Fred Cohen & Associates - Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Developing the science of information protection

At the dawn of the information age, like at the dawn of every other age, wild experimentation, rampant exploration, and many fits and starts have taken place, and are to be expected. But like any revolution, at some point, society settles down into normalcy. As the madness subsides, wild speculation yields to scientific exploration. Now is the time for the scientific approach to take its rightful position in bringing light were once there was only heat.

The ancient arts

In ancient times, information protection was employed using rules of thumb, clever tricks, and closely held secrets. Techniques like passwords have been around for 5000 years, they are largely unchanged, and they still work. In fact, they still work better than any of the available alternatives. While cryptographic systems of ancient times have largely yielded to mathematical innovation, the revolution in cryptography is only about 65 years old. The revolution started with Shannon's work, which largely explained the entire history of the field in a few simple equations, and introduced the basic concepts of confusion and diffusion, introduced fundamental limits relating to the length and redundancy to cryptographic strength, and brought out the notion of workload. The revolution took a wild turn with the notion of public key cryptography about 25 years ago, and the race toward leveraging complexity advantages associated with the limited knowledge of a small amount of information against the vast array of computing power than available, and anticipated for the future. With these mathematical and scientific notions, and the understanding is they have brought about, the revolution in cryptography is largely over, and we have returned to normalcy; in that we know what to expect and the limits of what we can do.

Trojan horses, were widely publicized thousands of years ago, when a spectacular failure to look a gift horse in the mouth, resulted in snatching defeat from the jaws of victory. If it looks too good to be true, it probably is! While Trojan horses of old were of limited, but substantial, a effect over a period of thousands of years, the revolution in Trojan horses is only about 25 years old. The revolution started with computer viruses, which unified the biological concepts of evolution and reproduction with Turing's concept of universal computing, sharing, and transitive information flow, flavored with a fair bit of deception, and applied the use of complexity as leverage to drive up workload for both attacker and defender. The revolution took a wild turn when the Internet combined with the PC, drove crime and other conflicts from the physical world into the information world. The same ancient frauds and deceptions used by criminals, politicians, and warriors for thousands of years, have leveraged the advantages of information technology, automation, and the global information infrastructure, to both optimized performance, and dramatically reduce the likelihood of being caught. They leverage computer viruses as a delivery system and sociological exploitation as a warhead to monetize their understanding of influence into a powerful information age weapon.

Risk management is, perhaps, the most ancient art. Every creature that survives, does so by managing risk, on a moment by moment basis, and for the more "advanced" creatures, over longer time frames, and using higher levels of depth, to leverage brainpower over physical power. And yet, the smallest virus, it operates over the shortest timeframe, has no brain power, and no physical power to speak up, but operates essentially no depth at all, can still bring down the most advanced creature, largely because of its capacity for reproduction. In the area of risk management, species rise or fall, making decisions about when to flight and went to flee; went to feed, and when to hide; went to compete, and went to cooperate. And yet the revolution and risk management, has yet to come for the information age. Whether it's our lack of the ability to overcome our cognitive limitations, the inherent difficulty of predicting the future, the imagination of criminals and lack thereof by defenders, the infeasibility of eternal vigilance, limitations on resources based on irrational exuberance, or the desire to simply run faster and hope the lion catches someone else, we don't yet know. But we do know that in this area, we are not making substantial advances. Perhaps, it is expecting too much for the human race to survive its success. We seem unable to stop ourselves from consuming our food sources till they collapse, destroying our environment so we cannot live in at, and running our governments into the ground until revolution seems the only solution. We have a long and irrefutable history of these self-destructive behaviors, and yet we are dominant, and using our dominance to destroy ourselves.

The lack of modern science

In reading article after article and submission after submission, of pattern emerges, and the pattern is not encouraging. At the IEEE Oakland conference - perhaps the best conference in the world on the field - year after year, we see speakers and read papers that fail to do an adequate job of reviewing history, and as they are doomed to do, repeat history's spectacular failures. It is a simple lack of rigor, and nothing else, and this conference is one of the best in its field. For some reason, in the information protection field, the community does not see the need to move beyond; "I have an idea... I'll try it... it looks like it works... let's employ it... we're done." For some reason, in the information protection field, those funding the research do not see the need to apply the same levels of scientific rigor that are applied to every other field. For some reason, the notion that 80% solution is good enough has taken hold, even though we don't even know how to measure the difference between 80% and 20%. The 80% solution sounds great, but when you can't describe 80% of what, you have a serious metrics problem. And that we have. And catching 80% of the million spam attempts per day to one Web site while only signaling a false positive on 20% of the legitimate messages, leaves only 200,000 undesired emails to go through manually, and only 1/5th of the important ones missed.

Somebody once said something to the effect that science starts with systematic observation. In the information protection field, we don't seem to have the most rudimentary tools for making systematic observations, or to the extent that we have those tools, we don't seem to apply them. Like the soothsayers of old, we think we see things, we waive our hands, we find new words that sound good to express ourselves, and we convince the collective crowd of the desperate who seek some certainty in their life to send us their money, and deliver in return, something that looks, smells, and acts like something they think might work. And like those soothsayers of old, like every confidence expert that ever lived, like the politicians we complain about, unlike those who create the Trojan horses that we disdain, we make bold sweeping statements without the numbers to back them up, without the scientific methodology, rigorous process, experimental basis, calibration process, or any of the other realities that science demands. All we have are the trappings of a science.

A future outlook

The world is moving increasingly toward and into the information age. The question is: Will it be an age of enlightenment and science, or another dark age full of fear and misinformation?

At the very heart of this question is the issue of how information protection proceeds.

- If the field moves toward science, there is some slim hope for gaining a handle on the challenges of integrity, availability, confidentiality, use control, and accountability, and there is even a potential of gaining deeper understanding of not only what we can do, but what we should do for the benefit of humanity.
- If the field continues to grope in the dark, the rich and powerful part of society will protect itself by any means necessary, likely involving the creation of the new religion of security. Search everybody (else) and put (my) safety above (your) privacy. Restrict this, but not that, because it is (financially) healthy for (my part of) society.

The logic behind this may seem flawed - and indeed it is, to a certain degree. How do we know that all of that science will lead to anything more than a better set of controls by those in charge? We don't. But we do know that without a science behind protection, we will rapidly grow the dark ages of the Internet, because without enlightenment, you can never see the truth, while with it, you have a chance.

So how do we get from here to there? That, it seems, is the hard part. Science is a labor intensive process that involves meticulous thought and careful measurement. But in the information age, the rush for more, better, faster (entertainment) trumps everything. There is no sense in denying the great benefits of the fusion of location information with mapping and Internet access. You can find the closest 100 coffee shops wherever you are, and directions on how to get there. Of course if you want my little shop, it will be harder to find, because I haven't paid for the advertisement and positioning. But money has always been related to power, and the decision to spend on and sell these capabilities, not only allows them to exist, it drives them forward with ever increasing force. Find more and better ways to suck a little more money out of as many folks as possible, and you will secure and assure another great year of rising profits for a few. To do this, however, the race forward inevitably leaves the providers with limited security and their customers with little or none. Nobody wants security that they don't need, we aren't looking out for each other as much as for ourselves, and this translates into almost no research in information protection at all.

The outlook is grim for the future of the science of information protection, unless we, as a society, decide to change our approach. Private industry is fantastic at driving short-term goals, and at innovations that apply special-purpose research and development over short time horizons. But the information protection field has seen about 20 years of poor quality research resulting in little or no scientific advancement. This will continue until and unless we take a strategic approach. And that is not in the current plan as far as I can tell.