2009

Tactical Analysis of Attack in Physical and Digital Security Incidents:Towards a Model of Asymmetry

Atif Ahmad
University of Melbourne

DOI: 10.4225/75/57a7f5179f483
Originally published in the Proceedings of the 10th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 1st-3rd December, 2009

Tactical Analysis of Attack in Physical and Digital Security Incidents: Towards a Model of Asymmetry

A. Ahmad
Department of Information Systems
University of Melbourne, Australia

Abstract

Asymmetric warfare is frequently described as a conflict where 'weaker' parties aim to offset their relatively inadequate resources by using particular strategies and tactics to their advantage. This research-in-progress paper develops a concept model of asymmetric warfare that represents 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 resulting concept model is used to discuss generic defensive strategies that can be applied by 'stronger' parties in the physical and digital environments. For example, defenders can make their assets difficult to access except under limited circumstances such as a carefully designed defensive system. In this way attackers are forced to engage targets under conditions that maximize the defenders own advantages.

Keywords

Asymmetric Warfare, information warfare, information security, physical 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). This kind of 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. In the digital environment a similar scenario can be seen with hackers and organized crime syndicates taking on large corporations. Although logic would dictate that the party with greater resources should prevail in all such conflicts, in actuality the attacking party is very much capable of 'winning' wars in part due to the overwhelming advantages it enjoys as the attacker rather than the defender (Mack, 1975).

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 transnational organizations like Al Qaida have emerged to take on members of the NATO alliance. 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.

This paper profiles two particular cases of asymmetric conflict 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 gave 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 takes place in the digital domain where a civilian hacker penetrates 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. On this day, a large corporate organization was attacked by a (seemingly) small group of highly trained professionals. A tactical analysis of the event is detailed 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 event of Nov 30, 1989:

1. Herrhausen left his residence for work according to his normal routine
    a. Note: Routine security was a three car armoured 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 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 a neighbour that unknowingly handled the arming cable while raking the garden. The road consisted of two lanes only, was narrow thereby giving the defenders little opportunity to swerve (consider the typical size and weight of armoured 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 analyses 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 were 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 was a shaped charge that released its full blast on the door adjacent to where Herrhausen was sitting, killing him instantly but only injuring the driver (keep in mind 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, (it appears from the article and subsequent research 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 (e.g. 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 MODEL TO AN INFORMATION SECURITY INCIDENT

The preliminary Asymmetric Warfare model will now be applied on a real-life account of a hacker attack. In this incident, Kevin Mitnick stole an important piece of software (the source code of a cellular phone that would have allowed Mitnick to modify its behaviour so he could evade cellular tracking and surveillance) from Tsutomu Shimomura, a computer security expert who was working at the University of California, San Diego (UCSD) at the time.

According to the text, the following key events took place on the 25/12/94 (Shimomura, 1990; 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 behaviour 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; He 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 a new computer called 'Ariel' despite the absence of a trust relationship between the two computers
    a. Tap allowed the intruder to hijack an existing network session (i.e. 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. Note that the intruder attempted to hide his tracks by modifying system logs

Each factor from the asymmetric model developed in the previous section will be analysed 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 Mitnick case was the particular server where the software oki was located. This location was not directly accessible to Mitnick 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 (a previous attack by Mitnick aimed at stealing 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 isn't 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 Mitnick scenario raises an interesting angle which 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 (e.g. 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

Mitnick 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 Mitnick 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 Mitnick from a single scenario. Mitnick chose tools and techniques that were successful in penetrating Ariel. This implies either Mitnick was aware of the configuration of Ariel or that he was prepared for a range of situations for which he had the tools on-hand. Regardless, the sophisticated nature of the attack is clearly the central focus of the story of Takedown. Mitnick used his hacking ability to his advantage by spoofing his way into Shimomura's home network and then hijacking an open connection to get on to Shimomura's work computer to get access to the target software.

Preparation Prior to Attack

Considerable evidence from the storyline of Takedown points to the fact that Mitnick had made preparations for the attack on Shimomura's network. Mitnick was pursuing the source code of a cellular phone that would have allowed him to ultimately modify its behaviour to evade cellular tracking and surveillance. He had previously targeted Mark Lottor, a hardware hacker who sold diagnostic and surveillance tools for cellular phones. Mitnick's first attempts at stealing the software were stymied by Mark so he 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 Mitnick used mainstream attack tools and techniques but then also used the Tap tool that was specifically engineered to hijack a network session. It appears that Mitnick 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 Mitnick 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 Mitnick 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.

Mitnick did not seem to capitalize on the advantages of remaining anonymous. 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.

Had the identity of the attacker (Mitnick) remained obscured, Shimomura (and others) may not have been able to focus their skills and effort on apprehending the target in the first place.

Best Use of Resources

There was not enough information in the scenario (as it was told from Shimomura's perspective) to determine if Mitnick 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).

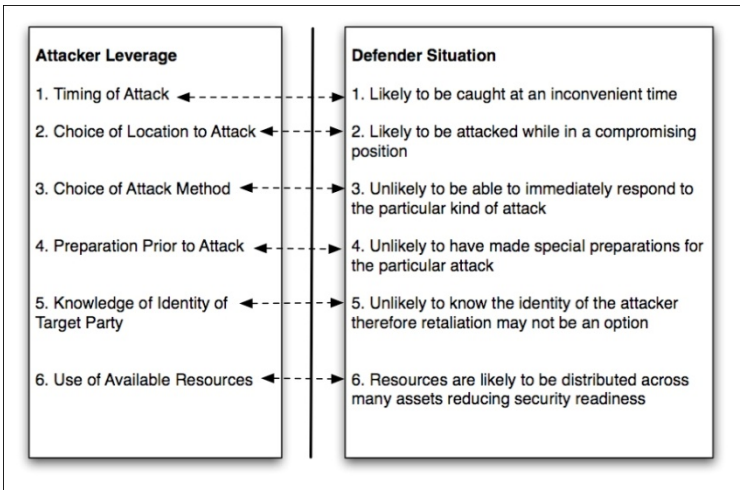

Figure 1: Opportunities for Leverage to Attacker

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 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 Mitnick 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 armoured three-car convoy with four specialist bodyguards. The cellular phone software in the Mitnick 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, i.e. encouragement to analyse 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 at hand.

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 neighbour, 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 Mitnick 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 levelled 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 Mitnick case, the object can be immobilized at a location within a defensive system (like a castle or a fortified computer network) 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. 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', i.e. 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.

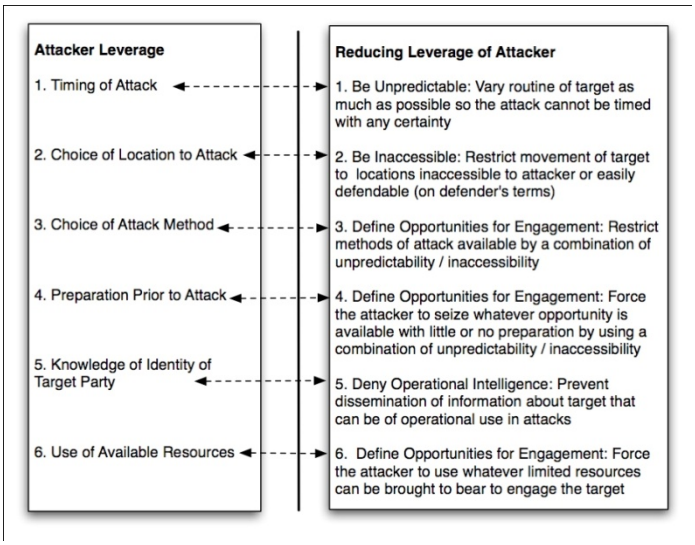

Figure 2: Reducing Leverage of Attacker

An interesting observation proceeding from this model is that after the attack takes place (figure 3). Prior to the attack taking place (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 survive 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 after the event has taken place, 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 as well as the time they had at their disposal.

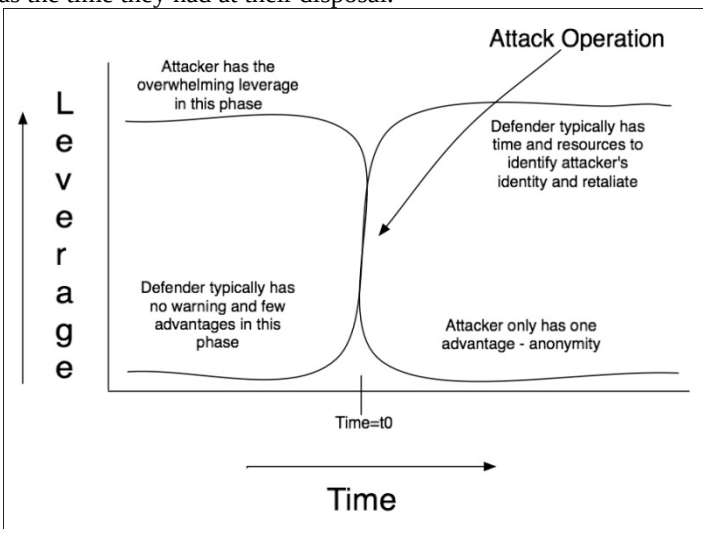

Figure 3: Attacker – Defender Leverage Graph

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 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. 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 the points of leverage to the attacker are 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.

REFERENCES:

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.

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. & 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, Retrieved October 21, 2009, from http://www.gulker.com/ra/hack/tsattack.html

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

COPYRIGHT