It's About Time:
The Unappreciated Fundamental Metric for Security[1]

By Winn Schwartau

During the Cold War, the US defended us poor, soon-to-be-nuked citizenry, with time.

If the Soviets got it into their heads to send over a six-pack of MIRV, the US had somewhere in the vicinity of 18-22 minutes to launch our thermonuclear response over the pole. The point wasn't to defend we the citizens; it was to kill as many of their comrades as we could in response. The 18-minute window was how long we had to respond before their nukes nuked our nukes. Yeah, a ton of people would die and then there was that 10,000-year uninhabitable planet issue to work out, but the real point was MAD: deterrence through Mutual Assured Destruction. Looks like it worked.

Physical home and business protection is also measured in time and we see it in a staple of cops and robbers movies: A crook breaks into a jewelry store (or home). The alarm goes off. It dials the cops (20 seconds); the cops examine the call to make sure it looks real (20 seconds); the cops go to the scene of the crime, presumably not across the street from the police station (1-5 minutes). To be on the safe side, the robbers give themselves a maximum of two minutes for the whole heist. The quantifiable question is, how much can they steal in two minutes?

At the office, time is often the first tier of protection. You unlock the door, open it and then run like heck to the supply closet so you can enter the security code into the alarm system. You have 25 seconds to do that or, in theory, the rent-a-cops come a running in a few minutes.

But There is No Protection

The history of conflict has been based upon the military concept of Risk Avoidance through Fortress Mentality. *How high can we build the walls to keep the marauding masses out of our wheat fields, lakes and castles?* Did that approach work? The Great Wall of China was an historical insignificance. The Berlin Wall was purely symbolic and the Maginot Line was ignored by the Germans. Hunkering down in defense for an attacker's seven-year siege hasn't worked (Troy, Hussein, e.g.) and the same approach hasn't worked for the

[1] Based upon the book, "Time Based Security," by Winn Schwartau. (Free on Kindle Unlimited. https://www.amazon.com/s?k=winn+schwartau)

Internet-style hunkering down we have attempted to defend against on-line adversasries. Just look at what's happening out there!

Using Fortress Mentality in computer and network technology as a defensive method assumes that things will work as they should – but we all know they don't and won't. Take a look:

- Increasing complexity causes software and networks to fail regularly in undepredictable ways.
- Networks are amorphous. Their insides and perimeters change every second, thus altering Risk & Trust dynamically. Failure, at one point, is the only option, no matter how hard we try.
- Administrators do not know every single network ingress and egress of their network.
- Connecting enterprise networks to partner organizations with unknown security weakens a network's defensive strength.
- Seemingly harmless applications often innocently create security vulnerabilities.
- 0-Days appear daily against leading applications, operating systems, browsers and security mechanisms. Organizations have a terribly difficult time keeping up with every new one and implementing the recommended patching protcols.
- It takes time and effort to install new patches to enhance security, and they don't always work.
- Well-designed security mechanisms are all too often installed incorrectly and/or completely misconfigured.
- Administrators and tech management often turn off security controls during audits and maintenance and forget to turn them back on.
- You can't adequately test the protective value of a network with any degree of assurance beyond the exact moment it was tested.Phew!

We cannot measure the efficacy of security products or protective systems – yet, using the security 50+ year old models we still inexplicably try, over and over again. (Read on!)
What that means is, not matter how many firewalls, controls, passwords, policies or patches you apply, it's a sure bet that you won't be 100% protected. There is no silver bullet, right? And there is no such thing as a deterministic 100% Trust or 0% Risk. Nope. Ain't gonna happen.

"What about perfect firewalls that only keep the bad guys out?" I often get asked.

"Fine," I'll answer. "Show me a good IP and a bad IP address."

"Oh."

Sure, you can put in the perfect security - an air gap - but that defeats the whole purpose of networks in the first place; allow businesses to seamlessly

communicate and interact with as many other networks and people as they can for whatever purpose they choose.

So, if the conventional protection mechanisms of the static Reference Monitor and Fortress Mentality don't work, what will?

It's About Time.

Let's go back to the jewelry store.

The owners know that the store's plate glass windows represent no defense or protection at all to their millions of dollars in jewelry. It's there for show and to keep the honest people out, not the criminals.

Now, for a bit of math. Let's say that Protection, **P,** equals '0', where **P** is measured in time. One hammer and it's all over; the bad guys are inside in an instant. How much protection does that window provide?

For our network analysis purposes, let's assume that all of our protective security efforts are for naught for the reasons listed above; they only serve to keep the good guys honest. Thus, as above, the Protection value in time, **P = 0**. (That is, of course, unless your favorite security vendor is giving you a written guarantee to the contrary.) From a risk management and Trust analysis standpoint, how can we say anything different? Do we have any confidence or proof or Trust that our security mechanisms will hold up in light of new attacks or errors? And for how long can we feel secure with the latest O/S service pack, server configuration, or similar upgrade? One week? One minute? One microsecond?

Our jewelry store, though, probably has good detection mechanisms to detect the bad guys doing bad guy things: taped windows, cameras, heat, sound and motion detectors. This represents another piece of the Time Based Security approach: Detection, where **D** is also measured in time. In this case, a detection should occur in something less than a second; after all, smashing though a plate glass window is no small sonic event. So, let's say that in this case **D = 1** second.

The next and last component in the store's security is Reaction, or **R**. The reaction has several steps:

1. Dial the cops (or security force): 20 seconds. Internet notice a whole lot faster, unless the bad guys cut the Response circuits!
2. The cops analyze the call: 20 seconds
3. The cops call a cop car to respond: 20 seconds
4. The cop car comes to the jewelry store: 1-4 minutes[2]

[2] These are wildly optimistic figures, to be sure, but from the bad guy's viewpoint, it is better to remain conservative and not to underestimate your adversary.

So, the robbers are assuming **R = 2** minutes – that they have 120 seconds to commit the crime and hightail it out of the area.

Since we assume a value of **P = 0**, (no protection), the store's entire defensive posture is then measured by **D + R**, the combined time it takes the detection and reaction systems to work. In this case, **D + R = 121** seconds.

If, however, we had any confidence or Trust in the protection value of the plate glass window (bullet-proof, hammer-proof), we might use the following Time Based Security formula:

P > D + R

which says, "if the time value afforded me by a protection device is greater than the amount of time it takes to detect and respond (repair, halt) to an attack, then I have a secure environment."

The time value of **P** is the common metric in many physical examples of protection. In banks or for home security, the amount of security that vaults offer is measured in time: how long will it take a given oxyacetylene torch of a given temperature to burn through the metal wall? These numbers provide a good metric base for choosing what kind of P-products, D-products and R-products to use in a complete defensive system.

But, since we do not know the measured protective strength (P) of systems in the networking world, we conservatively assign **P** a value of 0, thus giving us a new formula:

If P = 0, then D + R = E

where **E** represents Exposure, measured in time.

For the jewelry store their **E**, or exposure time, means that their greatest risk is how much can be stolen in 2 minutes. That value is no longer an information security number but one to be used by the bean counters, risk analysts and actuarial management who assess insurance rates. Assuming the **D + R** systems work, **E** becomes a quantifiable risk-measuring tool. The goal of course, is to make good business decisions which do not eliminate risk, but lower it to acceptable limits. Thus, in TBS, we want **E** $\Rightarrow$ **0**, or Exposure time to approach zero.

To use Time Based Security in our world, then, we merely have to apply the same logic. Let's say that your network is using really a whiz-bang Intrusion Detection System and that it can detect any known attack in the universe in 10 seconds.

D = 10 seconds.

Now for reaction , **R**, which consist of three parts:

1. **Notification**: The detection tools has to do something – like notify security folks on duty. In some cases this value is as high as 64 hours.[3] Let's call it an average of 120 seconds.
2. **Transit**: The person notified has to get to a place where he can do something about the problem. Nominally I allow audiences about five minutes so as not to embarrass them. But think about the real world; corporate campuses, lunch hours, on the highway/airplane, midnight at home, weekends. How long does it really take?

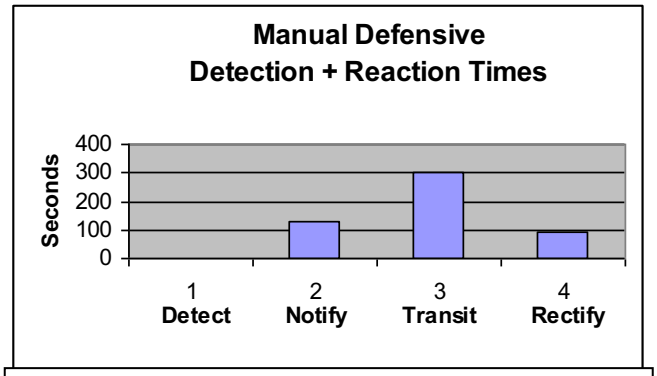

Figure 1: Take an Honest Look at Your Existing Methods of Handling Security Incidents.

3. **Rectification**: Fixing most problems appears to be the easiest for the common ones and is often less than a couple minutes according to hundreds of administrators. But, some high profile cases can take down an entire organization for hours or a day.

So the **R** (reaction) component now equals 2 minutes + 5 minutes + 2 minutes = 9 minutes, for a total of

D + R = 9 minutes, 10 seconds = E

The question the systems administrator in combination with his risk management equivalents, legal staff and auditors need to ask – and answer – is: "How much damage can occur to our networks and our company in 9 minutes and 10 seconds of unlimited access by a bad guy." (We're not looking at the insider problem yet.)

Only you can come up with that answer, but the groans are physically evident when I put audiences to this very test.

---

[3] As in the case of at least one major Defense Department advanced weapons project.

Putting it Together

This Time Based Security technique creates a new view of networks and their vulnerabilities by providing a common metric - time – to be used to gauge both risk and security under the same umbrella. We know (or should know) how fast our existing Detection and Reaction process is, even if we have no earthly idea how strong or weak our protective products and processes are.

The quantification of time to lost revenues, profits and image is not an exact science, but the DDOS attacks of February 2000 demonstrated that big e-commerce sites are already looking at time=money in web site terms.

Now the acute reader will have already thought that Time Based Security does not equally apply across the CIA infosec triad, and he is right. TBS does work in each case, but each one needs to be thought through and measured separately as breaches occur in different ways and over different time periods. There are charts and processes to apply TBS to each security fundamental.

Nonetheless, the most critical component of Time Based Security is reaction, a completely overlooked component of security.

Reaction Matrix			
		Desired	**Measured**
Detected Event (Anomaly)	**Chosen Reaction**	**Time**	**Time**
3 Bad Password Attempts	Log and Notify Admin	1 sec	2.4 secs
3 Bad Password Attempts	Turn off Account/Notify Admin	1 sec	.94 secs
Mulitple Port Scan	Initiate Trace Route	250ms	1.5 secs
Internal User - Audit Bahavior #1	Involve HR Immediately	5 mins	4 hrs
Ping of Death	Kill the Bastard :-)		
Syn-Ack Attack	Reaction # 23	2 secs	3.1 secs
Mail Bombs	Reaction # 81	10 secs	17 secs
Firewall Breach Attempt	Autofilter Source	100ms	2.7 secs
Traffic 2X Anticipated	Log and Notify Admin	10 mins	3 mins
Multiple Site Attack	Shut Down Network	3 secs	2 Days
Shut Down $ Server	Isolate Network	1 min	2.4 hours

Table 1: A Reaction Matrix is Critical for Effective Enterprise Security

Just as companies need to have a policy to implement security, they need to develop and be prepared to use a policy for reactions. Developing a reaction matrix is crucial for solving real-time security problems, but also for follow-up forensics, legal involvement, law enforcement investigation and prosecution.

The administrator needs to get the buy-off from management that under detected condition 'A' it is corporate policy for him to take reaction 'B', and then call management, the lawyers, police of aliens if necessary. I have seen companies come to a virtual halt during an attack because they had no policies or procedures in place to respond. Ideally, someone will always be on duty or available in a short period to manage security events.

Some people unfortunately think that buying the strongest firewall or other security device is the answer to their problems. Wrong. Using TBS, we find that the first steps are measure existing detection and reaction systems, then determine if they are acceptable. Getting several values to approach 0 is core to TBS. We want:

$$\mathbf{D \Rightarrow 0}$$
$$\mathbf{R \Rightarrow 0}$$
$$\mathbf{E = (D + R) \Rightarrow 0}$$

Only once we understand how the detection/response systems work with respect to our time metric can we realistically begin to choose the appropriate, risk managed choice, or protective systems.

There are many more Time Based Security formulas which really help make the information security process quantitative rather than mere guess work, but are outside the scope of this short article.[4]

1. How to determine exactly which files in a network are vulnerable
2. How to protect those files with non-traditional security techniques that require next to no products.
3. Solving Denial of Service
4. Applying Defense in Depth to Time Based Security
5. Extreme Intrusion Detection
6. Protecting against the insider
7. Tracking down the culprits

For the offensive information warrior who cares, we have also developed a set of equations for methods of safe attacks against target networks which use similar methods and metrics.

Time Based Security is not a panacea to solve all security problems, but it does offer tools to rethink the traditional view of security, and adds the necessary dynamics to reflect defense in ever-changing environments. But perhaps most importantly, TBS adds a common metric to security, where we can each measure

[4] For an in-depth examination with all of the work sheets and charts, you might find the book itself a useful tool.

aspects of our security environment, quantify them, replicate them and use them as benchmarks for performance today in the future.

If you have any comments or thoughts on how TBS can be expanded or improved, I look forward to hearing from you.

Winn