Fear, Uncertainty and Doubt: The Pillars of Justification for Cyber Security

Adam Slagell
National Center for Supercomputing Applications
University of Illinois at Urbana-Champaign
slagell [at] illinois [dot] edu

Introduction

One can readily find computer and network security courses in most computer science departments, but we are likely overly ambitious calling computer security a science. The profession certainly has the 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. Security metrics are highly desired, but they are difficult to come by. In fact, developing objective security metrics is considered to be one of the grand challenges of the field [1].

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 [2]. It is even harder to calculate the return on investment that managers like in order to make decisions about how to mitigate a risk. How much value does one give to their reputation, and how does one estimate the cost of loss of reputation due to a hack that has never happened before? Furthermore, there is a lack of good numbers on how often different industries suffer from different types of intrusions. Until recent laws were passed, companies would conceal most instances of attack from even law enforcement if they could [3]. These factors make it hard to make rational decisions about how to address the different threats from cyber attackers.

In many ways, cyber security tools are analogous to safety equipment for the manufacturing sector. Unless a company is specifically producing computer security tools, investing in security brings no direct, tangible benefits. Like making the workplace safer, the benefits are indirect. For example, hardening ones systems does not make their product faster, smaller or cheaper, but it may protect the company's intellectual property and reputation by not exposing private customer data. So security, much like workplace safety, is often treated as a non-functional requirement by management.

Where the safety equipment industry and the computer security industry really differ is that the security industry lacks standards and has no equivalent of OSHA (Occupational Safety and Health Administration). There are certainly software standards for interoperability, and there are various security standards and recommendations for government systems [4]. However, there are no universal standards for the secure configuration of computers in the commercial sector, and with the exception of banking, there are few enforced information security standards set for most industries[1].

One indication that the security industry had matured in this respect and had good metrics would be the development of cyber intrusion insurance as a common type of policy. If

[1] http://www.bankinfosecurity.com/

there were a way to solidly predict these risks, the insurance companies would be the first to create standards of practice for cyber security and sell insurance to cover losses due to such threats. However, as we said above, it is very difficult to not only calculate the likelihood of an attack in such a rapidly changing landscape, but it is even harder to estimate true cost of such an incident. The waters are too rough for the insurance industry to enter, yet.

Still, we all know something needs to be done to protect our computer systems, and we know that it must go beyond the boilerplate items of anti-virus, spam filters and firewalls. The devil is in the details though, as it is hard for even the most seasoned security professionals to agree on what mechanisms are needed in each case. These problems are a recipe for creative rationalizations, something we will show to be all too common in the justification of many security measures.

Fear, Uncertainty and Doubt

The computer security industry has a term: FUD (Fear, Uncertainty & Doubt). It is a reference to what is supposed to be the "old way" of justifying security measures and budgets to management. It is easier and often more effective to raise FUD in people's minds than to argue why they need to spend time or money on some sort of security mechanism.

Some of the best examples of FUD are seen in the modern day reporting of our 24-hour news agencies. From bird flu, to Y2K, to child predators, the next random terrorist threat or the next food poisoning "epidemic", we see plenty of FUD with little to no discussion of real risk grounded in actual facts and numbers.

FUD is not unique to security professionals or unique to seeking funding. FUD can be used by governments to justify giving them extraordinary powers [5], especially in times of crisis. It can be used by agencies within the government to grab power [6,7], and it can be used to bring funding to a particular problem [8]. When the government uses FUD, the buzzwords are often "cyber-terrorism" or "cyber-warfare" [9]. Vendors of security products also like to use FUD to sell their widgets. These often come in the form of scary and misleading statistics [10].

In addition to not being effective at telling us how to spend resources on security, FUD is very dangerous for another reason. Its overuse makes us numb to real, but less dramatic threats than cyber terrorism. It is this constant "crying wolf" that concerns us most because it can lead to inaction when a large serious threat must be dealt with quickly in the future.

Figure 1: Cold War Security Theater

*In*security at the Airport

Bruce Schneier coined a very apt term called *security theater* [11]. Once turned onto the concept, you see it everywhere. Security theater is security done just for show, or just to make people feel better. It is the placebo of our field. A great example can be seen in the public safety films shown to schoolchildren during the cold ware 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.

Security theater is not always bad. There is value in the psychological benefit it provides. However, it often costs money and resources. In those cases, one must consider whether or not it is a good investment. Resources are finite, and if we are taking them away from effective security measures, then we have a serious problem.

A more modern example of security theater costs us time at the airport, and presumably man-hours for TSA (Transportation Security Administration) agents and IT 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 "bad" people [12, 13]. How it works is 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.

The con works because there is no point at the airport where both the person's ID and the validity of the boarding pass are checked and compared to each other at the same time. Step 1: Buy a ticket with a stolen credit card from someone presumably not on the list. You can steal one yourself if you work in retail or at a restaurant, or luckily they can be purchased like a commodity on the Internet black market [14]. Step 2: Create a fake boarding pass using your real name. Most airlines allow these to be printed at home, and they turn out to be pretty easy to fake or alter [15]. Step 3: Use your real ID and fake boarding pass at the security checkpoint. If they make a mark on the fake boarding pass, make a similar one on the real boarding pass. Without computer and scanner—like they have at the gate—it is difficult for the security guard to validate the boarding pass. Step 4: Use the real boarding pass with someone else's name to board the plane. They check the boarding pass well enough here, but no one is checking the ID now—at least when flying in the United States.

While this may be a subtle problem with the No-Fly list, many instances of security theater are not so subtle and have higher costs. One of our favorite examples is that of the "3 ounces of liquid rule" in the United States. Simply stated, this rule says liquids must be in containers 3 ounces or less, and all of these containers must fit in one quart-sized Ziploc bag. This is to keep the potential terrorist from bringing on enough liquids to make some sort of explosive. Presumably, there is some minimal amount of liquids they need to create an explosive device. However, whatever that amount is, then it is only a matter of finding enough people to collude. It would in fact be almost unprecedented if there were only one terrorist aboard a plane during a hijacking! It seems the benefit is low, but the cost comes in time spent in security at the airport, the products that are thrown out because people packed too many liquids, the extra money spent to check bags because people cannot fit their necessary toiletries within the liquid limits of carry-on's, and the extra man hours of TSA agents.

The public is only lucky that the "Shoe Bomber" [16] was not the underwear bomber. It is bad enough taking off shoes through airport security. While this could be called security theater, it is more a case of addressing a very specific threat but not a general problem. It is all too easy for the adversary to switch methodologies to reach the same ends in

this case. Adding marshals to planes helps protect against many dynamic threats, reinforcing cockpit doors protects against the plane being used as a weapon regardless of how terrorists hijack the rest of the crew—be it with box cutters, ceramic knives, or socks filled with pool balls. Inspecting shoes for explosives simply makes people hide them elsewhere.

The War on Photography

An interesting case to analyze here is what has been called the "War on Photography" [17]. In recent years, people have been arrested, had their cameras confiscated, or been hassled by law enforcement for photographing particular targets [18,19]. To make matters worse, there isn't legislation to indicate what is illegal to photograph, and it is often instigated by reports from over zealous citizens or police who do not like to be photographed. Examples include, photographing an ATM, photographing police, and even photographing tourist landmarks [22,18,20,21].

The main problem with this approach is that while police may catch a terrorist photographing something, there are far, far more tourists taking pictures of landmarks and curious people with cell phones taking pictures of things they don't often 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 methodology is too high to be useful and efficient.

Furthermore, in this case there is likely nothing that can be done if law enforcement does find a terrorist taking pictures. Usually, people are not taking pictures of anything illegally unless they are trespassing. Also, one cannot reliably infer the intent of the photographer or prove it. The photographer can simply play dumb. So a potential terrorist risks little in taking photographs on the street. Even if police were a deterrence, Google images, Google Street View and other web technologies are making such reconnaissance by terrorists less necessary anyway.

Another drawback is that this is often used as an excuse to prevent people from taking photos or video of the police. This has little effect except to reduce police accountability. All in all, this sort of law enforcement practice is a very bad trade-off. One may catch a terrorist every once in a while, but only after harassing many innocent individuals and infringing upon their liberties. And even then, confiscating the camera would not get the terrorist off the street nor stop them from having a comrade try to take the photo later or from performing digital reconnaissance. To be useful, the false positive rate would have to be much, much smaller.

Back to Cyber Security

A theme we have been dancing around in many of these examples, but not making explicit, 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. One is never 100% secure and can almost always think of very esoteric threats they are not protecting against. So security comes down to using the best information one has to balance costs versus benefits. Let's look at desktop anti-virus technology.

Everyone should run antivirus software on his or her desktops and laptops, right? The landscape was very different in the late 80's and early 90's when this approach of signature-based virus detection was created. There were few viruses, they used known and old exploits, and they spread slowly. Most often, they were spread by floppy disk and not over networks to which most home PC's were not connected [23].

However, much of this has changed now. First, viruses are often polymorphic or use encryption techniques to thwart signature-based techniques, which fail at detecting as much as 80% of new malware [24,25]. These techniques of obfuscation are like creating one virus with a million different perfect disguises. This makes it difficult for any signature-based technique to match a virus. There are what we call "zero day exploits", unknown vulnerabilities used by the malware writers to spread their code quickly across the Internet, before a signature could even be created and distributed. Lastly, the signature databases have become huge—with millions of signatures—and they are growing exponentially [26]. This uses significant resources on all but the newest PC's. For a long time the exponential growth in computational power kept anti-virus technology in pace with the exponential growth of the number of viruses, however, that has begun to level off [27]. Signature-based anti-virus is simply an untenable approach to handle malware on computers anymore.

Lest it be said that we are arguing against a straw man, we recognize that anti-virus 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 of the matter 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 now since there are more pieces of software one does not want running than they do [24].

The point of this is not to say "do not run anti-virus 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 are so much more effective at preventing infection, and because signature-based anti-virus software consumes a significant percentage of a computer's resources, the author leans towards 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.

Firewalls

Another thing that people are told they must have is a firewall, even if they don't know what one is or how to properly configure one. 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 one understands 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 2 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 said the name of the software was "iTunes", the malware can call itself anything its creator wants.

Figure 2: Firewall alert

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 the adversary we imagine. Writing down a password will not make it more or less likely for an account to be compromised by an online adversary. However, putting a password on a Post It® note underneath one's keyboard at their office is a bad idea because there they have the additional threat of a nosey coworker. What if someone puts their passwords on a Post It® in their wallet? Presumably, they already put sensitive information such as their credit cards in their wallet. One has to think realistically about the threats they are exposing themselves to and weigh the trade-offs.

In this case, there can be some very bad trade-offs, especially if not writing down passwords forces the user to use simpler passwords or reuse them for multiple accounts. It is hard enough to remember a few good passwords, yet alone the dozens. Simple passwords can be easily cracked by computer software using variations of what are called dictionary attacks [28]. 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 grid community [29], 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 out there[2] which encrypt your many passwords with one strong password and even allow you to carry them

[2] http://passwordsafe.sourceforge.net/

with you on a USB flash drive. However, this goes against the often-recited warning about writing down passwords.

Website Security

One 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 [30], anyone can setup a website 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. One should ask, "Who am I trusting and to say what?" In this case, they 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 they are visiting www.example.com) is the running that web site. Furthermore, they are trusting that their web browser is correctly communicating with this website in a way that prevents others from eavesdropping on the conversation between their web browser software and the web server. While there may be reasonable doubts 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 what the lock icon is not asserting but people often assume it does.

There are several questions unanswered even if one has a "secure connection" to a web site and sees that nice lock icon. For example, how is the data handled on 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 their backup tapes that contain the consumer's data and how do they 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 still must trust the retailer to implement good security measures. This is probably not a terrible step to take if one is visiting Walmart's web site or Amazon.com. However, it is likely to be of little help if one wants to do business with the owners of cheapcrap.com[3]. 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 can be asked as to why. While this is outside the main thesis of this paper, we would like to present some of the more popular hypotheses. Bruce Schneier brings up a point we find particularly suited to explain much of our inability for reasoned risk analysis [31]. There is a mental mechanism psychologists call the "availability heuristic". This states that, "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 why we would evolve such a heuristic and how it would work well with the simpler risk analysis faced by hunter-

[3] Cheapcrap.com did not yet exist as of this writing, but the author eagerly anticipates its arrival.

gatherer's tens of thousands of years ago. However, it is just as easy to see how it falls apart in the modern world of 24-hour news channels. Through coverage and over-coverage of rare events, this naturally increases the ease with which a rare occurrence can be brought to mind, thus skewing probabilities in our minds.

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. One could reasonably say that they believe a lot of people are on the No-Fly list wrongly, but they do not want to personally be the one to take a person off the list. The fallout if someone taken off the list later hijacks a plane is something they would not risk even if it were a low probability event. In fact, the No-Fly list is evidently so hard to get one's name off of that it took 3 weeks to remove Senator Kennedy [12].

Frankly, FUD also 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 [32]. With such an effective motivator to get funding or get a security mechanism implemented, why would anyone take the much harder route of reason and analysis, especially when they cannot in the end give detailed quantitative numbers to the risk.

Lastly, some risks are just hard to deal with, especially ones that are high risk but of a very low probability. How many resources does one then apply? It is even more complicated when the risk is unlikely based on experience, but in theory the vulnerability is ripe for exploitation. While it seems unlikely that one can cause a large death toll [33] by poisoning the food supply, they can cause panic and economic damage by killing only a few unpredictably. Therefore, it would still be a very effective method of terrorism that is not too difficult to perpetrate with all the points of entry. Still, it has largely not been realized as an actual exploitation. Considering the complexity of how food is produced and distributed and how many people are involved, it would be extraordinarily expensive to revamp the whole process. Yet it still remains a serious threat that there appears to be little protection against. Addressing these sorts of risk are challenging even without faulty psychological heuristics at work against us.

Conclusion

In a field wrought with FUD and poorly justified solutions, there are many questions one should ask as a consumer or citizen. Be skeptical if promised 100% 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. One should always ask several questions. For instance, are there hidden or non-monetary costs to this security measure? Is this just something to make us feel safer? Is this a reasonable trade-off, and what are all the trade-offs? Here, we must balance the competing needs of security and usability, letting neither our fear nor desire for convenience to win. Does this security precaution still make sense in today's landscape, or are we just doing it of habit? Similarly, 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 make of any claim. Similarly, security is not the only realm that touches on deep needs and emotions that cloud critical

thinking. In that way, it is no different than any other field. However, it is a challenging place to apply critical thought and one where it is far too commonly not applied.

Acknowledgements

I would like to thank Von Welch of the National Center for Supercomputing Applications for his input and feedback.

References

1. INFOSEC Research Council, *Hard Problem List*, http://www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf
2. B. Schneier & M. Ranum, "Bruce Schneier andMarcus Ranum Debate Risk Management, *Information Security Magazine*, Oct., 2008
3. B. Schneier, "Identity-Theft Disclosure Laws", http://www.schneier.com/blog/archives/2006/04/identitytheft_d.html
4. Microsoft, *The USAF Standard Desktop Configuration*
5. Electronic Frontier Foundation, "EFF Analysis of 'Patriot II': Provisions of the Domestic Security Enhancement Act of 2003 that Impact the Internet and Surveillance" http://w2.eff.org/Censorship/Terrorism_militias/patriot-act-II-analysis.php
6. N. Shachtman, "Air Force Suspends Controversial Cyber Command", Wired Magazine. http://www.wired.com/dangerroom/2008/08/air-force-suspe/
7. K. Poulsen, "Put NSA in Charge of Cyber Security, Or the Power Grid Gets It," Wired Magazine. http://www.wired.com/threatlevel/2009/04/put-nsa-in-char/
8. J. Meserve, "Sources: Staged cyber attack reveals vulnerability in power grid" http://www.cnn.com/2007/US/09/26/power.at.risk/index.html#cnnSTCText
9. ForeignPolicy.com, "10 easy steps to writing the scariest cyberwarfare article ever." http://neteffect.foreignpolicy.com/posts/2009/04/11/writing_the_scariest_article_about_cyberwarfare_in_10_easy_steps
10. D. Winder, "Fewer flaws FUD wars as Microsoft paints misleading picture of Linux security," *DaniWeb IT Discussion Community* http://www.daniweb.com/blogs/entry1599.html#
11. B. Schneier, "Beyond Fear: Thinking Sensibly about Security in an Uncertain World," Springer-Verlag, New York, 2003.
12. S. Goo, "Sen. Kennedy Flagged by No-Fly List," Washington Post. http://www.washingtonpost.com/wp-dyn/articles/A17073-2004Aug19.html
13. J. Moore, "Are you on the No Fly List, Too?", The Huffington Post. http://www.huffingtonpost.com/jim-moore/are-you-on-the-no-fly-lis_b_42443.html
14. T. Zeller, "Black Market in Stolen Credit Card Data Thrives on Internet," The New York Times. http://www.nytimes.com/2005/06/21/technology/21data.html?pagewanted=all
15. Slate Magazine, "Boarding Pass Failure," http://www.slate.com/2152507
16. M. Elliott, "The Shoe Bomber's World," TIME. http://www.time.com/time/world/article/0,8599,203478,00.html

17. B. Schneier, "The War on Photography", *Schneier on Security*. http://www.schneier.com/blog/archives/2008/06/the_war_on_phot.html
18. K. Davis, "The Crime of Photography: Rewarded!" http://flash.popphoto.com/blog/2007/11/the-crime-of-ph.html
19. K. Davis, "The Crime of Photographing (or Reporting) a Crime," http://flash.popphoto.com/blog/2007/09/the-crime-of-ph.html
20. M. Fisher, "Union Station Follies," *The Washington Post*. http://blog.washingtonpost.com/rawfisher/2008/05/union_station_photo_follies.html
21. K. Shattuck, "Odyssey of State Capitols and State Suspicion," *The New York Times*. http://www.nytimes.com/2008/01/20/arts/design/20shat.html?_r=1&adxnnl=1&oref=slogin&adxnnlx=1210125984-qrPPfpI/kDlEi+wMrOvtEA
22. S. Becker, "Arrested for Taking Photo of ATM," *InfoWars.com*. http://www.infowars.com/arrested-for-taking-photo-of-atm/
23. R. Bloor, "Anti-Virus is Dead: The Advent of the Graylist Approach to Computer Protection," *Hurwitz & Associates White Paper*.
24. L. Tung, "Signature-based antivirus is dead: Get over it," *ZDNet*. http://www.builderau.com.au/news/soa/Signature-based-antivirus-is-dead-Get-over-it/0,339028227,339288527,00.htm?feed=pt_schneier
25. M. Kotadia, "Eighty percent of new malware defeats antivirus," *ZDNet* http://www.zdnet.com.au/news/security/soa/Eighty-percent-of-new-malware-defeats-antivirus/0,130061744,139263949,00.htm
26. J. Leydon, "Malware still malingering for up-to-date anti-virus user," *The Register*. http://www.channelregister.co.uk/2008/04/11/panda_infected_or_not/
27. D. Dauger, "Multicore Eroding Moore's Law", *MacResearch*. http://www.macresearch.org/multicore_eroding_moores_law
28. C. Null, "How Do They Crack Your Password?", *Yahoo! Tech*. http://tech.yahoo.com/blog/null/13947
29. L. Nixon "The Stakkato Intrusions: What Happened and What Have We Learned?", *In the proceedings of the Cluster Security Workshop (CCGrid '06)*, 2006.
30. S. Vaudenay & M. Vuagnoux, "Passive-Only Key Recovery Attacks on RC4", *Selected Arreas in Cryptography*, 2007.
31. B. Schneier, "The Psychology of Security", http://www.schneier.com/essay-155.html
32. R. Lemos, "Amero case spawns effort to educate," *The Register*. http://www.theregister.co.uk/2007/06/20/julie_amero_it_education/
33. G.R. Dalziel, "Food Defense Incidents 1950-2008: A Chronology and Analysis of Incidents Involving the Malicious Contamination of the Food Supply Chain", *Centre of Excellence for National Security (CENS)*, 2009.