All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Ten bad assumptions

In information protection, we often make bad assumptions that end up limiting our thought processes and driving us down potentially inferior lines of pursuit. Some of the most common ones I see – as gathered from postings in the last few days – are worth looking at again.

Bad Assumption 1: It's easy to forge digital records

It's easy to create any bit sequence you want in a digital system you have control over, but a successful forgery that will defeat a competent expert digital document examiner is far harder. Recent advances in examination methods have made it far harder to get away with forgeries, and while we see far more successful forged email attacks against end users, these fraud methods are generally not used or successful in defeating record keeping systems designed to retain reliable records of legally binding transactions.

Bad Assumption 2: IP addresses imply locations and/or people

While there was a time when an IP address could reasonably reliably indicate the location of a computer, this is increasingly less effective, and hasn't really been effective for more than 10 years. Associating people with IP addresses has never been reliable. Current online services assert that they determine the right country for IP addresses they claim to map to location more than 90% of the time, and that seems reasonably credible. The self-asserted rates are on the order of 50% correct for location within 10 miles or so and a bit better for a 250 mile radius – again only for IP addresses they have mapping data on. In terms of people, the vast majority of Internet-connected systems today have non-routable IP addresses, are mobile devices wherein IP address doesn't map to location, are behind network address translation (NAT) gateways, or use dynamic host configuration protocol (DHCP) and get different addresses over time. So there are typically any number of people that may use the same IP address over a period of seconds to hours.

Bad Assumption 3: It's easy to remain anonymous over the Internet

Just because it's not simple to map an IP address to a person, doesn't mean it's easy to stay anonymous over the Internet. For most people using the Internet today, either applications or Web browsers are used in access, and these mechanisms tend to track people, their buying habits, and other related characteristics. When a user fills out a form to purchase something from over the Internet it is common for the details to become available to multiple vendors who then track the user over time using technological methods. Using anonymizing services may have limited effect against some tracking, but subpoenas and other legal processes, flow tracking, application and browser tagents, and other similar technical approaches have been highly effective in attribution when the necessary resources are applied.

Bad Assumption 4: Effect implies cause

So-called experts in computer-related things often get this wrong. They see an effect and immediately jump to conclusions about the cause. But in the digital environment, while cause acts through mechanisms to produce effects, that does not mean that the same effect implies the same mechanism and/or cause. In fact, many causes may produce the same effect in terms of the observables typically available and the level of analysis undertaken. This ties directly into the issues associated with forgery.

Bad Assumption 5: We're the first ones to do X

Firsts declared in the computer world are rarely firsts at all – unless they are so specific that they become nearly meaningless. The first intrusion and anomaly detection systems existed before there were digital computers, the first you name it version of any fraud you are likely to identify was likely first used in computers at least 10 years before you heard of it, the zero-day attack you just learned about was likely not a zero-day for some one else for quite some time before it was publicized as zero-day, and the first [place adjective sequence here] [place noun phrase here] was likely not the first [place slightly different adjective sequence here] [place noun phrase here].

Bad Assumption 6: Teaching how to attack will teach how to defend

I am a big fan of the various venues being created to explore hacking (in the good sense of exploration). I think creative people need a good playground and playmates for the computing arena. But several initiatives underway to teach children (age 6+) how to attack, while fun and worthy in their own right, do not teach those same children how to protect themselves or others. At the same time, successful defenders do have knowledge of attacks and attack methodology. So to be clear, I am in favor of learning about attacks and testing them out in a safe way, but this has not proven an effective way – on its own – to teach how to defend.

Bad Assumption 7: Security by obscurity doesn't work

Sure it does. In fact, essentially all effective protection has elements of obscuration. Without it, any and all potential attackers are provided with all of the details they require in order to be successful in their attacks. The question of what has to be kept secret, versus what does not, is not one we have solved as a community. Limited historical experimental results show that some things related to deceptions can be revealed to positive effect in defense, but in the larger sense, there is no published scientific basis we are aware of that shows that less obscurity is harmless. So for now, only tell those that really need to know about what your protection approaches are and how they work. Otherwise, you may be fodder for anything from technical exploitation to elicitation.

Bad Assumption 8: The best defense is a good offense

While this may be true in some sports analogy, no team without a defense has ever won a Superbowl or any other championship. Tactically, all the offense there is today cannot defeat attacks. But many defenders have also failed to adequately defend, even when supplied with very substantial resources. Strategically, there are big questions still to be asked and answered. As information warfare and cybernetic warfare emerge, there is a real question about the potential for strategic deterrence. While the mutually assured destruction of the atomic age has seemingly been highly effective at keeping the peace for 60+ years, the analogy is not very clear for information and cybernetic warfare. There isn't really symmetry in the same way as there is for real WMDs, attribution is a lot harder to do with certainty, and the cold war was, by some accounts, won when the notion of a defensive shield drove the cost of assuring the offense so high that it helped bankrupt the Soviet Union.

Copyright(c) Fred Cohen, 2012 - All Rights Reserved

Bad Assumption 9: (eq equal eq)

It's obviously wrong, once you know the language. And that's the point. Lots of mistakes are made based on a lack of detailed understanding of the issues. High-level decision-makers today largely lack the clarity of understanding and quality of information required to make good strategic decisions. In large part this is because of a language gap. But even worse, the lower-level so-called experts don't have clarity of language internally that is present in other fields. The lack of common technical language and the sea of ever-changing catchy market speak that enters the security space is staggering and detrimental to effective communication and clarity of thought. Lots of the things that are made public are just plain wrong, but they sound good. And if you don't know what you are talking about, you may draw problematic conclusions. For many executives, the solution to better decision-making stems from better advice, and that comes from better advisors.

Bad Assumption 10: My folks are among the best experts there are

I have rarely, but occasionally, found this to be true. Time after time, I find folks who have been successfully attacked asking for assistance telling me that their folks are among the best security experts there are. Imagine if the dialogue went something like this:

> **Them:** My folks are the best security folks in the industry!
>
> **Me:** If that's true, why did you call me? - *OK that won't work... how about...*
>
> **Me:** Obviously not. - *OK that won't work either... how about...*
>
> **Me:** If they're so good, how come they got beat? - *Hmmm... how about...*
>
> **Me:** So are you saying that nobody can beat the 23 year old that just beat you? - *Is there a pattern forming here somewhere? how about...*

A better assumption – always – is that your folks are not the best experts out there in everything that they may have to do. Information protection is a team sport, and nobody knows it all.

Ain’t a horse that can't be rode - Ain’t a man that can't be throwed – old cowboy saying

Get used to the notion that you and your folks can always do better, and benefit from independent expert review and advice. Seek out that advice, but then consider it and make your own decisions. That's what risk management is about.

Summary

Bad assumptions lead to bad conclusions. But better assumptions don't necessarily lead to better conclusions. I like certain expressions. One of them is:

“Luck favors the prepared” - Edna (The Incredibles)

based on a far older expression:

“Chance favors only the prepared mind.” - Louis Pasteur.

Translating that to the current context, I conclude that

luck favors those with better assumptions