Thinking Critically about Computer Security Trade-offs

Good security decisions require making intelligent trade-offs, but far too often we settle for poorly justified security measures based on fear and ignorance rather than reasoned risk analysis.

ADAM SLAGELL

You can readily find computer and network security courses in most computer science departments, but it may be overly ambitious to call computer security a science. The profession certainly has aspects of an art, and it is fair to call much of the work engineering, but it lacks the rigor and objectivity of a science when put into practice. We highly desire security metrics to objectively measure the effectiveness of security technologies and to give the field this extra rigor, but they are difficult to come by. In fact, developing objective security metrics is considered one of the grand challenges of the field (INFOSEC Research Council 2005).

Part of the problem is the difficulty of quantifying risk in this field. Often, qualitative analysis is given with what are

arguably somewhat arbitrary mappings to quantitative values (Schneier and Ranum 2008). It is even harder to calculate the return on investment that managers need in order to make decisions about how to mitigate a risk. How much value do you give to your reputation, and how do you estimate the cost of loss of reputation due to a kind of cyber attack that has never occurred before? Also, we have too little data on how often various industries suffer from different types of intrusions. Until recent laws were passed, companies would conceal most instances of attack even from law enforcement if they could (Schneier 2006). These factors make it hard to make rational decisions about how to address the different threats from cyber attackers.

If the computer security industry had a good handle on these problems, you would expect to see the major insurance companies offering policies that allow one to transfer these risks. This is what we see with automobile safety, natural disasters, and physical theft. If there were a way to reliably calculate these risks, the insurance companies would create standards of practice for cyber security and commonly sell insurance to cover losses due to such threats, as they have done for other industries. However, it is very difficult to calculate the likelihood of an attack in such a rapidly changing landscape and even harder to estimate the true cost of such an incident. Therefore, cyber security insurance is just now beginning to appear—though not from major players—and is far from common practice.

Fear, Uncertainty, and Doubt

Without solid risk analysis, FUD (fear, uncertainty, and doubt) often fills its place when justifying a particular security countermeasure. It is easier and often more effective to raise fear in people's minds than to argue with them that they need to spend time or money on some security mechanism. This has presented enough of a problem that the statement of ethics for the major information security certification, the CISSP, specifically states that security professionals should avoid raising unnecessary FUD ([ISC]2 2008).

Raising fear, uncertainty, and doubt is not unique to computer security professionals. It is used by governments to justify exercising extraordinary powers (Electronic Frontier Foundation 2003), especially in times of crisis. It is used by agencies within the government to grab power (Shachtman 2008; Poulsen 2009), and it has been used to bring funding to pet projects (Meserve 2007). Vendors of security products also use FUD to sell their tools. This kind of FUD often comes in the form of scary and misleading statistics (Winder 2007).

In addition to not effectively informing people how to spend resources on security, FUD is dangerous for another reason. Its overuse makes people numb to real, but less dramatic, threats. This constant "crying wolf" can be dangerous because it can lead to inaction when a large, serious threat must be dealt with quickly in the future.

*In*security at the Airport

Bruce Schneier coined the very apt term *security theater* (Schneier 2003). Once exposed to the concept, one sees it everywhere. Security theater is security done just for show or just to make people feel better. It is the placebo of the field. A great example can be seen in the public safety films shown to schoolchildren during the Cold War era. These films showed children hiding under their desks for atomic bomb drills. There could hardly be a less effective countermeasure, but that wasn't the point. The point was to empower people so they felt like they could do something.

A more modern example of security theater costs us time at the airport and presumably man-hours for Transportation Security Administration agents and information technology staff. It is the "No-Fly" list. The goal of this list is to keep "bad" people off of planes, or at least people with names similar to those of "bad" people (Goo 2004; Moore 2007). It works by checking the name against a database containing the blacklisted non-flyers when tickets are purchased. The problem is that checks at the airport are very easy to bypass even if the list is accurate and specific—a precarious assumption (Bowers 2005).

The War on Photography

One interesting case is what has been called the "War on Photography" (Schneier 2008b). In recent years, people have been arrested, had their cameras confiscated, and been hassled by law enforcement for photographing particular targets (Davis 2007a, 2007b). Examples include photographing an ATM, police, and even tourist landmarks (Becker 2009; Davis 2007b; Fisher 2005; Shattuck 2008; Electronic Frontier Foundation 2003). There often isn't legislation to indicate what is illegal to photograph, and it is often instigated by reports from overzealous citizens or police who do not like to be photographed.

The main problem with this approach is that while police may catch a terrorist photographing something, there are far more tourists taking pictures of landmarks and curious people with cell phones taking pictures of things they don't frequently see—like an open ATM machine. This is simply because there are so few terrorists compared to non-terrorists. The signal to noise ratio of this approach is too high to be useful or efficient.

Furthermore, in this case there is likely nothing that can be done if law enforcement finds a terrorist taking pictures, as that alone is merely circumstantial evidence of terrorist activities. Usually, people are not taking pictures of anything illegally unless they are trespassing—in which case there are established laws to handle the situation. Add to this the decrease in police accountability if citizens are not allowed to photograph or record officers, and the trade-offs do not look so good. We likely harass and infringe upon the liberties of far more innocents for every terrorist encountered. And even then, confis-

Adam Slagell is a senior security engineer at the National Center for Supercomputing Applications, a division of the University of Illinois at Urbana-Champaign, and a certified information systems security professional (CISSP). He is a National Science Foundation principal investigator and has been performing computer security related research and operational security support for the past six years. You can visit his Web site at www.slagell.info/ and contact him at slagell@illinois.edu.

cating the camera would not get the terrorist off the street or stop him from having a comrade take the photo later or from using Google Street View®. To be useful, the false positive rate would have to be much, much smaller.

Back to Cyber Security

A common theme among these examples is that security is a trade-off. Even for effective measures, there are costs—if only of convenience and time. If we are not just propping up security theater as a substitute for real security, we are usually making a trade-off between usability and security. Furthermore, security is not all or nothing. Nothing is ever 100 percent secure, and therefore security comes down to using the best information available to balance costs versus benefits.

Let's look at desktop computer antivirus technology. Everyone should run antivirus software on his or her computers, right? The landscape was very different in the late 1980s and early 1990s when signature-based virus detection was created: there were few viruses, they used known and old exploits, and they spread slowly. Most often, the viruses spread by floppy disk and not over networks because most home PCs were not connected (Bloor 2006).

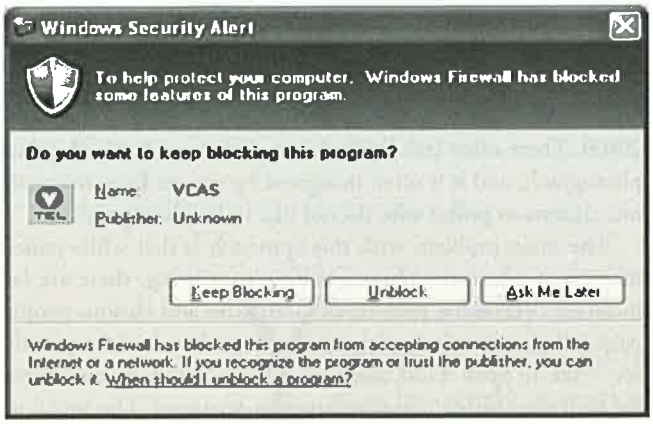

Figure 1. Windows Firewall alert

Much of this has changed now. First, viruses are often polymorphic or use encryption techniques to thwart signature-based detection, which fails at detecting as much as 80 percent of new malware (Tung 2008; Kotadia 2006). These techniques of obfuscation create one virus with a million different perfect disguises, which makes it difficult for any signature-based technique to match a virus. There is what we call "zero day exploits," unknown vulnerabilities used by the malware writers to spread their code quickly across the Internet before a signature can even be created and distributed. Finally, the signature databases have become huge—with millions of signatures—and they are growing exponentially (Leydon 2008). This uses significant resources on all but the newest PCs. For a long time the exponential growth in computational power kept antivirus technology in pace with the exponential growth of the number of viruses, but that has begun to level off (Dauger 2007). Signature-based antivirus is simply an untenable approach to handle malware on computers today.

Lest it be said that I am arguing against a straw man, I recognize that antivirus software has begun to try more behavioral-based approaches to look for misbehaving software. Unfortunately, this technology is still immature and often burdens users with cryptic messages. The fact is that even fully patched machines with the latest antivirus updates can still be infected. It appears that the "good guys" are currently the losers in this arms race until better techniques than the blacklisting approach of handling malware are developed. In fact, it may even make sense to consider white lists of allowable programs since there are more pieces of software people do not want running than those they do (Tung 2008).

The point is not to say "do not run antivirus on desktop PCs" but that enough has changed that one must really analyze the costs and benefits. Since keeping a machine patched and practicing good behaviors is so much more effective at preventing infection, and because signature-based antivirus software consumes a significant percentage of a computer's resources, I lean toward not running it. The tipping point was when it became so easy to restore a machine to a previous clean state with the advent of virtual machines. This allows you to freeze the exact state of a machine, do something that may risk infection of your computer, and revert back to that clean state afterwards and know that your machine is not infected.

Firewalls

Another thing people are told they must have is a firewall, even if they don't know what it is or how to properly configure it. Furthermore, there is a good chance that their Internet Service Provider (ISP) or office network already employs one. Host-based firewalls—ones that run on your local machine—can be great if you understand the messages. They will alert anytime a new piece of software wants to connect to the network, something almost all modern malware does.

Unfortunately, the average user does not know what programs should and should not run on their systems. For example, many users would see a message such as the one in figure 1 and not know what to do with it. In this case, it is necessary to allow a service pack to be downloaded, but how is the user supposed to know that? Furthermore, even if the alert says the name of the software is "iTunes," the creator of the malware can call it anything he or she wants. This often makes host-based firewalls very unusable, and users tend to just allow everything, effectively negating the benefit a firewall could bring.

So it comes back to trade-offs. Here we can potentially get more protection, but at the cost of usability if users unwittingly block necessary software. If they allow everything, they get no additional protection.

Password Mythology

One of the most common security mantras is to never write down one's password. Is this good advice? It depends upon who we are concerned might misuse the password. Writing down a password will not make it more or less likely for an online adversary to compromise the account. However, putting a password

on a Post-it® note underneath your keyboard at your office makes you vulnerable to the threat of a nosy coworker. What if you put passwords on a Post-it® in your wallet? Presumably, you already put sensitive information such as credit cards in your wallet. You have to think realistically about the threats you are exposing yourself to and weigh the trade-offs.

In this case, there can be some very bad trade-offs, especially if not writing down passwords forces you to use simpler passwords or reuse them for multiple accounts. It is hard enough to remember a few good passwords, let alone dozens. Simple passwords can be easily cracked by computer software using variations of what are called dictionary attacks (Null 2007). A dictionary attack is an unsophisticated but effective attack that simply tries millions of combinations of words from some dictionary in an increasing order of likelihood as the password in question. Because people do not use truly random passwords, these attacks are very effective. Poor security practices at another site can expose that password, letting the attacker try it for accounts in other domains. This is a problem we frequently face in the supercomputing community (Nixon 2006), where passwords are harvested at one site and reused at a collaborating site to get a foothold on new systems. This is often out of the user's control, too. Password reuse allows a small breach to more easily become a large one.

The best defense against these problems is to use many distinct, random passwords. Because of the limitations of human memory, this usually requires writing some of them down or using one of the many great password management tools,[1] which encrypt your passwords with one strong password and even allow you to carry them with you on a USB flash drive. However, this goes against the often-recited warning about writing down passwords.

Web Site Security

You will often see advertisements on Web sites, especially if they are selling something, that they are "hacker proof" or use "128 bit encryption." Ignoring the fact that not all 128 bit ciphers are equal (Vaudenay and Vuagnoux 2007), anyone can set up a Web site that uses encryption. If they are willing to spend a couple hundred dollars, they can even get a certificate so that the visitors' Web browsers will show a nice little lock icon "proving" their connection is secure.

Few people, however, really know what that lock icon means. You should ask, "Who am I trusting and to say what?" In this case, you are trusting that a certificate authority, like Xramp Global Certification, has done some sort of check that the owner of the domain (e.g., example.com if you are visiting www.example.com) is the one running that Web site. Furthermore, you are trusting that your Web browser is correctly communicating with this Web site in a way that prevents others from eavesdropping on the conversation between your Web browser software and the Web server. While there may be reasonable doubts about whether this is good (e.g., "Who is Xramp Global Certification, and why should I trust them?"), this in itself is not so bad. The problem is that the lock icon does not assert what people often assume it does.

Several questions remain unanswered even if you have a "secure connection" to a Web site and see that nice lock icon. For example, how are the data handled on the retailer's network after the Web server processes it? Is the credit card information stored on these systems and, if so, is it encrypted and protected adequately? How does the business handle its backup tapes that contain the consumer's data, and how does it prevent theft or loss? With whom do they share the consumer's data and for what purposes? All of these things could be answered in various ways regardless of whether or not that one communication channel between the Web browser and the retailer's Web server is secure.

The problem is that people must still trust the retailer to implement good security measures. This is probably not a terrible step to take if you are visiting Wal-Mart's Web site or Amazon.com. However, it is likely to be of little help if you want to do business with the owners of cheapjunk.biz.[2] The security that comes with that little lock icon proves to be necessary but hardly sufficient for a secure online transaction.

Why Do We Make Bad Trade-offs?

It is clear that we often make poor security trade-offs, but the question is: why? While this is outside the main point of this article, I present some of the more popular hypotheses. Bruce Schneier, a leading applied cryptography researcher, brings up a point I find particularly suited to explain much of our inability for reasoned risk analysis (Schneier 2008). There is a mental mechanism psychologists call the "availability heuristic," which states: "We assess the frequency of a class or the probability of an event by the ease with which instances or occurrences can be brought to mind." A corollary of this is that we are swayed more by vivid, personal experience than statistics. It certainly makes sense that we would evolve such a heuristic and that it would work well with the simpler risk analysis faced by hunter-gatherers tens of thousands of years ago. Further, it is just as easy to see how it falls apart in the modern world of twenty-four-hour news channels. Coverage and over-coverage of rare events naturally increases the ease with which a rare occurrence can be brought to mind, thus skewing our perceptions of the probability of specific events.

Another problem faced by politicians, security officers, and anyone who makes decisions about what security mechanisms to implement is that no one wants to be a scapegoat. This leads to a lot of CYA (cover your ass) security, as it is called in the trade. A government official could reasonably say that he believes a lot of people are on the No-Fly list wrongly but probably not want to be the one to take a person off the list. The fallout if someone taken off the list later hijacks a plane is something you would not risk, even if it were a low-probability event. In fact, it is so hard to get a name off of the No-Fly list that it took three weeks to remove the late Senator Edward M. Kennedy (Goo 2004).

Furthermore, fear, uncertainty, and doubt taps into deep emotions, especially when the protection of children is involved. We will make all sorts of silly and even dangerous arguments when we think children may be threatened (Lemos

2007). With such an effective motivator to get a security mechanism implemented, few wish to take the much harder route of reason and analysis, especially when they often cannot assign hard quantitative numbers to the risk.

Conclusion

In a field wrought with fear, uncertainty, doubt, and poorly justified solutions, a consumer or citizen should ask many questions. Be skeptical if promised 100 percent security or hacker-proof services. Be skeptical if promotional materials for a product are primarily based on FUD. Be skeptical if presented an all-or-nothing choice—a false dichotomy. In that case, ask several questions. Are there hidden or non-monetary costs to this security measure? Is this just something to make us feel safer? What are all the trade-offs? Are they reasonable? Here, we must balance the competing needs of security and usability, letting neither our fear nor desire for convenience win. Does this security precaution still make sense in today's landscape, or are we just doing it out of habit? Are we just doing this because everyone else does or says it is necessary? Who are all the parties being trusted, and what are they actually being trusted to do?

Many of these are the same sorts of questions skeptics ask of any claim. Similarly, security is not the only realm that touches on deep needs and emotions that cloud critical thinking. In that sense, it is no different from any other field. However, it is a challenging place to apply critical thought—one where it is far too commonly not applied at all. □

Acknowledgments

I thank Von Welch and Jim Basney of the National Center for Supercomputing Applications for their input and feedback, and I thank the James Randi Educational Foundation for the opportunity to present the original paper upon which this article is based at The Amaz!ng Meeting 7.

Notes

1. http://passwordsafe.sourceforge.net/.

2. Cheapjunk.biz did not exist at the time this article was written. It proved exceptionally difficult to find a name on that theme that was not already registered.

References

(ISC)2. 2008. (ISC)2 code of ethics. *(ISC)2 Security Transcends Technology*, July 1. Available online at www.isc2.org/ethics/default.aspx (accessed August 25, 2009).

Becker, Shane. 2009. Arrested for taking photo of ATM. *INFOWARS.COM*, May 12. Available online at www.infowars.com/arrested-for-taking-photo-of-atm/ (accessed August 19, 2009).

Bloor, Robin. 2006. Anti-virus is dead: The advent of the graylist approach to computer protection. *TechRepublic*, September 1. Available online at http://whitepapers.techrepublic.com.com/abstract.aspx?assetid=881470&node=2094&docid=395435 (accessed August 19, 2009).

Bowers, Andy. 2005. A dangerous loophole in airport security. *Slate Magazine*, February 7. Available online at http://slate.msn.com/id/2113157/fr/rss/ (accessed August 25, 2009).

Dauger, Dean. 2007. Multicore eroding Moore's Law. *MacResearch*, October 9. Available online at www.macresearch.org/multicore_eroding_moores_law (accessed August 19, 2009).

Davis, Kathleen. 2007a. The crime of photographing (or reporting) a crime. *PopPhoto Flash*, September 21. Available online at http://flash.popphoto.com/blog/2007/09/the-crime-of-ph.html (accessed August 19, 2009).

———. 2007b. The crime of photography: Rewarded! *PopPhoto Flash*, November 19. Available online at http://flash.popphoto.com/blog/2007/11/the-crime-of-ph.html (accessed August 19, 2009).

Electronic Frontier Foundation. 2003. EFF: Patriot ACT II analysis. *Electronic Frontier Foundation*, January 9. Available online at http://w2.eff.org/Censorship/Terrorism_militias/patriot-act-II-analysis.php (accessed August 19, 2009).

Fisher, Marc. 2005. Union Station photo follies. *The Washington Post*, May 20. Available online at http://blog.washingtonpost.com/rawfisher/2008/05/union_station_photo_follies. html (accessed August 19, 2009).

Goo, Sara Kehaulani. 2004. Sen. Kennedy flagged by No-Fly list. *The Washington Post*, August 20. Available online at www.washingtonpost.com/wp-dyn/articles/A17073-2004Aug19.html (accessed August 19, 2009).

INFOSEC Research Council. 2005. Hard problem list. *Cyber Security R and D Center*, November 1. Available online at www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf (accessed August 19, 2009).

Kotadia, Munir. 2006. Eighty percent of new malware defeats antivirus. *ZDNet Australia*, July 19. Available online at www.zdnet.com.au/news/security/soa/Eighty-percent-of-new-malware-defeats-antivirus/0,130061744,139263949,00.htm?omnRef=http://www.google.com/search?client=safari&rls=en&q=eighty%20percent%20of%20new%20malware%20defeats%20antivirus&ie=UTF-8&oe=UTF-8 (accessed August 19, 2009).

Lemos, Robert. 2007. Amero case spawns effort to educate. *The Register*, June 20. Available online at www.theregister.co.uk/2007/06/20/julie_amero_it_education/ (accessed August 19, 2009).

Leydon, John. 2008. Malware still malingering for up-to-date anti-virus users. *Channel Register*, April 11. Available online at www.channelregister.co.uk/2008/04/11/panda_infected_or_not/ (accessed August 19, 2009).

Meserve, Jeanne. 2007. Sources: Staged cyber attack reveals vulnerability in power grid. *CNN.com*, September 26. Available online at www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCText (accessed August 19, 2009).

Moore, James. 2007. Are you on the No Fly list, too? *The Huffington Post*, March 2. Available online at www.huffingtonpost.com/jim-moore/are-you-on-the-no-fly-lis_b_42443.html (accessed August 19, 2009).

Nixon, Leif. 2006. The Stakkato intrusions: What happened and what have we learned? *Cluster Computing and the Grid Workshops*. Singapore: IEEE Computer Society, 27.

Null, Christopher. 2007. How do they crack your password. *Yahoo! Tech*, January 22. Available online at http://tech.yahoo.com/blog/null/13947 (accessed August 19, 2009).

Poulsen, Kevin. 2009. Put NSA in charge of cyber security, or the power grid gets it. *Wired Magazine*, April 8. Available online at www.wired.com/threatlevel/2009/04/put-nsa-in-char/ (accessed August 19, 2009).

Schneier, Bruce. 2003. *Beyond Fear: Thinking Sensibly about Security in an Uncertain World*. New York: Springer-Verlag.

———. 2006. Identity theft disclosure laws. *Schneier on Security*, April 20. Available online at www.schneier.com/blog/archives/2006/04/identitytheft_d.html (accessed August 19, 2009).

———. 2008a. The psychology of security. *Schneier on Security*, January 18. Available online at www.schneier.com/essay-155.html (accessed August 19, 2009).

———. 2008b. The war on photography. *Schneier on Security*, June 5. Available online at www.schneier.com/blog/archives/2008/06/the_war_on_phot.html (accessed August 19, 2009).

Schneier, Bruce, and Marcus Ranum. 2008. Bruce Schneier and Marcus Ranum debate risk managment. *Information Security Magazine*, October 1.

Shachtman, Noah. 2008. Air Force suspends controversial Cyber Command. *Wired Magazine*, August 13. Available online at www.wired.com/dangerroom/2008/08/air-force-suspe/ (accessed August 19, 2009).

Shattuck, Kathryn. 2008. Odyssey of state capitols and state suspicion. *The New York Times*. January 20. Available online at www.nytimes.com/2008/01/20/arts/design/20shat.html (accessed August, 19, 2009).

Tung, Liam. 2008. Signature-based antivirus is dead: Get over it. *Builder AU*, April 29. Available online at www.builderau.com.au/news/soa/Signature-based-antivirus-is-dead-Get-over-it/0,339028227,339288527,00.htm?feed=pt_schneier (accessed August 19, 2009).

Vaudenay, Serge, and Martin Vuagnoux. 2007. Passive-only key recovery attacks on RC4. In *Selected Areas in Cryptography*, ed. Carlisle Adams, Miri Ali, and Michael Wiener, 344–359. Heidelberg: Springer Berlin.

Winder, Davey. 2007. Fewer flaws FUD wars as Microsoft paints misleading picture of Linux security. *DANIWEB*. April 21. Available online at www.daniweb.com/blogs/entry1599.html (accessed August 19, 2009).