often it pays off - but in my experience a lot of it is.

Peter Robinett • **March 25, 2008 6:07 PM**

I'm afraid I can't find a link, but I remember a car being stolen in the Bay Area in just the fashion you describe (I believe it was a Lambourghini from Stanford European). Basically the thief walked in, said he was there to pick up 'his' new car, and walked out with the keys. Apparently the car was last seen heading south on 101 towards Los Angeles, so the assumption in the news article I read was that the car was destined for Mexico.

Bruce Schneier • **March 25, 2008 7:11 PM**

"You can send someone 1500 live ladybugs for $10 via Amazon."

Good to know.

But the ants are completely anonymous; the ladybugs require you to leave a credit card number.

Bruce Schneier • **March 25, 2008 7:14 PM**

"@Bruce .. it explains some of your diatribe against things that 'normal' people won't think twice about. And frankly I will never think about sending a a tube of ants to someone I care or don't care about."

Of course you won't. Most people won't. The point is that there are bad guys who will try to abuse any system out there, and a good security engineer needs to be one step ahead of those bad guys.

---

bob • **March 25, 2008 7:19 PM**

@ Nick Lancaster

"(yes, I understand we've got more than a few people in D.C. playing the 'that which is not explicitly forbidden is legal' game)"

When was this ever confined to people in D.C.?

Roxanne • **March 25, 2008 7:36 PM**

I've not gotten jobs a few times now because the interviewer asked questions along the lines of: "Have you ever thought about how you would steal from a store?" Well, duh, that was part of my job at a bunch of places, so as to work out how to discourage theft. They don't want to hear that when you're going to be handling their money.

I would go so far as to say that most people don't want to think that the people around them are working out where the chinks are in the armor.

LadyLuck • March 25, 2008 8:57 PM

What's depressing about this enlightened thread is that the whole human effort to secure things, or even to invent things, becomes so futile.
Everything has a weakness waiting to be exploited, a goal, however good, to be thwarted or twisted. It's as if humankind would be better off simplifying life, understanding the basics of human survival and satisfaction, to improve existence. But, to do that will probably require global cooperation and equanimity-- peace. The whole game of outsmarting the other guy is a doomed cycle of endless frustration--the big picture would be to eliminate the need for security. Not by having big brother draconian surveillance, but by making it possible for everyone to meet their needs without conflict. If a human can think it, it might be possible. Cynicism and observation sometimes lead back to simple solutions, even if they appear naively idealistic.

YWo • March 25, 2008 9:42 PM

Ronald van den Heetkamp how does it prove his point and what exactly am I reading between the lines for?

You are an idiot who cannot construct an argument correctly because you are ambiguous in your claims and you don't state how it proves anything.

George Smiley • March 26, 2008 12:21 AM

Did you notice, Bruce, the *real* security device employed by Uncle Milton Industries? They do not send you (or someone whom you specify) a tube of ants. They send a tube of workers. No queen. And workers without a queen are, biologically, not-ants. It is as though I sent you a box with a severed hand in it, and you said that I'd sent you a "person."

Dave B. • March 26, 2008 12:35 AM

I wish to take issue with the "It's not natural for engineers." by relating an anecdote:

I live in Switzerland and one day I heard a siren. I asked my boss what the siren was and he told me that it was the nuclear attack warning siren. I was interested in how he knew, since I hadn't seen any warnings. It turns out that its done on the first Wednesday of every February.

My first thought, which I said without thinking, was "Aha, now I know when to nuke the Swiss for maximum effect".

There are engineers out there that think in the way you describe. If you're lucky you have doing your QA. If you're luckier you have them writing the specifications.

Pat Cahalan • **March 26, 2008 2:00 AM**

@ Dave B

> My first thought, which I said without thinking, was "Aha, now I
> know when to nuke the Swiss for maximum effect".

It's not often that a comment about nuking a country makes me cough up my drink. Nice.

Brad Templeton • **March 26, 2008 2:29 AM**

I have the security mindset. And for society, it can often be a curse, not a blessing.

We want a world without the security mindset, we really do. A world run by the security mindset is an armed camp with a moat around it. We want a world where, by other means, we just make it so that only a small fraction of the population are bad eggs out to do bad, and we can deal with the cost of them either with insurance, or with deterrence -- ie. we can scare them about being caught and punished rather than stopping them in advance.

Most of our wealthy societies managed to escape the security mindset for a while. It was an eden. Nice department stores have cashier stations scattered around the store and no guards or scanners at the door. Cheap department stores have tag sensors and guards and all the cashes right at the door. They cost a bit less, and some of that may be due to less "shrinkage." Which do you prefer?

Why have we returned to the security mindset in the online world? Because here, bad eggs can automate their evil, and touch us all in bulk. But we should still resist being taken into the security mindset, kicking and screaming.

Ibod Catooga • **March 26, 2008 2:39 AM**

I have a security mindset because I like stealing shit!

---

miw • **March 26, 2008 3:10 AM**

The security mindset is perfectly teachable. Similar mindsets are developed in almost any professional education. Legal professionals have to think about all possible ways a contractual relationship may go astray and deal with it. Most scientists look at theories and design experiments to find faults in them. Entepreneurs search for deficiencies in existing services and products. Managers do the same with organisations. So, equivalent mindsets exist in almost any profession. The only difference with security, is that it resembles becoming a criminal, a terrorist, a fraud or any other person that has negative social connotations. I'm sure that this social judgement is the only element that is different for a security professional. The mindset requirement is actually quite common.

Anonymous #3 • **March 26, 2008 3:55 AM**

@various commenters: The security mindset itself is not a bad thing. Choosing abuse instead of disclosure is bad. Encouraging non-disclosure by shooting the messenger, or at least threatening to do so is bad because it helps the abusers. Finally, designing for maximum security without a proper risk assessment is bad because it can yield unnecessarily restrictive systems or procedures.

The engineers vs. security people argument is also largely beside the point: Of course security analysis is part of engineering (or at least should be). What's less obvious: Engineering doesn't stop once the product ships. Users finding flaws and exploitable security issues are just part of the ongoing engineering process. In a world of technology, engineering never stops. This is why disclosure is so important.

TokyoDevil • **March 26, 2008 6:56 AM**

@LadyLuck ...

If nature had meant for us to be at peace with each other, we would be. It's simply not in the DNA -- and for good reason: competition weeds out the faulty code, and rewards the more robust code.

BTW, being competitive does not suggest an inability to empathize with others or experience and appreciate the full range of human emotions.

Alternatively, had the human code not been engineered (I'm assuming an intelligent designer), then we likely would not be communicating with each other. I dare say we'd be a dust-collecting oddity in some other life form's version of the Smithsonian.

Roxanne • **March 26, 2008 7:32 AM**

It occurred to me overnight that the line between "Security mindset" and "Clinically paranoid" might be a lot thinner than one might wish. We need to make sure we're teaching, "Why we don't want to break this," right alongside "This is how to look for ways to break this."

Robert Accettura • **March 26, 2008 8:40 AM**

What's interesting is how this reminds me of my childhood... but I don't consider myself a security guru.

Normally when I got in trouble at school, it wasn't for doing something random, it was for using someones words, or rules against them.

I remember as a joke appending " is an idiot" to my name in HS on a few tests... got in a lot of trouble.. they accused me of violating school rules for being insulting. I pointed out the rules clearly permit it because:

1. Rules target when you insult OTHERS. I am myself, and am not bipolar.
2. The word "idiot" is a good word. If I used "retarded" you could say I insulted the mentally disabled. "idiot" harms nobody.

The rules clearly didn't prohibit me from insulting myself.

Because they couldn't suspend me, I broke no rules... they decided to call my parents in for a conference and recommend counseling from a state funded quack.

Another time I decided it would be funny to copy someone else's work for a BS assignment at the end of the year, but rather than "plagerize" which is defined as copying someone else's work and taking credit. I cited the work and used MLA format.

James • March 26, 2008 9:13 AM

Bruce:
The lady bugs may require a credit card, but I can buy a credit card with cash at most malls and grocery stores. I can also get a (reasonably) untraceable email for the amazon account.

The fail in the Lady Bug Plan, to me, is that it would cost me $10. Now, if I can get yet another victim's credit card info...

James • March 26, 2008 9:21 AM

Scratch that, I doubt you could use a prepaid card on Amazon, as they likely require the card have a name attached.

Guess I would need to buy a gift card with CoinStar.
http://www.coinstar.com/us/WebDocs/A1-0-3-1

Bob • March 26, 2008 10:43 AM

A somewhat scarier experience than being able to pick up a car with just a name...yesterday, I returned from vacation, having put my postal mail on hold. I went to post office to pick up my mail and all I had to do was write down my name and address on a piece of paper and they gave me this big bucket of mail. They asked for no ID at all.

The last time I did this, they actually gave me someone else's mail bucket by mistake and I realized it as I went to put it in my car.

Personally, I'd rather lose my car than my mail.

---

rai • March 26, 2008 11:18 AM

Tokyo devil starts with a line about why people are not living in eden, about how we are one of our own worst problems, (wars are crimes committed by nations).
then he finishes with a line about intelligent design.
Heres a bumper sticker for all you kansans,

When evolution is outlawed, only outlaws will evolve. ;~}

paul • March 26, 2008 1:49 PM

One of the reasons the security mindset can be hard to develop is that people are typically trained to prove hypotheses, not to disprove the null hypothesis. Basic education in science and engineering is about things that work, and how they work. And in many cases, building something that works under *some* set of conditions is a serious accomplishment. So going on to build things that work even under conditions they weren't designed for doesn't even get considered.

CuriousBill • March 26, 2008 3:06 PM

I entered middle school at a time and place far away.

We were assigned a locker, and used our own 3-number combination lock in the door handle. Lockers came in units of 2 narrow vertical doors side by side, topped by 2 book compartments as wide as both doors together, each about 9" high. Each book compartment had its own access door.

Each locker door allowed indirect access to one of the book compartments. Closing a locker door pressed on a roller, raised a bar and hook, and engaged a small plate on one of the book doors, thus locking it.

The designers allowed for the possiblity that the locker door would be closed and locked before trying to close the book door. The latch plate on the book door was allowed to move up and fall down by gravity. It would rise up when it was pressed agianst the sloping outside of the locking hook, then fall back down on the other side, thus locking the book door.

What if I could raise the latch plate with a tool, without bothering to unlock the locker below? The latch plate was a light piece of metal about 1" x 1/2". The book door had three ventilation slots in the middle. The latch plate was exposed near the side of the book compartment door, not shielded by metal.

I found that I could bend a paper clip into a gentle curve, with a kink on the end, slip it through the middle ventillation slot, and catch the bottom of the latch plate. A small twist raised the latch plate, and the book door would open. This worked for all the bottom book compartments. The top compartments required a mirror-image paper clip tool.

I didn't steal anything, and didn't want to steal anything. I was merely amazed that it could be so easy to open something that had been designed for a school. How could the designers have been so dumb? Since I was proud, I told a friend or two about what I had discovered.

A few days later, one friend showed me how adept he had become. He walked along the lockers, deftly using his version of the paper clip to open one book compartment every 2-3 seconds. I didn't want to participate, and left.

The next day, the school found all 200 book compartments open on that floor. The school issued a stern warning that anyone doing this would be punished. Fortunately, the whole business calmed down in a week. People stopped opening book compartments, and students didn't use the compartments to store anything valuable. No one wanted to steal the books, anyway.

giafly • **March 27, 2008 1:45 PM**

Back when I was a child, I remember that school treachers tried to talk me out of this security mindset. Back then it was called "Finding Fault With".

Now it has a longer name, "collect[ing] information of a kind likely to be useful to a person committing or preparing an act of terrorism [without] a reasonable excuse", but is still disapproved of.
http://www.opsi.gov.uk/acts/acts2000/ukpga_20000011_en_6

CG • **March 27, 2008 4:21 PM**

@YWo

when someone leaves their blog URL you may want to at least take a look before you call someone an idiot. Ronald is part of GNUCITZEN and if you look at his blog as put out some really forward thinking security research.

Your knee-jerk reaction is enjoyable though.

---

markm • **March 27, 2008 9:01 PM**

I'm a EE and have worked as a test engineer at an electronics plant for 17 years. Engineers do think about how things fail, especially test engineers - but it's different from Bruce's mindset. I'm professionally paranoid about how equipment can break down by itself, not about how people can deliberately break it. That is, I do think about possible user interface issues, but in terms of user confusion and mistakes and of ability to recover from hitting the wrong button, not in terms of protecting against sabotage, and in any case I spend much more time working on ways of preventing and limiting the effects of electrical failures than on user interface problems.

---

askme233 • **March 27, 2008 11:17 PM**

A bit of a security mindset, usually ends up either disconcerting me, my friends or my wife with the things I bring up, I also see the inherent trade-offs that are needed to have a civil world. If we always planned for breaches, we would lose too much value of convenience, simplicity, etc.

The other day I received a call on my cellphone on a Sunday afternoon from someone purporting to be from the IRS. before proceeding, she wanted to 'authenticate' me and demanded sensitive information like SSN and bank details. Although I was not wholly surprised to get a call from the IRS, I pointed out that I would not routinely give out that data to a random caller that was not authenticated to me.

To my surprise, the IRS caller politely agreed and we quickly came up to a compromise in which we quoted alternate digits of my SSN and bank numbers to each other. This confirmed us to each other in a simple, convenient manner.

I liked that she understood (and respected) the need for mutual authentication and agreed to it (from a gov employee no less). She had enough of the security mindset to see my point of view.

She still told me I had to file my tax return.

PS: all you Engineers, calm down. there is a difference between good design (including failure mode) and actively seeking to pervert a system. But that is not a knock on engineers.

---

askme233 • **March 27, 2008 11:38 PM**

@CuriousBill

Just re-read your story and recalled my grown-up version:

Almost all high-end offices have fancy glass doors that are always magnetically locked. Access from the outside requires a cardkey to get into. From the inside, a motion detector is triggered when a person walks towards the door and unlocks the doors. These are high end security systems in class-A space and they are all the same.

A warm deck of cards and a quick flip of the wrist through the crack between the doors has always worked.

Never figured out why they keep these things, but I stopped showing co-workers after a little while after getting a bit too much interest.

LadyLuck • **March 29, 2008 12:14 AM**

back @TokyoDevil

Sure, American Science education teaches us that we are what we are--dna rules. I won't argue that we are just another bunch of aggressive animals on Earth. However, Intelligent Design or Fluke of Evolution, mankind sits on a new precipice with an awareness of it's own precariousness on this planet.

We can worry ourselves endlessly on how to treat/cheat/subvert or anticipate the next small or large attack on our structures. Or we can view it all from the angle of how to preserve the best of human knowledge and efforts at understanding the world.

The security mindset is so important because it asks: What is your motive? What is your goal? What are all the pitfalls?

If your goal is selfish, greedy, or trivial, well, that's category 0, or give it a variable name. If your goal is to improve things but you won't consider others in your equation, that's a different category. If you simply want to offer improvements with no obvious, immediate benefit to yourself, that's yet another category, maybe 'opensource'.

But long and short, you can tail twist a long time on these simple philosophical dilemmas and the logic always comes back to the premise: how do you see the world, and how do you choose to see your set

of possible solutions?

If you choose a world view that has to condemn other people as evil, your logic train changes. If you view a world in which everyone is struggling to attain the same things you want, food, safety, future, you see it differently.

Schneier's social books on Security are a good place to understand how difficult security is in the real human world--he explains well why security is only as strong as the humans who implement it, and live it. What Schneier hasn't yet been given credit for is that his books inspire in some people, who never cared for history, a desire to understand more of human history to figure out how we got to where we are now.
Humanity and the issues of security are very old...
But I'm as thrilled as the next person to learn of new exploits at the ATM machine...I'm only human.

E • March 31, 2008 8:52 PM

After reading "Inside the Twisted Mind of the Security Professional" and the example of the student who was able to receive her car that was being services just by giving the last name, I had a slight feeling of deja vu. Last week I stopped by our local CVS Pharmacy where my girlfriend picks up her prescriptions, but she was unable to because she wasn't in town, so she asked me to pick them up for her. I mentioned to her that I probably wouldn't be able to unless I she had given my name to the pharmacist and I provided ID, or at least that should have been the procedure. But I was able to walk in, give the last name that was on the prescription, $20, and that was that. It's unfortunate that the pickup policy for prescription medication that could be extremely important to an individual and can be abused by a different individual is so bad.

Alan • April 17, 2008 9:56 AM

In thinking about One Laptop Per Child, a colleague was concerned that the children would be susceptible to Nigerian letters. His solution - include a tutorial on how to write one.

Koen • April 18, 2008 4:26 AM

What I find really surprising in all comments here, is that only one mentions the actual profession of a test engineer. As a professional in exactly this field, I recognize a lot of points made in this article about mindset. A good tester is not only looking for ways on how to break things, but also what things are most likely to break first or which will break most often. In short: where are the risks highest.
Maybe the profession of security and testing are overlapping in a lot of fields... Hmmm, anyone who can comment on that? Maybe I should mail Mr. Schneider directly about this.

DaveL • **April 22, 2008 10:48 AM**

I actually work as a security professional, but in a former (government) life I was an engineer. Based upon my experience, failure modes are considered in both disciplines - but engineering rarely considers cascaded "what if" scenarios, which are tantamount to security exploits. What if the glass cabinet door is lifted out of the groove, and then what if the glass is hinged away from the cabinet, allowing the user to then slide the lock assembly completely off the inner piece of glass and then completely removing the outer piece of glass and then removing the expensive contents? That sort of thing. Admittedly, not all security penetrations are predicated on cascades, but many are - SQL injection is a fine example. It is as Gasparov said of chess; a fine player considers every move available, a really good one considers every possible response to every valid move, while a great chess player will consider the move tree five moves in. Engineers tend to be single-tier thinkers, while security people tend to think in N-move gambits.

ReadArmy • **April 25, 2008 9:48 PM**

Ok, who just sent me these ants?

John Tate • **April 30, 2008 11:25 AM**

Here's an extreme example from xkcd, the web comic which has had a few good ones on security and cryptography in the past:
http://www.xkcd.com/416/

Cindy • **April 30, 2008 5:54 PM**

I have been in INFOSec since 1985, and this is SO right on. And SO ignored in commercial INFOSEC. My training was originally reverse engineering and exploiting the bad guys technology and then worked at AirForce Information Warfare Center (AFIWC) (It was AFCSC before that), developing policies and procedures. I am now in the commercial sector and am continually amazed at the naivety of the "kids" who think because they have some letters behind their last name they are security "experts" (that has some value, but it takes psychology and understanding warfare, and that is what is totally lacking today) .... I wonder how many of them have read the "Art of Warfare" by Sun Tzu written in the second century, B.C.? That book is critical to understanding INFOWar (yes, we are engaged in (asymetric) infowar, with the same bad guys we fought during the "cold" war (which never really ended, only morphed). Make NO mistake about that). Think outside the box, think like a redhat, use the mindset that our enemies use, attack where least expected, using tactics that are not expected. Find where they will plunge the knife, before the bad guys do. THEN you are thinking like a security professional.

---

limeshot • **August 27, 2008 10:08 PM**

This must be the most interesting discussion I've read on a blog. Ever.

@YWo: Personally, I don't think one has to be a 'hacker' or a security specialist to have the security mindset. I'm a bloody graphic designer, what do I know about hacking?

And yet, I have the mindset. Maybe it's related to being from a country from the former Communist block, where
1. one had to find underhand ways of getting access to oranges or coffee since there was no 'legal' way of doing that (and no, I don't mean stealing, I mean black market) and
2. one has to always watch one's handbag, mobile phone and car stereo, as people tend to have very sticky hands...

Whatever the reason, I don't think this makes me special (@YWo), but it gives me a different perspective. I just never realised there was the name for this quirk of mine.

Anyways, really enjoyable article and comments.

Anonymouse_A17 • **December 8, 2008 10:37 AM**

Regarding sending ants to anyone, am I the only one who collects all of the magazine subscription cards from the doctor's office waiting room? :-)

Glen • **April 6, 2012 7:46 AM**

While people are busy protecting their identities, higher-risk vulnerabilities for taking-down a system or corrupting the data remain unmitigated. This is typically the case in healthcare, where HIPAA and state regulations strongly sanction identity-linked incidents while almost ignoring data unavailability or corruption that could actually harm or kill people. A security mindset would help.

John Rehwinkel • **April 8, 2012 9:19 PM**

I'm yet another one. I went to my bank to get the PIN for my ATM card reset. I handed them the card, and they set it for me. Whereupon I pointed out to them that in the future, when a random person comes in with one of the bank's ATM cards, at least ask for ID before resetting the PIN for the card.

Jim Bergstrom • **April 17, 2012 8:58 PM**

I, too, have always been interested in why I think like a criminal. The "Be Prepared" motto of Boy Scouts to the nth degree seems to be part of it. I was always the scout wondering if we could set up our tents in a storm or whether our campfire would possibly burn our tents in the night if it was too close and the wind came up. Just what is the secure distance?

In college, my Judo instructor called me "professor What-If". For every move I had a possible countermove. What would he do then?

It seems that to a Security Mindset mind the whole world is one big puzzle that has the ability to intrigue and excite at any moment. The finer the focus and one-pointedness, the deeper the tunnel goes. Training across a multitude of disciplines exposes one to challenges uncommon; actually involving onself in them exposes one to a unique form of experiential gain.

---

anitha • April 15, 2013 11:34 PM

We had a series of bomb blasts in Bangalore in 2008. A series of nine low intensity crude bombs exploded in different parts of the city . Although the human loss due to the blasts were low, the incident had a large "scare value". People were scared to go out to crowded places for a few days. Although, India being India, the "scare value" wore off in a few days time.

I work in a Tech Park, which houses around 25000 employees from different companies, and I was in the communication security research team. The day after the blasts, the fire/emergency alarms went off, and the entire Tech Park was evacuated and there were some 25000 people standing in hot sun, in the safe assembly area by the compound wall of the tech park. Later it turned out that is was due to a hoax phone call announcing a bomb placed within the premises.

As a security researcher, when the alarms for evacuation started ringing, my first thought was, it will be difficult and risky to penetrate the enhanced security at the Tech Park entrance and post a bomb inside the premises. What would be easier is to set off a fire alarm inside the buildings, get the people to assemble in the safe assembly area, and throw a few gelatine sticks into the crowd from outside the Tech Park Boundary. Or, allow a bomb placed close to the boundary wall to go off when the people assemble there. Especially, given that those blasts seemed to be designed to create panic, than to cause any serious harm.

In spite of all these thoughts, I still went to the safe assembly area, gave my attendance to the emergency response team, and started searching for my colleagues (some of whom are also security researchers). I couldnt find any of them, until few hours later, since some of them thought about the same threat, and had decided to skip the safe assembly area for a lesser crowded place.

Allowed HTML: <a href="URL"> • <cite> <i> • <b> • <sub> <sup> •   • <blockquote> <pre>

Preview Submit

← Paper Enigma Machine

Martin Hellman on the Invention of Public-Key Cryptography →