Global Information Assurance Certification Paper

Physical Security vs. Information Security:

Redefining the Layered Information Security Model

Version 1.0

Submitted by:

Brian D. Taylor

Tucker rubbed his cold hands together and took another sip of his tepid coffee. Even with gloves on, the bitter Pyongyang winter air chilled him to the bone. The old but venerable Mitsubishi Fuso truck had few amenities. Heat was just one of the comforts missing, however Tucker paid it little mind. "Clean" vehicles were very difficult to come by in North Korea and the Fuso was sturdy enough to carry its payload to the destination. In his line of work, John Pae was known only by the name of "Tucker". Born of South Korean immigrants who had defected to Seoul years before his birth, Tucker had both the look and the demeanor of a maintenance technician coming to do regular maintenance at the *Democratic People's Republic of Korea Strategic Missile Facility #5*. Though he was already fluent in Hangeul from his upbringing, several years at the Defense Language Institute, Foreign Language Center in Monterrey, California had honed his linguistic skills to a razor's edge. Tucker could speak gutter Hangeul with a Hyesan accent of a blue-collar working man. Tucker took another swig of his coffee and turned up the radio slightly. The Fuso's old radio could only pick up state-sponsored radio programs that blared patriotic music or the usual propaganda, but the appearance of normality had to be maintained.

As the queue at the gate got shorter, Tucker nudged his truck forward far enough to see the gate guards. The gray uniform and red shoulder patch indicated that Intelligence had finally been correct for a change. The guards were indeed ProTec employees. ProTec was one of the few privatized security companies in North Korea that had sufficient clearance to get contracts at military and government installations. It was rumored that North Korea's ruler Kim Jong Il had ProTec provide security at his winter home down in Haeju. Aside from their distinguishable gray military styled uniforms, every ProTec guard was usually armed to the teeth. The gate guard carried a Russian AKMS rifle and his cohorts were likewise armed. The blue steel of the Kalashnikov made Tucker temporarily forget about the evening chill. He was not armed, as the guards would definitely find any weapons on his person. But dealing with ProTec, he knew he would not need any—at least he hoped not.

The guards of ProTec International were known by the American Intel community to be some of the finest in Asia. With their armament ranging from former-Soviet issue weapons to high-tech German Heckler & Koch submachine guns, ProTec guards made North Korean army regulars look like Rent-a-cops. Everyone "in the know" was aware of several incidents where highly-trained South Korean spies and commandos attempted to sabotage or otherwise infiltrate installations manned by ProTec guards. Every last one of them went home as part of prisoner exchange programs, or more often than not in body bags. Brute forcing past ProTec was something that just was not done.

Tucker was not your average spy. All of his career was totally dedicated to infiltration and "base cracking". He was well aware of how their security systems and procedures worked and remained confident despite the pack of armed guards that lay ahead of him. He also knew the holes and limitations of those systems. ProTec was excellent at stopping unwanted traffic, at making sure that any visitors were authorized to set foot on the installation and at checking against things out of the ordinary. Anything past "the ordinary" was out of ProTec's power. The North Korean military, ever-reluctant to release full control to a private company, kept a state-of-the-art intrusion sensing system at every military base. Nicknamed "Red Dragon", it was as advanced as any Western

system of the same function. At several checkpoints located strategically around each base, there were cameras equipped with biometric analysis systems. These "BA" systems would match physical features of anyone's captured image and reference it with a staggeringly massive database housed on a Hyundai supercomputer. The database contained known and suspected spies as well as shape patterns that could detect even a small pistol under a winter coat.

There was an army-green two-and-a-half ton truck that was taking an unusually long time to be inspected. The "deuce-and-a half", as they were affectionately called by military personnel, held several troops. Most of them were missile technicians or engineers. There were few guards inside as once a person was admitted past the tight perimeter security, it was fairly easy to navigate throughout the bases. There was tighter security in the secured areas, but it was child's play compared to the gate. A spoofed badge with a red stripe was all one needed to move throughout the missile facility. The truck finally moved forward and the short, stocky guard armed with the AKMS waved Tucker forward. Tucker turned down the volume on the scratchy radio as the guard approached the cab of the truck. Unlike the military personnel on base, this ProTec guard had no name tape.

ProTec is the only damn name you need to know, huh? Tucker chuckled softly to himself. He rolled down the window and handed the guard his manifest, bill of lading and other paperwork.

"Bacuro guju, gae sakiya." *Cold out here, isn't it?* Tucker said in his best Hangeul, as he concentrated on his "disguise" of a weathered tech. The guard merely grunted and nodded in approval. His eyes never left the papers that he was scrutinizing. *These ProTec guys sure aren't much on small talk.* Tucker lazily yawned and made a big show of vigorously rubbing his hands together again.

"Drive forward to the black and yellow lines." The guard motioned Tucker forward to a holding area right in front of Gate 80.

Security at the gates was even stricter. Along with the BA cameras, Red Dragon had weight sensors that would measure the weight of a vehicle and match it against yet another database. Based on the factory weights of fueled vehicles and the expected cargo listed on the drivers manifest, Red Dragon could detect anomalies and variations on these figures. For example, the Mitsubishi Fuso FK that Tucker was driving was known by Red Dragon to weigh 8,233 pounds with a full tank of fuel. When Tucker stepped out of the cab to hand over the manifest, the BA system estimated him at slightly under two-hundred pounds. The manifest listed roughly three-hundred pounds of electrical parts. After all was said and done, Tucker's entire payload should have registered around 8,700 pounds. This was fine, except for the extra 3,000 pounds of explosives placed throughout the frame of the Fuso. Unfortunately, this info was not accessible to the ProTec personnel. The biometric information, camera feeds and Red Dragon data was fed directly to computers at the Ministry of State Security to be analyzed later. The data was great for showing intrusion attempts after the fact, but because the ProTec guards had no access to the data, it meant nothing at the time. Rarely, the MSS would watch the data real-time at the bases. A few times, they managed to detect intruders or anomalies and radio the ProTec guards to act on their findings. But those were done only when policy

required mandatory monitoring or when there was a State official present for a "dog and pony show". The North Korean government wanted that data separate and confidential from ProTec. Tucker thanked the Koreans for their paranoia.
Finding all of his paperwork to be in order, the ProTec guard handed Tucker a red-striped badge, affixed a magnetic decal to the front of the Fuso emblazoned with the same red stripe and waved him through. Every cell in Tucker's body breathed a collective sigh of relief as he shifted the aged gearbox and rumbled through the gates towards the missile storage building. Another agent had previously mapped an escape route in the form of an electrical conduit that terminated outside of the facilities walls. In a matter of days, the man known as Tucker would be back in Virginia giving his briefing on what the American intelligence community already knew about the North Korean base defenses. The Ministry of State Security would be alerted to the fact that the agent known as "Tucker" had infiltrated their base once the Red Dragon data was analyzed by their Internal Security officers. But not before three-thousand pounds of Cordite explosives ripped through the storage facility like a small child tearing open the wrapping on a Christmas present.

The above scenario is, of course, fictional. There is no Tucker or ProTec International. Any modern-day security professionals who read this will more than likely shake their collective heads in dismay (*or disgust*) at the poor security model and policies in this scenario. In an age where physical security is nearly a precise science, these policies and procedures would almost seem unbelievable to any company or organization's Security Officers. What should be more shocking and disturbing is that this type of model is used by thousands of companies and governments throughout the world. Though something like this would (hopefully) not be found in physical security, the Red Dragon scenario is the current status quo in a field of security that is as vital, if not more vital than the disciplines of physical security. This scenario frequently occurs in the world of Information Security.

As electrons and paper, buildings and servers, LANs and physical plants are considered to be worlds apart from one another, the thinking in ways of protecting them has also differed. Though there are many similarities between the two disciplines of security, the two have also taken wide and even diametric differences in their execution. If one adds business or bureaucratic aspects such as outsourcing, inter-departmental politics and costs, matters get complicated even further. What are the actual differences in thought between Physical Security and Information security? Of those differences, how many are prudent and necessary? In the zeal to be revolutionary and groundbreaking, many Information Security professionals and engineers have separated their technology and wisdom from the traditional arts of security. Is this progressive or is this trend weakening the overall security of our networks? A good amount of evidence points towards the latter.

In this paper, I will discuss flaws in the current conventional wisdom in Information Security. As the discipline of Physical Security is substantially older and therefore more "battle tested", I will use current models in Physical Security as a basis for comparison and contrast. The Department of the Army/Department of Defense

procedures outlined in US Army Field Manual FM 3-19.30 will be one such document that I will draw from to compare the two models. Lastly, I will attempt to propose a more updated model for Information Security that mirrors some of the more solid doctrines of Physical Security along with the "Best Practices" of current Information Security models.

A Closer Look at the Physical Model: Ft. Anywhere

"Physical security is defined as that part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard against espionage, sabotage, damage, and theft. As such, all military operations face new and complex physical-security challenges across the full spectrum of operations. Challenges relative to physical security include the control of populations, information dominance, multinational and interagency connectivity, antiterrorism, and the use of physical-security assets as a versatile force multiplier." --US Army FM 3.19-30

In order to effectively compare and contrast these two fields of security, it is important to start with a baseline. As I believe that physical security is quite a bit more "battle tested" than its newer counterpart, we will use a physical model as our base of comparison. When choosing a real-world example, several come to mind. Banks, corporate facilities where sensitive information is stored (e.g. Research and Development) and government facilities are the most suitable candidates for discussion. Military installations, however best suit this discussion due to the intrinsic importance of security and the military's high commitment of resources to provide this security. The Department of Defense (DoD) created an excellent document on physical security in the US Army Field Manual 3.19-30. Using the guidelines in this document as well as the author's personal knowledge of defense methods of military installations, we will analyze this using the fictional *Ft. Anywhere*.

"An ESS (Electronic Security System) is used to provide early warning of an intruder. This system consists of hardware and software elements operated by trained security personnel." --FM 3.19-30 (6.3)

A potential intruder trying to infiltrate Ft. Anywhere would be detected well before even reaching the main perimeter. In any form of security, early warning is key to gain the advantage on an intruder. Intrusion Detection Systems or IDS are vital to the defense of Ft. Anywhere. Having identified the threat vectors, these points of entry are guarded by several systems. These are systems monitored 24-7 by trained staff that can interpret and react to threats. The perimeter is dotted with Closed Circuit TV (CCTV) cameras that are monitored by security personnel. Should one manage to evade detection from the cameras, a number of sensors are placed to detect any attempted compromise of the perimeter. In this case, our perimeter is a fence. These include seismic sensors that can detect movements in the ground nearest to the perimeter. Electromagnetic field sensors

and motion detectors are also employed. Generally, at least two are used to provide redundancy as well as a more comprehensive picture about the attack. The use of multiple IDS components in perimeter defense is designed to have a synergistic effect. When a sensor is tripped, for example, the security personnel can zero in to the location with CCTV cameras and obtain a clear "snapshot" of the details of the attack. All perimeter IDS components are designed to complement and validate each other. For example, a common tactic of physical penetration testers is to take advantage of the surroundings to defeat IDS. For facilities in rural areas, there may be wildlife living nearby. A common tactic is to release several good-sized indigenous animals near the perimeter to trip the sensors. Another is to take advantage of a windy day for the same effect. If there were only seismic or motion sensors, the stream of false positives may lull the personnel into a false sense of security (as frequent false positives lead to the system being ignored altogether). However, with the CCTV system in place, the security personnel can zoom in on the problem, and determine the nature of the alerts and immediately dispatch personnel to attend to any threats. Lastly, there are sentries that make their "rounds" throughout the perimeter. This can be thought of as an active IDS, as they have the capability to detect and instantly respond to any attack in real-time.

"Protective barriers are used to define the physical limits of an installation, activity, or area. Barriers restrict, channel, or impede access and are fully integrated to form a continuous obstacle around the installation. They are designed to deter the worst-case threat. The barriers should be focused on providing assets with an acceptable level of protection against a threat." --FM 3.19.30 (4.0)

Probably the most essential piece of the security puzzle at Ft. Anywhere is the perimeter defense. A strong, fortified perimeter serves not only as effective defense, but as a deterrent if it is intimidating enough. The sight of a 12 foot-high chain link fence with Triple-Standard Concertina razor spiral across its top is enough to deter the most dedicated attackers. But more important is its ability to physically stop any would-be intruders. An interesting note in Ft. Anywhere is the stockade. Built to contain criminals, it has its own perimeter defense to keep the inmates inside the perimeter. As the methods of security in prisons have taught us, perimeter defense is the same when dealing with intruders. The only difference is that the perimeter is switched, where the stockade represents the "outside world" and everything outside of it represents the protected resources or the "inside". The motor pool has similar measures to prevent theft of vehicles. Though a facility may have a main perimeter, it may also have several internal perimeters. Some of these may be "inverted perimeters" such as the examples of Ft. Anywhere's stockade and motor pool. Of course, the perimeter(s) are monitored and patrolled for intrusion or suspicious activity by the measures above. As previously stated, armed security personnel serve a hybrid role. In this case, they are a part of the perimeter defense as they can repel threats once they have been detected.

"Perimeter barriers, intrusion-detection devices, and protective lighting provide physical-security safeguards; however, they alone are not enough. An access-control system must be established and maintained to preclude unauthorized entry. Effective access-control procedures prevent the introduction of harmful devices, materiel, and

components. They minimize the misappropriation, pilferage, or compromise of materiel or recorded information by controlling packages, materiel, and property movement." – FM 3.19.30 (7.0)

Attackers come in all shapes and sizes and skill levels, ranging from the "village idiot" all the way up to the professional penetration tester (or worse). Very few, however, are foolhardy enough to attempt a "brute-force" penetration of Ft. Anywhere. The preferred method is to gain entry through legitimate means such as the gates. As a good amount of traffic passes through Ft. Anywhere's gates, there is a decent amount of risk involved. Most malicious traffic will be posing as normal, legitimate and expected traffic. This is especially true for espionage or sabotage attempts. As the primary points of entry are the main gates, these are highly controlled areas. First, any traffic passing through is controlled by a series of choke points. These are generally barrier-based with guard posts supplementing them. A visitor to Ft. Anywhere first has to stop at a heavy steel gate secured by a manned guardhouse. Vehicles are then thoroughly and systematically searched manually and with electronic devices to detect explosives or other suspicious items. The serial numbers on the trucks' seals are double checked with the loading manifests. This is similar to a checksum function in the network world. This is to ensure that the contents have not been tampered with in transit. All persons are required to pass through metal detectors and searches in order to gain admittance. Other threat vectors such as mail, standoff weapons and airborne attacks are taken into account in Ft. Anywhere's security. The security model is designed so that ANY possible avenue for attack is evaluated and then analyzed for potential risk. Those risks are then mitigated, eliminated or accepted.

The security at Ft. Anywhere does not end once someone passes through the gates. All visitors (and even employees) are checked against an access-control roster to ensure that only the appropriate personnel are admitted to certain areas (or even allowed inside). These rosters are dynamic in nature and are kept current, verified and accounted for by the base commander or a representative. They also validate and authenticate this roster. Anyone not appearing on the access-control roster can only access a restricted area with permission of the commander. Even then, the persons involved will more than likely not be permitted entrance without an escort. Identification tags are given that clearly identify which areas personnel have access to. And throughout the interior of the base, there are several access-control points to validate that a person is in the correct area. The theory of "once you're in, you're in" definitely does not apply. Access to restricted areas is constantly validated and authenticated throughout the base. Other measures like biometric security, tokens and standard challenge-authorization are maintained at these points, as well as random points by security personnel. This prevents trust relationships from being exploited. In addition, all of these control points are linked to other points for redundancy and containment. In the event of a compromise, areas can be sealed off or isolated to prevent the compromise from spreading to other parts of the base. Redundant monitoring stations ensure that if a checkpoint is stealthily compromised, the other stations can detect and react to any threats.

The security process of Ft. Anywhere is designed to be as streamlined as possible. Many government or military personnel will joke that this is in direct conflict with government and military policies that call for as much red tape to be deployed to a problem as possible. However, when dealing with potential threats, speed and efficiency is of the essence. There is a strict and well-defined security policy from the top down. Security personnel are given strict and clear orders on how to deal with situations. Where a high ranking officer such as a General may be able to override a number of protocols in his area of influence, when it comes to security, he is nothing more than a potential threat if policies are not followed. The personnel have clear authority to enforce the policy which validates its effectiveness. In the creation of the policy, all components of Ft. Anywhere's security are meant to work cooperatively with each other and are managed by the same group. This increases the efficiency of the security system as a whole and prevents bottlenecks, mix-ups and misunderstandings because a component or department was kept "out of the loop". Though there are some policies that are base or even area/system specific, the general security policy is used by every other friendly military installation on the planet. One component is not any more (or any less) vital than the others, and the security plan is addressed as a whole and not by the sum of its parts.

"Inspections and surveys are valuable tools to a commander's physical-security program. These tools collectively measure and identify the readiness of a commander's physical-security program. The survey provides the installation commander with an overall security posture of the installation." --FM 3-19.30 (11.0)

Lastly, the security at Ft. Anywhere is tested regularly (of course at random days with no notice) and vigorously. This not only allows officials to gauge the readiness of the security personnel and countermeasures, but also to gauge if the training, security measures and security plan are effective and up to date. As technology increases, new methods are used to defeat defenses. Security personnel must not only employ countermeasures to defeat these tactics, but also train their personnel on how to utilize these countermeasures to recognize and defeat these new threats. The willingness of the security staff to enforce the policies is also measured during penetration tests. As we all know, the best security policy is not worth the paper it is printed on if there is not strict and consistent enforcement. The penetration testing is conducted by highly skilled teams who intimately know Ft. Anywhere's security measures and are trained to defeat them. The knowledge an attacker has regarding the defenses of a target must never be underestimated. This is why it is important to employ highly-skilled and knowledgeable penetration testers.

Comparing the Layered Information Security Model: AB&C Corporation

Having discussed the physical security measures of Ft. Anywhere, we now turn to its counterpart in the private sector, AB&C corporation. AB&C is a major software company with satellite offices across the globe. AB&C specializes in software that controls traditional coal and nuclear power plants as well as water treatment facilities. Because of this, AB&C has a high number of government contracts and stores several terabytes of sensitive information within its network. One does not have to greatly tax their imagination to realize what damage could be done if this network was somehow compromised. AB&C's corporate headquarters is located in a high-rise in a major metropolitan city. This is also where the majority of AB&C corporation's servers, databases and R&D team are kept. Therefore, the corporate headquarters is where we will focus when discussing AB&C's information security. AB&C's network is protected like most others networks of large companies. AB&C uses the Layered Model of information security for a base for their security design. As single measures or methods of protection can generally be defeated by the attack du jour, a layered security scheme provides the "defense in depth" needed to protect AB&C's network from harm. In our comparison and contrast of these models, we will use the same categories in the analysis of Ft. Anywhere against AB&C's Layered Security Model.

Intrusion Detection

As stated in the history of Information Security, Intrusion Detection Systems (IDS) were not initially given the importance that they are today. In the earlier days, there were very few, if any commercial companies that made affordable IDS solutions for the private sector. Nowadays, this has changed. Products like NFR Security's *Network Flight Recorder* and Enterasys' *Dragon IDS* have gained extreme popularity and are now a part of any solid Information Security planning and implementation. AB&C uses NFR for their IDS solution. In order to maximize the efficiency of the IDS, AB&C uses a mixture of Host-based and Network-based IDS. The data received is collected by two Central Management Servers. One is located on-site at AB&C's headquarters and the other is at a satellite office in accordance with the Disaster Recovery plan. While this sounds like a solid plan, let us look back at the model of Ft. Anywhere. Their IDS components function the same way—to detect unauthorized traffic or malicious activity. But what separates the two is the fact that Ft. Anywhere's IDSs are combined with an immediate response capability to handle threats or attacks. AB&C's on the other hand are primarily for information gathering purposes. There are certain attack signatures that are set up to page a Systems Administrator or a member of the Information Security staff. Attacks such as the recently discovered SNMP1 vulnerability are considered a high priority and the IDS systems are configured to notify upon detection.

As we in the security profession know, however, by the time it takes a snoozing Admin to receive a page, arise from his sleep and "dial-in" to the IDS and/or suspect host, the damage has already been done. It is very much an "after the fact" process. Rarely, the security personnel get notified in time to watch a slow attack in process. They then are able to configure their firewalls or routers to block the attack(er). This is definitely the exception to the rule, as most attacks are found when analyzing the IDS logs some hours or days later. If the "Red Dragon" situation in the introduction narrative seemed far-

fetched, re-read it with AB&C's IDS process in mind. What is even more interesting is that most commercial IDS solutions (including the two named above) operate in the same manner. This is not to take away from the importance of an IDS solution. On the contrary, IDS is one of the most integral components of "Defense in Depth". It just needs improvement from its current state. This will be discussed in the next section.

Perimeter Defense

With the exception of a few web servers, and VPN servers that reside outside of the perimeter (albeit in a triple-tiered DMZ), AB&C's network is protected by an extremely robust perimeter defense consisting of a mixture of Checkpoint Firewalls, Cisco routers (functioning as both border routers as well as internal) and Nokia VPN/Firewall solutions. Of course, these firewalls are all stateful in nature. The border routers are equipped with the Multi-layer Switch Feature Card in order to provide routing to the VLAN's that AB&C uses as an extra measure of security. All in all, AB&C's perimeter defense rivals that of many ISPs in its robustness. The average attacker will have an extremely difficult time, to say the least.

There are, however a few problems with AB&C's perimeter defense. First, although there is content filtering integrated into the firewall, this is not enough to stop all of the hostile traffic that comes through. As is the case on the physical side as well, most hostile traffic with the highest threat potential will appear to be legitimate traffic. In a poorly configured IIS server, a simple GET request that would pass through any firewall, can lead to a system compromise. There is also the fact that certain traffic may not be immediately recognized such as Unicode-based attacks that made Code Red and Nimda so deadly. Rain Forest Puppy's Whisker stealth scanner is another example. Though most IDSes will detect the splicing attacks that Whisker employs, firewalls may not. Once compromised, these servers can exploit trust relationships that we will discuss later.

The second point is a rehash of the IDS problem. An IDS will detect most of the malicious traffic posing as legitimate traffic. The problem is that our routers and firewalls do not communicate with the IDS. What generally occurs is once an attack has been detected by the IDS or has been publicized through advisories, appropriate counter-measures are taken. This can be anything from adding firewall rules, to patching systems to updating content filtering methods. The same problem with speed exists. A lot of times, this is done "after the fact". The latency between the time of an actual attack and the time it takes to apply the appropriate countermeasures may be as short as a few hours or as long as a day or two. This is unacceptable because most attacks take a fraction of that time to execute. This could be minutes or even seconds.

Lastly, the Checkpoint FW-1 firewalls are housed on Sun computers running Solaris. Like any other operating system, Solaris has its share of vulnerabilities and bugs. The threats range from Denial of Service to outright system compromise. Unless a stringent regimen of updating and patching the system is followed, there is moderately high risk attached to this host. Again, this is no different than Windows 2000, Red Hat Linux or

any network operating system. The greatest danger lies in the fact that if this firewall were to be knocked down or compromised, it could leave the entire network vulnerable to attack.

Access-Control and Trust Relationships

One of the greatest features of modern perimeter defense is access-control. Not only can routers or firewalls be configured to allow certain hosts access to certain areas of the network (or not at all), the stateful component allows the ability to keep track of unsolicited connections and deal with them as the administrators see fit. If the US Postal Service could enable stateful filtering on our mailboxes, the world would be such a nicer place!

The greatest danger is one that has plagued Information Security professionals since the old days. That is the tactic of exploiting trust relationships. Mitnick used this tactic in his famous attack against Tsutomu Shimomura back in 1994. Mitnick took advantage of the Berkeley "r-utilities" such as rlogin and rshell. In a nutshell, this attack works because of the trust relationships between systems. Once a trusted host is compromised, it can cause damage to other systems. The biggest difference in the thinking of Physical Security and Information Security is compartmentalization. In our example of Ft. Anywhere (as well as the feudal Japanese castle example from the history section), the various sections are compartmentalized so that if one is compromised, it can be isolated from the rest of the network without weakening it as a whole. In Information Security, this is generally not the case. At a meeting of security professionals last year, the CIO of a major Southern telecommunications company was asked what he did when the Nimda worm struck. His answer? "We pulled the plug on everything". This is not an acceptable response for an attack. The fact that the amount of global network attacks is increasing further reinforces the need for redundant and compartmentalized design in networks.

Organization and Policies

AB&C excels over most companies in the fact that they have a security policy that is clearly communicated to all members of the company. Networks are designed with security in mind in all aspects of the life cycle. The downside to a strong security stance is cost. For CISOs and other Information Security practitioners, security is extremely important and is reflected in the budgets. Other executives may not see it with the same importance, especially when a measure of a good security process is transparency. When everything works well, Information Security is all but invisible. Because of this, it can be difficult to show those outside of the department the "fruits of labor". As a result, buy-in or large financial commitments may be hard to obtain. With shrinking budgets, security managers look to cut costs without sacrificing the integrity of the security infrastructure. One such way is outsourcing. There are several outsourcing companies that provide services such as MIDS (Managed Intrusion Detection Systems), managed firewalls or auditing. In order to keep costs of highly-skilled security professionals to a minimum,

AB&C out sources a portion of their security—the firewalls. AB&C employs a well-known and well-respected managed firewall company to handle the firewall needs.

This is not to take anything away from companies who provide this type of outsourcing. On the contrary, many of them do an excellent job at an affordable price. On the physical security side, outsourcing is extremely common and has basically become the norm. The main difference is that companies that outsource physical security generally are in charge of all components of physical security. From gate sentries to key cards to manned patrols, physical security companies for the most part have full control over the security picture. This streamlines decision processes and makes for more efficient protection of the client. In information security, on the other hand, generally certain components are outsourced. As all of the components of information security should be complementary to each other, this can provide bottlenecks in communication or interaction. This is especially true if the IDS and firewalls are handled by two separate entities. As there also may be proprietary matters. Obtaining information on events may experience delay, or in the worst case, extreme difficulty.

The Layered Security Model is an excellent groundwork for a security policy and design. No one can argue that several layers of defense mechanisms provide for the "Defense in Depth" that is needed to provide protection of networks. The problem is that having multiple layers is not enough. The interaction and design of these layers is generally ignored in the current conventional wisdom of Information Security. These factors, however, have been considered in Physical security since man's earliest history. The four main points that need to be addressed are:

- Integration and communication of components to provide a dynamic defense system.
- Minimizing response time to attacks to increase the overall efficiency of the security systems.
- Compartmentalization to mitigate the risks of compromise of one or more segments of the network.
- Centralized management without sacrificing compartmentalization.

In order to achieve these goals, we may need to rethink the Layered model, as it is incomplete. Again, no better framework can be found than the Layered model, however we must take it one step further to ensure the most efficient manner of protection for our networks.

The HAS2 Security Model

The security model that I propose to replace the Layered Security Model is called the Holistic Approach to Security, 2nd Generation, or HAS2. The original HAS model was

created by a company called LIRIC Associates to be compliant with ISO 17799. The original HAS model was an enhanced-layered model that incorporated several elements of security (including physical) along with LIRIC's proprietary technology. Each layer was designed to support the other. Unfortunately the technology did not fully provide the levels of integration and protection that I believe to be robust enough to meet the challenge of the future. The HAS2 model is based on the layered security model. However, where the Layered model focuses on multiple layers and components, the HAS2 model sees these components as necessary parts of the whole puzzle—hence the term holistic. These components must be considered not as individual layers, but as the sum of its parts. No one component is any more or less important than the others. The main differences are that HAS2 addresses the shortcomings of Information Security and supplements it with elements of the Physical Security models. These elements are applied to Information Security in a manner that strengthens the overall model.

Integration and communication of components to provide a dynamic defense system and minimizing response time to attacks to increase the overall efficiency of the security systems.

HAS2 accomplishes this by employing Next Generation Intrusion Prevention. In standard Intrusion Detection, malicious traffic is detected for analysis. However, in the event of an attack, this latency is entirely too slow. To address this problem, HAS2 calls for an Intrusion Prevention System. There are several companies and technologies that address this problem. Secureworks' iSensor is one such device that integrates an IDS with a dynamic firewall to provide an Intrusion Prevention System. When an attack or malicious traffic signature is detected, the firewall component automatically takes action to drop the offending packets or block the attacker altogether. This is done in real-time and is backed by a 24x7 security staff at a SOC. For those who wish to keep all security matters in-house, there are other new technologies that integrate an IDS solution with firewalls to provide immediate response. IDS data is still logged and can be analyzed at a later date for further research. In a HAS2 network, the line between IDS and firewalls is nearly transparent, as the two act together to provide a synergistic effect. This also allows heterogeneous components to be used in a network as long as they have a means of communicating with each other and can provide dynamic changes to perimeter defense. This greatly minimizes response times to attacks. When properly configured, Intrusion Prevention Systems provide a proactive solution to threats and attacks, where Information Security in the past has been mostly defensive and passive.

One piece of technology that would have to be added to any devices on a HAS2 network is a secure communications protocol between security devices such as the Layered Object Transport Protocol. As there are a few in production and several in development, I cannot recommend one with confidence at this time (as it is beyond the scope of this document). The only requirements are ease in porting to various operating systems and devices, that the protocol is stable, secure and that there is low-overhead to decrease network traffic.

Compartmentalization to mitigate the risks of compromise of one or more segments of the network.

In a network using the HAS2 model, networks are segmented a bit deeper than most conventional networks. This is mainly a consequence of design, as there are several ways to achieve this such as VLANs, secured intranets, etc. This is done by many security professionals with excellent results. The technology component of the compartmentalization relies on omitting technologies where trust relationships can easily be exploited and replacing them with more secure protocols. Remote Procedure Call (RPC) and the r-utilities as well as file sharing services like NFS or NIS may need to be seriously reevaluated for their use in a HAS2 environment as there are several trust issues that have great potential for exploit. In the event of a global attack such as Nimda or Code Red, network administrators must have the ability to quickly isolate an Exchange server or rouge web server from the rest of the network to contain damage. As human intervention may not be fast enough, this technology may be built into routers, switches and other network devices in the near future. This minimizes reaction time and ensures compartmentalization.

Centralized management without sacrificing compartmentalization.

This may seem like a direct contradiction of the previous point. It seems that in security, compartmentalization can be weakened by any sort of centralized management (and vice-versa). However, the HAS2 model can achieve this without sacrificing the strength of the network. The majority of centralized management is based on organization and not so much technology. In our example of AB&C, central management is weakened by outsourcing individual components of their information security system. This can be made to be HAS2 compliant by a number of means:

- Outsourcing the entire information security infrastructure by use of a managed security company. At first thought, this may seem scary to some seasoned network managers, but when one considers that this is the norm in the physical security world, it does not sound as threatening.

- Keeping the information security infrastructure in-house. This is simply the inverse of the above solution. This may not be cost-effective for smaller companies, however, larger companies may find this to be an appropriate solution.

- Using out-sourced companies that use HAS2 methods, including the aforementioned security appliance communications protocol. If the managed firewall company that AB&C employs uses this protocol, then integration with other devices is not reduced. Either company (or both, preferably) could monitor and manage traffic and work together to make changes. Great care must be taken

not to "step on each other's toes", however with strong policies in place this can be achieved.

Should the IDS/Firewall combination be compromised or forced offline, redundant firewalls and routers should fall over to a Draconian policy to protect the network until the problem can be addressed. These backup perimeter defenses should have no communication with the main IDS/Firewall combination except to monitor it for health and wellness. When an outage or potential compromise is detected, it should immediately cut over and activate.

Conclusion

In conclusion, the disciplines of Physical Security and Information Security have made great strides to reach the development of the present day. As Information Security (as it applies to computer networks) is a newer discipline, it still has some growing pains and kinks to work out. Because of the separation in many companies between Information Security and Physical Security, we have forgotten some basics of every form of security. By recognizing that its physical counterpart offers tried and tested methods and tactics, I believe that we Information Security practitioners can apply these methods to strengthen our networks and countermeasures against malicious attackers. Even though the two fields are inherently different, the goals and many of the means to achieve them are the same. By taking the best from each discipline and applying them to our own needs, I believe that we can provide robust security to meet the challenges of the future.

References:

1. U.S. Department of the Army, Physical Security, Field Manual #3-19.30, 8 January 2001
URL: http://www.adtdl.army.mil/cgi-bin/atdl.dll/fm/3-19.30/toc.htm

2. LIRIC Associates, LIRIC's Holistic Approach to Security,
URL: http://www.liric.co.uk/cgi-bin/frame.cgi?c=http://www.liric.co.uk/has.html

3. National Computer Security Center (NCSC), Guide to Understanding Trusted Facility Management
(Brown Book), June 1989
URL: http://members.fortunecity.com/botkiller/brown-book.txt

4. Prud'hommeaux, Eric, LOTP Security Model, Version 1.5, WC3 Webpage
URL: http://www.giac.org/GIACTC_citations.php

5. Marshall Abrams and David Bailey, Abstraction and Refinement of Layered Security Policy. Information Security Online
URL: http://www.acsac.org/secshelf/book001/05.pdf

6. Brockway, Bockie, "Layered Security: An ISP Case Study with Cisco and Solaris"
Sans.org Reading Room, 19 October 2000
URL: http://rr.sans.org/firewall/layered_sec.php

7. Faile, Jonathan; S. "Security Outsourcing"
Sans.org Reading Room, 25 August 2001
URL: http://rr.sans.org/managed/sec_out.php

8. Tuesday, Vince, Security Outsourcing: Don't Bet on it Yet. June 11, 2001.
URL: www.computerworld.com/cwi/story/0,1199,NAV47_STO61232,00.html

9. Kogut, Richard. "Razing the Firewall", Information Security Magazine, November 2000 pg. 74