All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

Changing the leverage

Suppose a million well-funded, well-educated, well-trained, and skilled people from a wide array of disciplines and from all over the World start to spend their lives trying to destroy the information society we have built up and are starting to live in. That's the situation we are or soon will be facing as information warfare is being elevated to the highest levels of national governments across the World. It used to be that a few individuals or small groups worked tirelessly for a few days, weeks, or months to come up with an attack that would defeat a small team of defenders at a company. At the national level, teams have always existed, but even these teams were relatively small, even if they were backed up by enormous technology investments. But the game has changed.

There was a time when defenders could reasonably leverage their skills and knowledge to create systems that were unique enough or protected enough to be safe for periods of years against all but the most vicious and rare sorts of attacks. But leverage has changed heavily in favor of the attack. Today, there are almost no individuals, and very few groups, who can operate in the networked information world we have created, take advantage of most of the positives that come with it, and not be significantly harmed by attackers. Even the precautions of the most expert defenders are unlikely to stay effective for long these days. From the hardware to the firmware to the operating systems and libraries to the applications to the content they apply, nearly everything in the information environment is...

Out of control … and we like it

As a society we have, for the last 15-20 years, decided we like the free flowing wildness of the Internet, the freedom of mobile devices, the lack of effort of the cloud, the automation of the big companies and their platforms, speed and minimal effort of the credit and debit card, the instant ways of the modern cell phone / personal assistant, and everything else about the path of information technology. And who can deny the benefits to individuals and society of these magnificent tools. Many of us no longer have land lines; use VoIP services for under $20/y for global phone service and number transportability and transparency; carry our calendars, maps, address books, notes, credit cards, bank accounts, music, and all manner of other things in our pockets everywhere we go; don't even bother to write things down when going on a trip across the country; email or text each other over a global infrastructure when we are in different rooms of the same building; count on real-time mapping and Internet service while driving to tell us where to get off; and the list goes on and on.

No matter how seemingly fragile any or all of these things may look from the inside, when they reach the level of reliability under normal load that is adequate to everyday use, we run to them, and very few people even ask about how well or if it will work tomorrow. We throw the dice at the magnificence of the future vision realized in front of us, tell our phones to order us a pizza for delivery when we arrive at our next stop, and only get the anchovies by speech mis-recognition once every few weeks. And when we do, it's fun. A roll of the dice in the mystery of life. Something different, interesting, humorous, and not too harmful. And when some bad things happen to someone, it usually them and not us. We like it.

Will information warfare change this?

Global information war – World War 3 – has long been underway.[1] The intensity is just heating up a bit. But what should we do about it? Do we really expect that the population of the modern world will huddle in their homes and offices and go back to pieces of paper? I think not. If you look at strategies for defending against information attack, one of the key strategies largely ignored by the computer security industry is "run faster". But this is largely embraced by the rest of the IT world. If and as long as I can develop new technologies faster than you can figure out what they are and how they work, the theory is that you will always be behind in your race to defeat those technologies. By the time you figure out how to take advantage of today's systems and mechanisms, I will already be on the next generation. Not only that, it means that the information world has to keep paying me for the eternal upgrades, new versions, etc. Your attacks may even benefit my business by causing more churn (but buy buy) in the marketplace and thus more turns of inventory per year. Not only that, but I can lower the price if you have to buy it more often and still get more profit because the incremental cost per unit of software sold is so low. You get the perception of lower prices (it's only $1.99 after all) while I get the reality of more money.[2]

In the meanwhile, as more and more public breaches are exposed, it becomes less of a shock and less of a worry to the public at large. By now, most people in Western societies have had their credit cards changed more than once because all of the information was taken, most people have had their social security numbers stolen, and they are starting to realize that they are widely exposed anyway – to every merchant we ever applied to and all of the others they communicate with in regard to those applications, and everyone we ever worked for and all of the folks they used as vendors, and all the vendors they used, and so forth. And the world has not ended for them. Society will adapt and largely has adapted to these changes by altering the pricing and expected losses. Theft of private information is now just a cost of doing business. Corruption of records is the same thing. Denial of services is expected every once in a while, and we may change vendors because of more dropped calls, but nobody is rushing back to land lines instead of using cellular phones. It's expected as part of the new technology.

Leverage and its role

Come the role of leverage. We are now largely in a regimen of risk management. The balance of the expected gains and losses against the rate of progress in the market and the cost of protection, and risk management is largely about leverage. The attempt to use cleverness to allow a relatively smaller amount of cost and investment to gain a relatively larger amount of loss reduction and return. The goal of leverage in the "run faster" world of information technology at the bleeding edge is to continue to come up with something that gets you to the next update without too much lost revenue or increased cost. Security through obscurity? Why not? As long as you can come up with something that gets you 30 days of confusion in the attacker community that cares about attacking your systems, you have won – because you update 30 days later and their attacks are against the old version. It only harms the folks who are no longer paying you, and it acts as a motivator for them to keep paying you.

[1] F. Cohen, "World War 3: We are losing it and most of us didn't even know we were fighting in it - Information Warfare Basics", ASP Press, 2006 details why I have taken this view for the last 6 years.

[2] That's $1.99 / month for the next 3 years for a total of $71.64 for something you might have paid $50 for in the 1st place.

But some care must be taken. For example, automated attack analysis is becoming better and better. When patches are released, it only takes a matter of minutes to an hour before an attack exploiting the older version is released[3] in a computer virus that can spread around the globe in a few hours.[4] But so far, before patches are released, there is no solid evidence that it takes less than 30 days to detect an exploitable flaw. So let's look at running faster...

Security through obscurity?

Of course we have and depend on obscurity for security. We always have. But in the “run faster” paradigm, it forms a basic tenant of the art. All the defender has to do is make something obscure enough so that the actual threats seeking to attack don't figure out how to get around whatever was done for a month. If they start figuring it out sooner, we have to update more often. We then have a race between the threats and the defenders, where the defenders are in a never-ending rush to innovate and the attackers are always trying to catch up. In some sense, this is better than the current race where the attackers take their time in innovating and the defenders wait around and have to catch up after an attack works. But in any case, it becomes a race, and in races, those with more resources have advantages. And it seems that on average, the resources dedicated to innovating in information technology far outweigh the resources seeking to destroy it. So we are left with focussed attacks where threats focus larger portions of their total resources on a smaller subset of targets. And to some extent we see this today. This process can be made harder for the attacker by a number of methods, some of which I will mention here:

- **Conceal the code** so that it is not readily available to the attacker to examine. For example, deploy it directly to the end device encrypted rather than leaving it in update files on systems others have access to.
- **Obscure the code** so it is harder to understand for attack purposes. Many techniques have been available in this space for a very long time.[5]
- **Use many different methods** changing around which combinations are used. For example, if you have 5 different ways to encode a password and 7 different ways to store it and 3 different ways to accept the entry, that gives you 105 different combinations to be used, one combination every month. And along the way, come up with some other ways, so that the selection set increases with time.
- **Make things change often and forward only**, like cryptographic systems and keys. As an example, suppose the key to the next update (and the public and private keys used for the process) change with every update. If the present update updates the keys as well as the code, then breaking the keys only gets you one update and you have to do it again every month.

Of course there are many other such techniques available, but you get the idea. It's a race that may be won most of the time against most of the threats, and that is all that is required in the world out of control. You don't have to be able to outrun the tiger. You just have to outrun everyone else trying to outrun the tiger.

[3] Based on reports by industry experts updating corporate systems in a timely fashion after such releases.

[4] Giuseppe Serazzi and Stefano Zanero, “Computer Virus Propagation Models”, Tutorials of 11th IEEE/ACM Int Symp on Modeling, Analysis and Simulation of Computer and Telecommunications Systems (MASCOTS’03).

[5] See for example, F. Cohen, Operating System Protection through Program Evolution”, IFIP-TC11 `Computers and Security' (1993) V12#6 (Oct. 1993) pp.565 – 584.

Who is really responsible for defending against war?

Arguably, it is the government's job to provide for the common defense. So at the level of a massive electromagnetic pulse attack or some such similar thing, it is reasonable for commercial industry to simply ignore the threat, or at most, follow government mandates for protective controls. Similarly, if nation states or other similar interests choose to purchase companies and use those purchases to attack infrastructure or other mechanisms controlled by those companies, this again is not within the purview of companies to defend against. It is the responsibility of government to take control over such situations and the responsibility of government to create and enforce laws to provide for such contingencies. In short, defending against acts of war are beyond the rational decision-making range of institutions other than governments.

Finding more leverage

The history of defense in the information arena has largely been one of seeking perfection. But in the fast and loose information world of today, perfection is not usually an option. But just because we can't have perfection, doesn't mean we can't have sound and well thought out protective approaches. Rather than seek the lowest common denominator of low surety defenses[6], it makes a lot more sense in many cases to seek medium surety solutions[7]. These solutions tend to allow a defined level of performance against a defined threat and tend to be more tunable than low or high surety defenses.[8]

For example, the use of obscuration technologies and changing cryptographic systems and keys on a regular basis allows a tradeoff between actual attack capabilities demonstrated over time and defensive effort applied. Even if a radical change occurs at some point in time, defense-in-depth, risk diversification, and rapid adaptation allows for a short window of less protection while the system adapts as a whole back toward more protection.

There is an enormous wealth of potential in the space of changing the leverage. As an example of recent work in this area, efforts in digital forensics to use consistency analysis to detect subversion of systems and alteration of records has been increasingly successful, and is very hard to overcome. While most seem to believe that it is trivial to forge a digital record, under scrutiny, such trivial forgeries rapidly yield to detection and, in many cases, attribution.[9]

Summary

In the modern information age, perfect defense is infeasible because it is not desirable. As a society, we seek the edge between out of control and rapid progress. It is human nature to only control things to the point where they are "safe enough", and sacrificing safety for rapid change is the way we are able to progress so quickly.

The ever changing solution to information protection comes from seeking and finding better and better ways to leverage risk to gain reward. In today's environment, that means run faster and step more surely, but don't sacrifice the former for the latter.

[6] Typically known "bad" detection and similar sorts of things.

[7] Generally in the form of transforms, such as cryptography, cryptographic checksums, redundant coding, etc. and other highly predictable mechanisms under assumptions that are imperfect but largely controllable.

[8] High surety defenses tend to be things like separation and trusted system technologies. For a more detailed discussion of surety levels, see F. Cohen, "Enterprise Information Protection", ASP Press, 2008.

[9] For a more detailed discussion see: F. Cohen, "Digital Forensic Evidence Examination", ASP Press, 2008-12