Ahmad, A. 2010. Tactics of Attack and Defense in Physical and Digital Environments: An Asymmetric Warfare Approach. *Journal of Information Warfare*. 9(1). 46-57.

Tactics of Attack and Defense in Physical and Digital Environments: An Asymmetric Warfare Approach

A. Ahmad

Department of Information Systems,
University of Melbourne,
Australia
Email: atif@unimelb.edu.au

Abstract

Asymmetric warfare is frequently described as a conflict between two parties where the 'weaker' party aims to offset its comparatively fewer resources by making use of particular tactical advantages. This paper develops a concept model that captures the leverage available to the 'weaker' party over the 'stronger' party simply because the former is attacking rather than defending. Points of leverage include choice of timing, location, method of attack, best use of limited resources and time to prepare. The leverage model is then used to discuss tactics from the perspective of the defending party. In particular, a defense-in-depth approach negates much of the natural leverage available to attackers by forcing them to engage targets under conditions that maximize the defenders own advantages.

Keywords: *Asymmetric Warfare, Information Warfare, Information Security, Physical Security, Defense-in-Depth, Network Security*

Introduction

A classic asymmetric conflict is one involving at least two parties and where the challenging party is considerably smaller in number and/or in resources to the defending party (Mack, 1975). According to Metz (2001), "asymmetry' in warfare is 'acting, organizing, and thinking differently than opponents in order to maximize one's own advantages, exploit an opponent's weaknesses, attain the initiative, or gain greater freedom of action".

This kind of unconventional warfare is becoming dominant as conflict in the physical environment has moved away from the symmetry of superpower confrontation as seen in the Cold War, to asymmetric engagement where sub-state groups are waging war against traditional superpowers (Friedman & Friedman, 1998). In the digital environment a similar scenario can be seen with hackers and organized crime syndicates taking on large corporations (Carr, 2009). Although logic would dictate that the party with greater resources will prevail in all such conflicts, in actuality it is the attacking party that tends to win such wars (Geis, 2008).

Interestingly, there was wide speculation after the fall of the Soviet Union and the end of the Cold War that peace would break out in a largely unipolar world. However, classic symmetric warfare has given way to asymmetric engagement where trans-national organizations like Al Qaida have emerged to take on members of the NATO alliance (Hoffman, 2004). The parallel digital environment has long featured conflict between the 'weaker' hackers and other such

small groups armed with unbounded time and technical knowledge of the intricacies of internetworking and computing systems on the one hand and 'stronger' corporations on the other (Carr, 2009).

This paper examines the operational aspects of asymmetric conflict and suggests that a reason why the attacking party tends to prevail is rooted in the overwhelming tactical advantages it enjoys by taking the initiative to go on the attack. Two particular cases of asymmetric conflict are profiled where the 'weaker' attacker uses natural leverage to advantage against a 'stronger' defender. The first case describes the assassination of a prominent business leader in the physical domain. Individual factors that give the attacker leverage over the defender are identified towards the development of a concept model. The concept model is then used to analyze a second case that took place in the digital domain where a civilian hacker penetrated a computer network to seize an important piece of software. Thereafter, the discussion shifts to the perspective of the defender and aims to identify general defensive tactics that reduce the leverage available to attackers.

Tactical Analysis of a Physical Security Incident

A classic example of an asymmetric engagement in the physical environment can be seen in the case of the assassination of the German chairman of the Deutsche Bank, Alfred Herrhausen on November 30, 1989 (Crawford, 2007; Hambling, 2008; Morrissey, 2007; Scotti, 1990). On this day, a large corporate organization was attacked by a (seemingly) small group of highly trained professionals. Although a number of articles refer to details of the operation, the most comprehensive description incorporating a tactical analysis is in Scotti (1990). Scotti claims that the Herrhausen assassination changed the way personal security is perceived by security professionals primarily because of the sophisticated manner in which the attack was carried out. To justify his claim Scotti conducts a detailed tactical analysis of the assassination and makes a number of observations regarding the meticulous planning and attention-to-detail of the attacking party.

The following notes summarize the events of Nov 30, 1989:

1. Herrhausen left his residence for work according to his normal routine
    a. Note that routine security was a three car armored convoy with four bodyguards (two in the lead car, two in the rear car).
2. Approximately 500 yards down the from his residence, the middle car of the three car convoy carrying Herrhausen broke a light beam generated by a photo-electric cell which triggered 44 kg of TNT to explode precisely at the rear door of the car where Herrhausen sat.
3. Herrhausen was killed instantly however his driver survived with injury

From Scotti's tactical analysis and the context surrounding the incident, a high-level conceptual model can be extracted that represents the balance of power (or leverage) between the attacker and defender in an asymmetric conflict. A number of distinct advantages can be identified from the attacker's point of view:

The first two advantages are that the attacking party chooses where and when the attack will take place. Effective use of these advantages requires the attacking party to select a time and place when the defender would be surprised and unprepared for the attack. Further, the attack

would be at a location (the battlefield) that maximizes its advantages in terms of its style of operation, expertise, and so forth and conversely disadvantages the defending party.

The attacking party in the Herrhausen case made use of these advantages. Given the Herrhausen protective detail would certainly have taken precautions such as protecting the contents of Herrhausen's daily itinerary, both the timing and location had to be predictable. The location of the attack was 500 meters down the street from the Herrhausen residence. The area had been studied for at least four weeks prior to the operation as evidenced by reports that a neighbor unknowingly handled the arming cable while raking his garden. The road, consisting of two lanes only, was narrow thereby giving the defenders little opportunity to swerve (consider the typical size and weight of armored cars), and was bordered by woods. The time of the attack was chosen to be when Herrhausen made his routine drive to work.

Thirdly, the attacker also determines the method of attack. In the case of Herrhausen the particular choice of a vehicle ambush may have been selected for a number of reasons. Bomb-making and bomb-deployment expertise may have been available to the attacking party. Another reason might be because the forensic evidence that may be used to identify the attackers was incinerated during the attack. Further, available intelligence might have pointed to the method of attack chosen. However, it is difficult to comment on the range of methods available to attackers from the information given in this single attack scenario.

Fourthly, the attacker has the opportunity to prepare for the operation prior to the attack whereas the defender must attempt to strategize (if possible) during the operation. Attacking parties may get considerable leverage from this factor especially if they are disciplined and professional. There is much evidence to this effect in the Herrhausen case. Although road-side bombs have been used on numerous occasions, Scotti notes that they have not been used effectively largely because of the inability to time the explosion with accuracy, a critical factor when it comes to targeting a moving vehicle. Scotti analyzes the tactics of the operation in detail with a view to identifying a number of salient points that highlight the sophistication with which the attackers planned and executed the Herrhausen assassination.

Among these was the comprehensive surveillance conducted and the routine patterns identified by the attacker prior to the operation. Further, the sophisticated design of the trigger mechanism, the fact that the bomb detonated when the middle car (rather than the lead car) cut a light beam generated by a photo-electric cell, that the bomb impacted the door adjacent to where Herrhausen was sitting, killing him instantly but only injuring the driver (the car was moving at the time), and that the attackers had to time the detonation precisely within a margin-of-error of less than one-tenth of a second to achieve the desired outcome.

Fifthly, the fact that the attacker knew the identity of the defender whereas the converse was not true, (subsequent research reveals that the attackers were never identified or apprehended) is another source of leverage that can be used to great advantage to the attacking party. Even after the attack has taken place the defender is unable to retaliate, as there is neither target nor trail to pursue.

Sixthly, the attacker can make best use of the resources at its disposal in the one confrontation whereas the defender, because it is unaware of when and where it will be confronted, is forced to commit sizable (defensive) resources around the clock at all points of perceived vulnerability. In the case of Herrhausen, there isn't enough information on the resources available to either side, however a hypothetical case can be made. The attacking party had the

opportunity to choose a method and a time that would enable it to make use of its resources (for example, materials needed to make and deploy the IED, skill and experience in the management of the vehicle ambush) to its best advantage. Since there was no intelligence available to the Herrhausen security team on the particulars of the impending attack there was no other option than to commit a high level of security around-the-clock.

For defending parties with many vulnerabilities (number of assets, reputation, etc) that must be protected it is difficult to maintain a high-level of readiness over a prolonged period of time. The expense incurred is another advantage to the attacker. Further, in terms of effort and resources the attacking party is again at an advantage because it simply has to look like it is capable of attacking the defender, for the defender to commit its resources. Also, if an attack does eventually take place then the attacker does not have to score a comprehensive victory; rather it simply has to appear like it was successful for the defender's reputation to suffer.

Applying the Leverage Model to an Information Security Incident

The preliminary leverage model will now be applied to a real-life account of a hacker attack. In this incident, an important piece of software (the source code of a cellular phone that allows users to modify their behavior so they can evade cellular tracking and surveillance) was stolen from Tsutomu Shimomura, a computer security expert who was working at the University of California, San Diego (UCSD) at the time.

According to Shimomura's version of events surrounding the attack on his computer network, the following key events took place on the 25/12/94 (Shimomura, 1995; Shimomura, 1997):

1. An IP spoofing attack was launched from toad.com (the attack came from a computer located in a private residence known as 'Toad Hall'). The first probes were aimed at mapping out the trust relationships between the systems on the target network. The attacker had already gained root access on toad.com.
2. Six minutes after the initial attack, the trust relationship between two systems located on Shimomura's home network - 'Rimmon' and 'Osiris' was exploited.
    a. A large number of connection requests were made in order to fill the connection queue on server 'Rimmon' (SYN Flooding). These requests were made to 'gag' the server so it wouldn't respond while the intruder masqueraded as Rimmon in order to establish a connection with another server called 'Osiris'. Osiris had a trust relationship with Rimmon.
3. The attacker then proceeded to study the behavior of the target server Osiris determining a particular number that was then used to authenticate its credentials thus establishing a communication channel from which commands could be given to Osiris
4. The attacker then used his new privileges to instruct the server to trust all external network connections and all external users. The attacker then connected to Osiris.
5. From Osiris, the attacker inserted a special program named 'Tap-2.01' into the kernel via loadable kernel modules allowing him to jump from Osiris to another computer 'Ariel' despite the absence of a trust relationship between the two computers.
    a. Tap allowed the intruder to hijack an existing network session (that is an already authenticated login session) between Osiris and Ariel that had been previously established by Shimomura and was still active. In essence, the intruder had used the network session as a portal between the two computers.
6. The intruder then copied across sensitive information (the object of the attack) from the victim's account on Ariel.
7. The intruder attempted to hide his/her tracks by modifying the system logs

Each factor from the asymmetric model developed in the previous section will be analyzed to further develop the model and to understand the significant role it plays in the success of an attack.

Choice of Location

The choice of location in this scenario was not to the advantage of the attacker but rather the defender. The 'location' in the Shimomura case was the particular server where the software oki was located. This location was not directly accessible to the attacker so the challenge of the attack was quite different to the Herrhausen case. Here the challenge was getting access to the location. The only issue with timing was to ensure the attack would not be disrupted (according to Shimomura, a previous attack that had aimed to steal the same software was prevented when the owner of the software realized the attack was in progress and pulled the Internet connection off the target host machine).

Recall that in the Herrhausen case 'location' signifies where the asset is to be found which is not necessarily fixed to one place. Therefore, the attacking party had a choice of possible locations where the attack could be staged. They chose the most predictable combination of time and location – when Herrhausen would leave his house for work in the morning.

The Shimomura case raises an interesting angle that can contribute to the tactical model. Although attackers have (in principle) a choice of location, the choice can be restricted by placing the potential target in a location that is inaccessible to the attacker. In this way the defender can force the attacker to engage the target within a carefully designed defensive system that maximizes the advantages to the defender rather than the attacker. This is the principle by which castles and fortified cities are made. If the king stays inside his castle then the opposing army has to penetrate the castle's defenses to get to him. While the opposing army is busy trying to penetrate, the defending army is able to attack from a position of strength (for example, from within towers and from behind fortified walls). In this way there is a role reversal where the attacker's advantages are effectively diminished while the defender's advantages are increased.

Choice of Timing

The attacker used timing to his advantage by staging the attack on Christmas day. Tsutomu Shimomura was far away from home visiting friends and the attack was timed to take advantage of his absence. The 'Tap' software would not have worked had Shimomura used the remote login session from Osiris to Ariel (while the attacker was trying to hijack it).

Choice of Method

Like in the Herrhausen case, it is difficult to comment on the range of options available to the attacker from a single scenario. The attacker chose tools and techniques that were successful in penetrating Ariel. This implies either that the attacker was aware of the configuration of Ariel or that he/she was prepared for a range of situations for which the tools were on-hand. Regardless, the sophisticated nature of the attack is clearly the central focus of the story of Takedown. The hacker used his/her ability to advantage by spoofing their way into Shimomura's home network and then hijacking an open connection to access Shimomura's work computer and the target software.

Preparation Prior to Attack

Considerable evidence from the storyline of Takedown points to the fact that preparation had been made prior to the attack on Shimomura's network. The attacker was pursuing the source

code of a cellular phone that would have allowed the hacker to evade cellular tracking and surveillance. He had apparently targeted Mark Lottor, a hardware hacker who sold diagnostic and surveillance tools for cellular phones. The attacker's first attempts at stealing the software were stymied by Mark so he/she targeted Tsutomu Shimomura as he had assisted Mark Lottor in the engineering of the code.

The duration of the entire attack on Shimomura's network, from reconnaissance (14:09 PST) to the exploitation of the existing channel from Osiris to Ariel (14:51 PST) took about 42 minutes. During this attack mainstream tools and techniques were used as well as specialized tools specifically engineered to hijack a network session. It appears that the attacker had conducted his reconnaissance on-the-fly, mapping the trust relationships between Shimomura's computers from toad.com. However, use of the Tap to hijack the connection from Osiris to Ariel may suggest that the attacker was aware that there was an existing connection from Osiris to Ariel.

Immunity from Retaliation

One of the key distinguishing factors between the Herrhausen case and the Shimomura case is the issue of anonymity. The party that attacked Herrhausen managed to keep their identity secret in the lead up to the assassination and apparently did not leave any clues on the scene of the crime either. Smaller parties are particularly vulnerable to larger parties as the former usually cannot protect their fixed asset from a focused attack by the latter. The only way to escape the inevitable wrath of the larger party is to become out-of-their-reach or maintain anonymity.

Although Shimomura alleges the attack was committed by 31 year old hacker Kevin Mitnick, a later text by Jonathon Littman counters by suggesting that Mitnick was not behind the attack and that the culprit was was possibly a third party (an Israeli Hacker) (Littman, 1996). If Shimomura is correct in his suspicions then Mitnick did not seem to capitalize on the advantages of remaining anonymous and this mistake eventually lead to his arrest. Shimomura puts forward some evidence to support his claims. There was enough contextual information to suspect Mitnick to begin with. He had revealed his interest (and apparent motivation) in the cellular phone software to Mark Lottor during a phone conversation and even queried Shimomura's involvement in the engineering of the code. Subsequently he penetrated Shimomura's network and left a number of voice messages taunting him.

Best Use of Resources

There was not enough information in the scenario (as it was told from Shimomura's perspective) to determine if the attacker made best use of his resources.

Defender's Perspective: Reducing the Leverage to the Attacker

In general, without forewarning of an attack and/or a clue to the identity of the attacker, not much leverage is available to parties on defense. Since the defender is unlikely to know the timing and the location of the attack, they are likely to be caught unprepared and in a location of disadvantage. In fact, the particular type or method of the attack might be deliberately chosen to exploit the defender's vulnerabilities. This tactic also reduces the likelihood of an effective defense (see figure 1 for more description of the defender's situation).

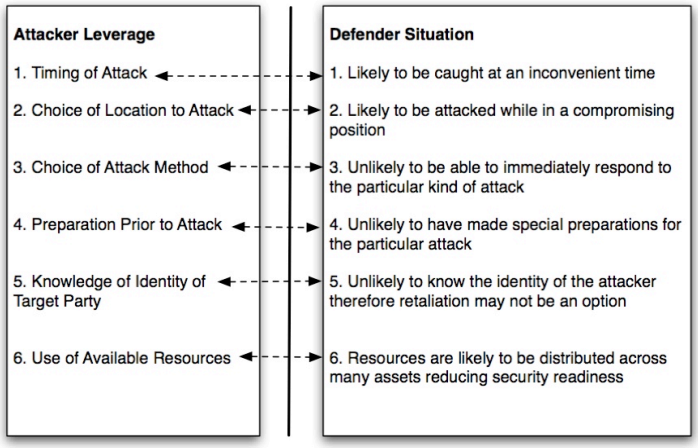

Figure 1: Opportunities for Leverage to Attacker

The overwhelming advantages to the attacker has given rise to the strong belief among physical security professionals that a determined assassin is like 'a force of nature' and cannot be stopped at all (Marquart, 1999). However Marquart believes this notion is 'ridiculous' and argues instead that assassins can be deterred by 'security presence'. He suggests that assassins choose their target well in advance and carefully consider security measures around the target when deciding on a course of action. In all the examples Marquart presents, the would-be assassin is deterred by the heavy security presence around the target so the assassin chooses a softer target instead. It must be noted though, that in these cases the assassins begin their mission with more than one target in mind and were motivated by a desire to kill a public figure rather than a specific person.

The Herrhausen and Shimomura cases appear to be in a different category to the cases that Marquart brings up. Firstly, the level of sophistication and the meticulous planning and execution of the attacks outstrip the opportunist killers in the Marquart examples. Secondly, the targets (Herrhausen and Shimomura's network) were already hardened - Herrhausen was riding in an armored three-car convoy with four specialist bodyguards. The cellular phone software in the Shimomura case was on Ariel, which did not share a trust relationship with Shimomura's home network (although there are other measures that Shimomura did not take like using packet filtering effectively).

The problem with Marquart's approach is that although a visible security presence does act as a deterrent, to the dedicated attacker it poses a challenge, that is encouragement to analyze and then 'crack'. Essentially, focusing on a show of force - 'security presence' serves to escalate the conflict rather than defuse it. The same mentality is prevalent with information security professionals. They tend to focus on purely preventive measures like firewalls to block out hackers. This tactic works to deter amateur script kiddies but encourages more competent hackers to learn about the defensive perimeter and then penetrate it. While the hackers take the opportunity to learn about the security system in place, the defender remains relatively oblivious to the escalating levels of risk.

Interestingly, it is not Marquart but Scotti that identifies a means of reclaiming some of the leverage available to the attacking party. He points out that the key to a successful defense lies in the need of the attacking party to conduct significant surveillance and intelligence collection on the target prior to the operation. During this phase the attacking party will reveal itself (whilst making enquiries, putting in support infrastructure for operations, or conducting surveillance) – during the Herrhausen case the arming cable was handled by a neighbor, who

had no idea what it was. Further, the explosive carrying satchel was lying in position for weeks before the attack. Scotti points out that had the anti-surveillance been more comprehensive, the satchel should have been discovered.

This tactic can be seen working in the Shimomura case as the Shimomura attack was preceded by recon probes from toad.com. Unfortunately anti-surveillance is more problematic in the information domain given the large number of automatic probes that are leveled against networks in general. These form a 'fog' of sorts from within which reconnaissance can be carried out with ease (anti-surveillance of this kind is somewhat infeasible). There are more effective means of anti-surveillance such as the use of a false network perimeter (that extends beyond the real network perimeter) to filter out script kiddies from more competent hackers and the use of honeypots and honeynets to discover the nature and intentions of hackers is a way of regaining some leverage against an attacking party doing its 'homework'.

The leverage model can be used to identify principles for defensive tactics which in turn reduce the leverage available to the attacker (summarized in figure 2):

An unpredictable routine in the case of Herhausen would have made it more difficult for the attacker to choose a reliable time to mount the road-side operation. Restricting the choice of location to the attacking party can be another way to reduce their leverage. For example, where the target is an object like the source code in the Shimomura case (or the more traditional 'king' in a medieval sense) the object can be immobilized at a location within a defensive system (like a fortified computer network or a castle) forcing the attacker to penetrate the defenses and then conduct the operation in a place of the defender's choosing - note that in this case, unpredictability is sacrificed for inaccessibility as the king is definitely housed within castle walls but is largely inaccessible. Following from the preceding logic, a combination of inaccessibility and unpredictability can be used to reduce the choice of attack method and the time available for preparation. For example, in the case of a defense-in-depth system of castle walls, the attacker's options of attack are reduced and in contrast the defender's options in terms of combating the attacker while penetration is in progress are increased (see the following section for more a more detailed discussion of defense-in-depth).

Preparation for attack and efficient use of attacker's resources can also be reduced by making the target's routine so unpredictable that the attacker is forced to seize any opportunity and whatever resources are at hand regardless of whether it is prepared or not or whether the resources are appropriate or not. Finally, knowledge of the target party can be denied to the attacker by obscuring any information of value to the attacker from an operational perspective. Although 'security through obscurity' has been widely dismissed as a legitimate strategy (Simson and Spafford, 1996) (the argument being that 'good' security systems are those that are difficult to 'break' despite the attacker knowing all flaws and vulnerabilities), this tactic has its place in 'defense-in-depth' where it functions as a 'speed bump', that is one obstacle in a series. This strategy would focus on the routine timings/locations where the target can be attacked but also include a range of other kinds of information such as known vulnerabilities.

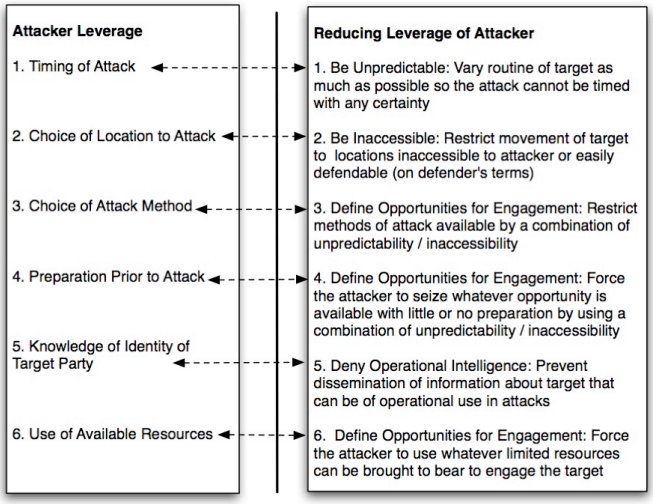

Figure 2: Reducing Leverage of Attacker

How Defense-in-Depth Reduces Attacker Leverage

The fundamental principle behind the defense-in-depth model is the placement of defensive layers between the attacker and the object of attack (for example a series of perimeter walls of varying heights that enclose a single building or small town or village). This is certainly not a new concept. In fact the tendency to surround asset(s) with a single 'wall' of collective security that keeps the 'bad guys' out and the 'good guys' in, is the standard method of security in the physical and digital domains. However, the defense-in-depth model is a far more sophisticated tool if it's true potential is realized. The following points demonstrate how the defense-in-depth model can be used to negate/reduce almost every advantage the attacker has according to the leverage model.

The leverage model states that the fact that the defender is unaware of the location and timing of an attack before the attack takes place makes it extremely difficult to gather resources to mount an effective defense. However, the defense-in-depth model encourages the defender to place the object of attack behind a series of layers like a castle (for this example we will not address mobile defense-in-depth scenarios). In this way the choice of location falls to the defender rather than the attacker. If the castle is placed on high-ground like a hill or a mountain then an approaching attacker can be spotted from miles away. This advantage allows the defender to gather resources, send messages to nearby castles for help and initiate 'lockdown' in preparation of the attack.

The choice of attack method available to the incoming party is restricted by the fact that the perimeter walls must be breached before the asset becomes accessible. Only those methods that allow the walls to be attacked are useful thereby narrowing the choices available to the attacker and making those choices known to the defender prior to the attack so the defender has ample opportunity to mount a tactical defense. In medieval times the typical means of attacking castle walls involved heavy machines (siege towers, ballistas, trebuchets and so forth) that would either have to be transported by the attacker to the perimeter walls consequently reducing the speed and stealth of an approaching attacker or constructed on-site which took time and implied the army had to include carpenters and transport necessary materials.

According to the defense-in-depth model, the primary aim of the walled system is to delay the attacker from penetrating the city's defenses long enough so that the castle can be rescued by allied armies garrisoned in nearby castles and fortresses. At the heart of this philosophy is the

realization that no defensive system can keep a motivated and resourceful attacker at bay indefinitely.

But the defense-in-depth system is actually an asymmetric warfare tool. Using this system a small number of defenders can effectively defeat a large number of attackers. Firstly, a well designed system of walls was always difficult to destroy even with heavy machinery (e.g. the siege of Constantinople by the Ottoman Army in 1453). Secondly, the system of walls may have towers along the walls from where defenders will be able to engage the attacking army from a position of relative safety. The attacker is likely to be distracted from attacking the walls while continually suffering losses of resources (manpower and machinery). In this way, the attacker is forced to expose itself to retaliation while it (slowly) breaks down the perimeter defenses.

Although not the focus of this paper, these advantages can be utilized by modern organizations when designing their perimeter networks. One might jump to the conclusion that a firewall is the virtual translation of a perimeter wall. But this is not exactly accurate, rather the firewall is the gate, and as long as every network connection has a gate (a managed firewall) and there are no gateless (unguarded) network connections between the organization and untrusted territory, then there are no holes in the perimeter.

A multiple walled perimeter system can be modelled on a network by placing a series of firewalls rather than a single firewall. Although routing traffic through multiple firewalls does have a negative impact on performance, the notion of a DMZ has taken hold and used effectively to introduce proxying and other tactical defensive maneuvers to prevent external traffic from interacting directly with mission critical servers. However, the real defense-in-depth advantage from creating multiple layers on the perimeter is a tactic rarely utilized on modern day networks. This technique, as previously mentioned, involves the use of a false network perimeter that extends beyond the real network perimeter allowing organizational security to filter out less competent attackers so resources can be gathered and concentrated on negating the threats posed by more competent adversaries. Further parallels can be drawn between the defensive tactics used on the perimeter of the castle and the perimeter of the network, however these will be examined in detail in a future paper.

Shifting Leverage After the Attack

An interesting observation proceeding from the leverage model concerns what happens after the attack takes place (figure 3). Prior to the attack (time=t0), the majority of the leverage is with the attacker whereas the defender has relatively little leverage. But if the defending party survives, then after the attack (after time=t0) it will typically have considerable time and resources to investigate the identity of the attacker and then retaliate against the interests/assets of the attacker. Now the attacker must go on the defense and focus on surviving attempts by the defender to retaliate in kind. Hence the leverage to the attacker drops dramatically in figure 3.

As figure 3 shows in describing the leverage to the attacker post-event, anonymity is key to the survival of the attacker-turned–defender. Although in the case of the Herrhausen attack, the offensive party was never publicly identified (perhaps this is why the road bomb was chosen as the method of attack as much of the evidence would be incinerated), this is quite rare given the advanced forensic technologies available to corporations and governments and the amount of time they have at their disposal. In fact one might speculate that in the hacking case (if Mitnick was the real attacker as per Shimomura), had Mitnick realized and expected this shift in leverage, he may not have been so eager to reveal his identity to Shimomura.

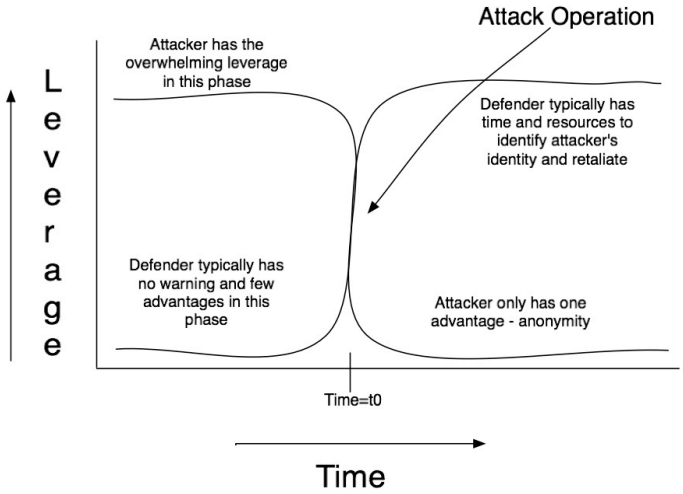

Figure 3: Attacker – Defender Leverage Graph

Conclusion

In warfare, smaller parties have much to gain by going on the offensive against larger parties. Choice of timing, location, method of attack, best use of limited resources and time to prepare - all allow the attacking party to leverage their comparatively inferior resources against a stronger adversary. However, it must be pointed out though that once the attack has taken place, the advantages fall heavily on the defender's side since it has considerable time and resources to mount an investigation to determine the identity and location of the attacking party. This is not a problem for an attacker that plans to disappear permanently once the aim is achieved. However, if the attacker is vulnerable to retaliation then it is extremely important for it to maintain anonymity in the preparation stage of the attack as well as during the operation itself.

Although there is considerable leverage to the attacker prior to the attack itself, there is much defenders can do during this period to restrict the leverage available to attackers. In particular, defenders can force attackers to engage targets within a carefully designed defensive system that maximizes the defender's own advantages. The classic defense-in-depth model that positions a series of obstacles or challenges between the target and the attacker is an example of such a philosophy. Useful parallels can be drawn between castles and networks that can further enhance the security of modern organizations. However, in modern warfare not all targets can be protected by a sophisticated shield of defensive obstacles. In such a case, unpredictability and 'security by obscurity' (as previously discussed) may be used to the advantage of the defender where the target must remain mobile.

Further Work

This paper developed a concept model that identifies points of leverage that have been used by attackers in the physical or digital domain. The second phase of this research aims to give this model discriminating power such that, when applied to an existing defense strategy, the model can be used to determine to what extent are the points of leverage to the attacker effectively diminished? One of the key aims in developing this model is to compare the leverage available to defenders in the physical battlefield to that of the digital battlefield. This discussion will seek to better understand the influence of the nature of the battlefield on offensive and defensive strategy. Also, more in-depth examination of defense-in-depth tactics

used on the perimeter of castles is intended over future papers. Lessons drawn from castle perimeters will be applied to network perimeters in to evaluate and improve current approaches to network (perimeter) defense.

REFERENCES

Carr, J. (2009) *Inside Cyber Warfare: Mapping the Cyber Underworld*. O'Reilly Media.

Crawford, D. (2007, September 15). The Murder of a CEO. *The Wall Street Journal*, p. A1

Friedman, G., & Friedman, M. (1998), *The Future of War: Power, Technology and American World Dominance in the Twenty-First Century*, St Martin's Griffin, New York, NY.

Geis, J. (2008). "The Strength of Weakness: Why the Weak Win in Asymmetric Warfare" Paper presented at the annual meeting of the MPSA Annual National Conference, Palmer House Hotel, Hilton, Chicago, IL Online. Retrieved from http://www.allacademic.com/meta/p267874_index.html on April 13, 2010.

Hambling, D. (2008, July 29) Superbomb Mystery: The Herrhausen Assassination. *Wired Magazine*. Retrieved from http://www.wired.com/dangerroom/2008/07/the-assassinati/ on April 13, 2010.

Hoffman, B. (2004). "The Changing Face of al Qaeda." Studies in Conflict and Terrorism. 27.6, November/December.

Littman, J. (1996). The Fugitive Game: Online with Kevin Mitnick: The Inside Story of the Great Cyberchase, Little, Brown & Co. Inc., Boston, MA.

Mack, A. (1975). Why Big Nations Lose Small Wars: The Politics of Asymmetric Conflict, World Politics, 27 (2):175–200.

Marquart, J. (1999). Can a Determined Assassin be Stopped? Security Management, 43 (4): 109-110.

Morrissey, M. (2007). Alfred Herrhausen – terrorist victim? In *Looking for the Enemy* (pp. 69-71). Lulu.

Scotti, A. (1990). A calculated assassination: how a German executive and his protection team were outwitted by terrorists and how further such attempts can be thwarted. Security Management. American Society for Industrial Security. 34 (11): 27-31

Shimomura, T., and Markoff, J. (1995). *Takedown: The Pursuit and Capture of Kevin Mitnick, America's Most Wanted Computer Outlaws - by the Man Who Did It*, Hyperion Press.

Shimomura, T. (1997). Tsutomu Shimomura's newsgroup posting with technical details of the attack described by Markoff in NYT, URL http://www.gulker.com/ra/hack/tsattack.html, Accessed 21Oct 2009.

Simson G. and Spafford, G. (1996). *Practical Unix and Internet security (2nd ed.),* O'Reilly & Associates Inc., Sebastopol, CA.