Risk mitigation in mobile computing:
Managing risks associated with company owned and employee/vendor owned devices through the use of VPN technologies

Jason Smith

Fort Hays State University

Abstract

Many companies today have developed applications that use Internet technologies that offer the advantage of allowing employees access to databases and information contained within the corporate network. Many of these systems rely on only account names and passwords to protect the information (Loo, 2008, p. 69). In addition to weak access control measures, mobile computing threats also include malware, phishing and social engineering, direct attacks by hackers, data communications interception and spoofing, loss and theft of devices, malicious insider actions, and user policy violations (Friedman & Hoffman, 2008, p. 161). Using standards adopted by the National Institute of Standards and Technology, this paper attempts to perform a qualitative baseline risk assessment on both the corporate owned laptop and the employee/vendor owned laptop taking into consideration some assumptions made to the initial security of each device. Using a lab setting, the study demonstrates some of these weaknesses using vulnerability scans and traffic sniffing. As a means of mitigating these risks, the study focuses on the solution of Virtual Private Networks to encrypt and secure the data transmitted between the mobile computing device and the corporate network. Again, in a lab setting the study demonstrates the effectiveness and limitations of this solution. Once the solution has been deployed and verified, a subsequent risk assessment is performed to determine if the level of risk has been mitigated by the solution.

Introduction

Mobile computing provides employees with the freedom of accessing network resources from remote sites at time more convenient for them. From the corporate perspective, mobile

computing allows employees to stay in touch by phone, email, fax and web based methods when away from the office.

Allowing workers to telecommute or work from home is rapidly becoming a part of more family-friendly working options. Telecommuting employees can vary between working a few hours from home each week to working full time from home. Research has shown that smaller companies and companies with a large international workforce are more likely to embrace telecommuting for its employees (Mayo, Pastor, Gomez-Mejia & Cruz, 2009, p. 918).

Some studies have also found that the rise in mobile computing has also resulted in increased productivity. A study conducted by Cisco Systems in 2003 found a 13.4 percent average productivity gain due to the use of mobile computing (Deeson, 2005). The study found that certain industries benefited from strong productivity gains such as insurance adjustors and sales engineers in the healthcare and pharmaceutical field. It also found that hotel guests were more likely to select a hotel that offered broadband access and were willing to pay almost 7 percent more for this service.

A more recent survey in 2011, more than 80 percent of respondents stated their productivity either increased or greatly increased through the use of their Smartphone (Kalkbrenner & McCampbell, 2011, p. 4).

Mobile computing, however, also offers a slew of new concerns for businesses including the security of such devices. Because these devices operate outside the confines of the internal corporate network, they do not benefit from the same security measures that protect internal resources. Moreover, because the very nature of mobile computing requires that internal resources be accessed over the public Internet, the confidentiality, integrity and availability of this data must be addressed.

This study takes a comprehensive look at the risks associated with mobile computing, looking at real world examples and using a lab setting to determine how such risks may be exploited. Mobile computing, for the purposes of this study, is defined as any device that is used to access internal resources from a remote location. This includes laptops and Smartphones.

This study also looks at two separate types of mobile computing; that which is performed on devices owned and controlled by the corporation and those which are not (i.e. owned by employees or vendors). In considering these two scenarios, the study makes certain assumptions as to the base security level of each device and as such will present separate risk assessments on each scenario based on these assumptions.

A case study will be conducted to assess the effectiveness of commercially available security solutions designed to protect mobile computing for both scenarios. The study focuses mainly on the use of laptops as the means of mobile access but does also offer some additional information on the protection of mobile computing via a Smartphone, in particular an iPhone.

Baseline Risk and Vulnerability Assessment

When it comes to mobile computing there are many risks that security professionals should be concerned about ranging from theft of mobile devices to sniffing of communications to inappropriate use of corporate resources. All of these raise significant questions to the security of mobile computing and how best to mitigate the risks.

The National Institute of Standards and Technology (NIST) defines risk as a measure of the extent to which an entity is threatened by a potential circumstance or event. It is determined by a combination of the level of impact to the entity if such an event were to occur and the likelihood of such an occurrence. (NIST, 2011)

The first step in establishing a baseline risk analysis and vulnerability assessment is to identify the security threats for mobile computing. Using the threat events defined by the NIST's "Guide for Conducting Risk Assessments" (2011) the following should be considered possible threat events for mobile computing:

1. Access sensitive information through network sniffing.
2. Compromise information systems or devices used externally and re-introduce into the enterprise.
3. Exploit known vulnerabilities in mobile systems.
4. Externally placed adversary sniffing and intercepting of wireless network traffic.
5. Hijacking information system sessions of data traffic between the organization and external entities.
6. Intercept/decrypt weak or unencrypted communication traffic and protocols.
7. Mishandling of critical and/or sensitive information by authorized users.
8. Opportunistically stealing or scavenging information systems/components.

To simplify matters, the above listed threat events were grouped by similarity into the following subcategories, Communication Security, Device Security, Loss/Theft. Threat events 1, 4, 5 and 6 were placed in communication security. Threat events 2 and 3 were placed into device security and threat event 8 was placed into loss/theft. Threat event 7 can fit into all three categories depending on the type of mishandling of the information.

Methodology

The next step is to perform the risk analysis and vulnerability assessment. In a survey conducted by the FBI and the Computer Security Institute (CSI), 80 percent of companies that participated reported financial losses due to security breaches but only 44 percent could quantify

their actual losses. Without a proper risk analysis it's difficult to justify spending more to improve security. There are two basic types of risk analysis methods to consider – quantitative risk analysis and qualitative risk analysis. Quantitative risk analysis attempts to assign independently objective monetary values to the components of the risk assessment and to the assessment of the potential loss. Qualitative risk analysis on the other hand is more scenario-based. (Tan, 2002)

For the purposes of this study a qualitative approach was used. The choice of a qualitative approach is not simply due to its simplicity but the scope of the study limits the method to that of a more scenario-based assessment.

The risk assessment will use the qualitative values defined by NIST (2011) of very low, low, moderate, high and very high. Using their template, I will gauge each threat event in the following areas:

- Likelihood of attack initiation – determines the likelihood that the threat event is initiated.
- Vulnerabilities – identify the vulnerabilities that could be exploited and the pre-disposing conditions that could increase the likelihood of adverse impacts.
- Likelihood initiated attack succeeds – determines the likelihood that an initiated event will result in adverse impacts.
- Overall likelihood - determines the likelihood that the threat event will be initiated and result in adverse impact. It is derived from a combination of the likelihood of initiation and likelihood of success.
- Level of Impact – determines the level of impact for the corporation from the threat event.

- Risk – the overall level of risk, determined by a combination of impact and overall likelihood.

Level of impact is specific to the organization conducting the risk assessment. It takes into consideration the potential harm to organizational operations, organizational assets, individuals, other organizations and the nation. For the purpose of this study, it is assumed that the level of impact of the threat event, were it to be successful, to be at a minimum high impact. This means the event could be expected to have severe or catastrophic adverse effects on the organization. (NIST, 2011)

Risk and Vulnerability Assessment

To help determine the risk assessment of each individual mobile computing device, I used a combination of real world examples combined with data derived from a lab setting. The lab was comprised of a central firewall protecting internal resources. A single server running Windows Server 2008 and operating as an Active Directory server for user authentication, an Exchange server for email delivery and an FTP server for remote file access represented the internal resources.

The external network was comprised of two Windows XP laptops, one representing the corporate owned laptop, and the other representing the employee/vendor owned laptop. It also includes a single Smartphone in the form of an iPhone. The attacker system was also installed running Windows XP.

The first threat event category to be assessed was the device security. For this category, some base assumptions were made to their overall baseline security implementation of the two systems. For the corporate owned device, the assumption was made that a corporate policy was

in place requiring the use of strong passwords for all computer systems; the use of firewall, anti-virus and anti-malware software; and all the latest security patches deployed. For the employee/vendor owned laptop, the assumption was made that no security implementations have been configured.

Based on these two assumptions, the corporate owned laptop was installed with the latest security patches from Microsoft and the Windows firewall was activated on this system. For vulnerability assessments concerning other device security features such as protection from malware, the assessment was performed under the assumption that software was installed on the system to prevent such attacks. The employee owned laptop on the other hand included no security patches and had the Windows firewall disabled.

To get a baseline vulnerability assessment, each system was scanned with penetration testing software to discover any holes in their defenses. Using both Metasploit and Nessus penetration testing utilities I scanned both machines and found that the corporate owned system revealed no open ports for which a hacker could gain access.

The employee owned laptop on the other hand revealed that ports 135, 139 and 445 were listening on the system. Port 135 is part of Microsoft's DCE-RPC protocol suite and has had several known vulnerabilities associated with it. Ports 139 and 445 are for file and print sharing services. The W32.Blaster.Worm is an easily spread worm that exploits a buffer overrun vulnerability that can be exploited via ports 135, 139 and 445. ("Port 135 details")

The findings generated from this scan agree with similar findings from a survey conducted by Tim Chenoweth, Robert Minch and Sharon Tabor (2010) in which they examined the security behaviors of wireless users of a university wireless access system. For their study, the researchers performed continuous network scans for a 41-day period, collecting information

from 3,331 unique systems. Of the 3,331 devices, more than 8 percent had a detectable open port with 65 percent of the open ports presenting a serious security vulnerability. In fact, the top three ports that were most often open were ports 135, 139, and 445.

With this information we can perform the risk assessment for device security by assigning a risk value to each of the risk assessment categories mentioned earlier.

For likelihood of initiation, we can assume it very highly likely that at some point these devices will be scanned for vulnerabilities by attackers. Therefore, for both the company owned laptop and the employee owned laptop I placed very high in this column.

For vulnerabilities, the company owned laptop has the benefit of a corporate security policy that includes the required use of a firewall, strong passwords, mandatory patch updates and anti-malware software. The lab test has shown that these measures are successful in lowering the vulnerability of the unit so the vulnerability score for the corporate owned laptop was rated low meaning relevant security control or other remediation is fully implemented and somewhat effective.

The employee owned laptop on the other hand has no firewall, no anti-malware software and has not received a single security patch update therefore its vulnerability rating would be very high.

Likelihood of success is dependent on the adverse impact the event would have if it were successful. It is determined by considering the likelihood of initiation and the security measures put in place to prevent the threat event. Based on the security measures already put into place and the results of the vulnerability scan, the corporate owned laptop was rated low. The employee owned laptop on the other hand could be considered to have a high adverse impact.

Overall likelihood is derived from a combination of likelihood of initiation and likelihood of success using the table below:

Likelihood of initiation	**Likelihood of success**				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	High	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

(Source: NIST, 2011)

Similarly risk is derived from overall likelihood and level of impact. Since level of impact will be a static high rating, the risk will be determined using the table below:

Overall Likelihood	**Level of Impact**
	High
Very High	Very High
High	High
Moderate	Moderate
Low	Low
Very Low	Low

With this information the risk assessment chart can be filled in with the relevant information as seen in the two tables below:

Corporate Owned Laptop

Threat Category	**Likelihood of Initiation**	**Vulnerabilities**	**Likelihood of Success**	**Overall Likelihood**	**Level of Impact**	**Risk**
Device Security	Very High	Low	Low	Low	High	Low

Employee/Vendor Owned Laptop

Threat Category	**Likelihood of Initiation**	**Vulnerabilities**	**Likelihood of Success**	**Overall Likelihood**	**Level of Impact**	**Risk**
Device Security	Very High	Very High	High	Very High	High	Very High

These tables clearly illustrate the vast difference in the device security of a corporate owned laptop versus an employee/vendor owned laptop. Information security professionals should be highly concerned about allowing these devices access to internal resources.

Communication security is another area of concern as both the corporate owned and employee/vendor owned devices must use the same, insecure Internet to reach the internal resources.

In the lab, the attacker system was setup to sniff all packets coming and going over the wireless network using the program Wireshark. I then initiated an FTP and email connection to the internal server. With FTP I was not only able to capture the username and password that was transmitted, I was also able to capture the data transfers and recreate file being transferred.

With email, the same was true. Not only was I able to easily sniff information on the sender and recipient, I was able to read the entire contents of the email message and recreate the attached document file.

This test shows how easily it is to eavesdrop on Internet communications from a common LAN. However, sniffing is not the only concern for security professionals as remote access users are also vulnerable to session high jacking. Additionally, users are known to browse to insecure websites and offer up personal or confidential data without concern. In my test, I was able to also easily capture HTTP traffic from the client machine and read the contents entered into a simple web form.

Many applications also require Internet access to transmit and receive data. Each application comes with its own set of vulnerabilities and security concerns. One of the biggest security concerns involving applications are peer-to-peer file sharing applications that allow the sharing of files such as music, movies, and information.

In fact, Pfizer experienced a breach when an employee's spouse installed file sharing software on the employee's Pfizer issued laptop. This exposed the information on about 17,000 current and former employees to unauthorized parties (Culnan, et al., 2008, p. 50).

Peer-to-peer (P2P) clients allow users to share data in particular folders or directories. This allows for the possibility to accidentally share confidential information, downloading malware from the P2P network that exposes the system to further risks, or the P2P client software has bugs that result in un-intentional exposure to sensitive information (Johnson, 2008).

According to the FTC (2010), more than 100 U.S. companies and agencies are regularly exposing sensitive information via P2P networks. According to their report, information they found that had been leaked included health-related information, financial records, and drivers' license and Social Security numbers.

Based on the lab results and the above information, the risk assessment for both types of systems have been give then following risk rating.

Threat Category	Likelihood of Initiation	Vulnerabilities	Likelihood of Success	Overall Likelihood	Level of Impact	Risk
Communication Security	Very High	Very High	High	Very High	High	Very High

The final category examined, loss or theft, is another serious concern for security professionals. Mobile computing devices have built in storage media, capable of holding gigabits of data, some of which could be confidential in nature. If devices are lost or stolen, the company can assume the data on that device to be lost as well.

In a survey of 36 large and 70 medium sized U.S. airports, the Ponemon Institute (Ponemon, 2008) found that travelers lost more than 12,000 laptops per week. It found that 53

percent of the business travelers surveyed admitted their laptop contains confidential or sensitive information while 65 percent of them stated they do nothing to protect or secure that data. Surprisingly still, the survey found that while more than half of the travelers worry about losing their laptop, they often ask a fellow passenger to watch it for them while they runoff to do something. (Ponemon, 2008)

When it comes to performing the risk analysis on both the corporate owned and employee/vendor owned devices, some assumptions were again made concerning the base security policy of the devices. With the corporate owned device, the assumption was made that the corporate security policy required the use of strong passwords and full disk encryption to protect the data stored on the laptops. For the employee/vendor owned laptop, nothing is assumed concerning the security of the device except that no security exists.

Taking these assumptions into consideration combined with the data provided from existing research on this issue, the following risk assessments were calculated according to the same scales used previously.

Corporate Owned Laptop

Threat Category	Likelihood of Initiation	Vulnerabilities	Likelihood of Success	Overall Likelihood	Level of Impact	Risk
Theft/loss	Very High	Moderate	Low	Moderate	High	Moderate

Employee/Vendor Owned Laptop

Threat Category	Likelihood of Initiation	Vulnerabilities	Likelihood of Success	Overall Likelihood	Level of Impact	Risk
Theft/loss	Very High	Very High	High	Very High	High	Very High

Based on the complete risk assessment, we can see that the employee/vendor owned systems represent a very high security risk in all three categories while the corporate owned ranged from low to moderate to high in the three categories. This shows us that without proper mitigation, mobile computing presents a significant weakness in the corporate security policy.

VPN Based Risk Mitigation for Mobile Computing

This paper looks at the use of virtual private networks (VPN) as a solution for mitigating the above-mentioned risks associated with mobile computing. Using commercially available tools from Check Point Software Technologies, this study implements a solution whereby VPN technology is deployed from a centralized corporate firewall to attempt to reduce the risks associated with both the corporate owned laptop and the employee/vendor owned laptop. While the tools developed by Check Point were the ones chosen for this study, it should be noted that similar results should be expected from other vendors with similar products.

VPN is a network that uses a public network such as the Internet as its communication medium to connect two or more devices or private networks. It operates by passing data through encrypted virtual connections often referred to as VPN tunnels (Riaz Ahamed & Rajamohan, 2011).

Most VPN connections use the Internet Protocol Security (IPSec) protocol suite which includes Encapsulating Security Payloads (ESP) to provide confidentiality, data origin authentication, connectionless integrity, an anti-replay service, and limited traffic-flow confidentiality. In tunnel mode, ESP encapsulates the original IP packet in its entirety with a new packet header added. This affords the protection to the whole inner IP packet (“IPSec Basics”).

IPSec VPN for mobile computing requires that a client be installed on each of the devices to facilitate the negotiation of the tunnel parameters and the encryption of the data. This is fine for corporate owned mobile computing devices however for employee/vendor owned systems, it may prove difficult to deploy the clients. As such a second, semi-clientless option is available in the form of Secure Sockets Layer (SSL) VPN. SSL VPN uses the built-in SSL functionality of most Web browsers to establish the secure connection. While the connection is mostly clientless, most non-browser based applications will require the installation of a plug-in to interface between the application and the SSL VPN connection (Friedman & Hoffman, 2008, p. 173).

The benefits of both options are very similar. Both IPSec and SSL based VPN deployments can use the existing firewall policy to restrict access to internal resources. However, VPN only protects encrypted data to and from the client and the firewall. All other traffic sent from the client is still sent un-encrypted and in the clear. Fortunately, both options allow that all traffic be sent over the tunnel so even the user's casual browsing is encrypted. Furthermore, this allows security administrators to monitor the traffic from the remote user and use the existing firewall policy along with application control and URL filtering to further restrict access to malicious or in-appropriate sites and applications. This access can be tailored to the individual users, giving some more access than others through the same central deployment (Oien, 2008).

VPN alone however does not mitigate all the risks associated with mobile computing, particularly those associated with the employee/vendor owned laptop in regards to device security and theft/loss. Whereas the corporate owned laptop benefits from a corporate security policy that mandates the use of firewall and anti-virus software coupled with full disk encryption and strong passwords, the employee/vendor owned system does not. Therefore additional measures need to be taken to ensure the security of those devices.

This can be achieved through the use of two additional solutions combined with VPN. These are security compliance scanning and desktop virtualization. Compliance scanning allows the company to scan the user's machine and verify that it meets corporate security standards before allowing the user to connect to the network via VPN. Failure to meet one or more of the requirements should result in the user being denied the ability to connect to the VPN.

Additionally, the corporation must protect data from being misused or falling into the wrong hands. When that data is stored on mobile devices that do not benefit from the security policies of the corporate environment, it becomes exponentially more vulnerable to attack or theft. To prevent this, desktop virtualization can be deployed. With desktop virtualization, all information and data generated during the VPN session is stored in local memory only. Once disconnected, all traces of the session are removed from memory, making the data virtually impossible to retrieve.

Testing of the Solution and Re-Assessing Risk

To test the solutions mentioned above, I modified my lab and implemented both an IPSec VPN solution for the corporate owned laptop and an SSL VPN solution for the employee/vendor owned laptop.

The firewall protecting the internal network is an open platform server running Check Point's R75.40VS firewall software. This firewall is managed by a separate management server also running R75.40VS from inside the network.

Beginning with the corporate owned laptop, I installed the Endpoint Security VPN client. The Endpoint Security VPN not only acts as a VPN client but also provides for local desktop firewall support as well. This allows the security administrator the ability to not only ensure that

all corporate owned laptops have a firewall installed on them, but also to be able to tailor the firewall policy to the individual users or groups of users. For this lab I created a simple desktop policy that blocked all traffic inbound to the client and allowed all outbound traffic from the client when connected to the firewall. When disconnected, all traffic inbound and outbound was blocked. This forces the users to connect to the VPN to be able to be able to communicate in any way over the Internet.

I also enabled the application control and URL filtering blades on the firewall to perform deeper packet inspection up-to layer-7. I also set the clients to route all traffic through the firewall so that all of their Internet connections would be sent to the firewall for inspection.

With the solution fully implemented, I connected to the site and began the vulnerability scans and network sniffing again to gauge the effectiveness of the solution in mitigating the risks mentioned earlier. Because this solution provides no additional protections against theft/loss of the laptop, there is no need to perform an additional risk assessment on that category for the corporate owned laptop.

For the vulnerability assessment, the scans performed by Metasploit and Nessus yielded the same results as earlier indicating the deployed firewall was at least just as effective as the built-in firewall on the client at thwarting network scans. For this risk assessment, the results were the same as the baseline assessment with overall risk still have a low rating.

For the sniffing test, I again opened a connection via FTP to the internal network and sent email across as well. This time however, the connections benefited from the protection of the secure VPN connection and the hacker system no longer received any confidential information during his network sniffing. In fact the only thing he saw from the corporate system was a bunch of ESP packets that at most, revealed the public facing IP address of the corporate firewall.

This shows that the VPN connection completely renders the ability of the hacker to sniff the sessions or even hijack the session impossible. And, because all traffic must be routed through the firewall, the security administrator is able to monitor and regulate other traffic from the client system destined for networks outside of the scope of the corporation. With the application control and URL filtering blades enabled, the administrator now has the ability to centrally restrict access to malicious sites initiated by the user or by applications installed on the system. This includes the ability to access or use P2P sharing software and sites.

To test this ability I installed the popular bit-torrent client uTorrent on the corporate system and attempted to use it to share files. I also attempted to browse various P2P websites and sexually inappropriate websites – all of which were blocked by the application control and URL filtering policy installed on the corporate firewall.

These tests indicate that the VPN deployment was highly effective in not only protecting against malicious individuals looking to capture confidential information as it moves over the local network segment but also in preventing inadvertent dissemination of sensitive information by the users. Thus, we can recalculate the risk factor for corporate owned laptops for the category of communications according to the table below:

Corporate Owned Laptop

Threat Category	Likelihood of Initiation	Vulnerabilities	Likelihood of Success	Overall Likelihood	Level of Impact	Risk
Communication Security	Very High	Very Low	Low	Very Low	High	Low

The vulnerability rating was lowered from very high to very low as the relevant security controls have been fully implemented, assessed and deemed effective. As such, likelihood of

success was also lowered from high to low. This resulted in the lowering of both overall likelihood and the overall risk factors from very high to very low and low respectively.

For the employee/vendor owned laptop, the corporation may not be able to install an IPSec VPN client on the user's system; therefore, it must rely on SSL VPN to secure the communication. To enable this on the same gateway running IPSec VPN, I deployed the Mobile Access blade, which allows the security administrator to create an SSL VPN policy for regulating remote access for these users. When deployed the users open an HTTPS web connection directly to the corporate firewall. Once authenticated the users can access internal web applications, such as web mail, through the portal page. Additionally, the clients can download and install the SSL Network Extender plug-in to be able to use native applications such as ftp clients or email programs outside of the portal page. Like the IPSec VPN deployment earlier, the SSL VPN policy can be modified to force the clients to route all traffic through the gateway to ensure that while the clients are connected, the firewall will have the ability to inspect all traffic from the mobile system.

With SSL VPN deployed I again performed the packet sniffing test to see what information may be made available to potential hackers eavesdropping on the network. The only packets received by the hacker were the secure SSL packet communications between the client and the firewall. All data within the packets was encrypted and protected.

This shows that the SSL VPN was just as effective as the IPSec VPN in protecting the data during transfer between the client and the internal network. As such, the risk assessment for communications security has been adjusted in the same manner as the corporate owned laptop earlier:

Employee/Vendor Owned Laptop

Threat Category	Likelihood of Initiation	Vulnerabilities	Likelihood of Success	Overall Likelihood	Level of Impact	Risk
Communication Security	Very High	Very Low	Low	Very Low	High	Low

While SSL VPN was effective in mitigating the risks associated with communication security, it does nothing to address the risks from device security or theft/loss as the systems still lack the protection of any deployed security implementation such as a local firewall or anti-virus software. As such, SSL VPN must be combined with additional features such as endpoint compliance scanning and desktop virtualization.

With endpoint compliance scanning enabled, the employee/vendor owned system was successfully denied access to the site for failing to meet the security requirements of having a firewall software, anti-malware software, and the latest patched applied to the system.

With desktop virtualization, when the client connected it received a secure, virtual desktop from which to work while connected to the site. This prevented any data from the session from being stored locally on the machine.

With the additional features mentioned we can now re-address the device security and theft/loss of the employee/vendor owned laptop. For device security we have successfully blocked access to the corporate network from devices lacking security. With this deployment, the risk assessment has been adjusted as follows:

Employee/Vendor Owned Laptop

Threat Category	Likelihood of Initiation	Vulnerabilities	Likelihood of Success	Overall Likelihood	Level of Impact	Risk
Device Security	Very High	Very Low	Very Low	Very Low	High	Low

I have lowered Vulnerabilities to very low as the compliance scanning was effective in preventing the insecure system from connecting to the site, thus preventing sensitive information from being accessed and possibly leaked by the system. As such likelihood of success and overall likelihood were also dropped from high and very high to very low, effectively lowering the overall risk to low.

For theft/loss, we were able to reduce the risk of data being stored locally through the use of a virtual desktop. However, other avenues, such as emailing information to personal and/or free email accounts is not prevented by this deployment and so an avenue of risk still exists. Therefore, the risk for this category has been adjusted as follows:

Employee/Vendor Owned Laptop

Threat Category	Likelihood of Initiation	Vulnerabilities	Likelihood of Success	Overall Likelihood	Level of Impact	Risk
Theft/loss	Very High	Moderate	High	Very High	High	Very High

As can be seen, the only change to the risk was in the vulnerability rating from very high to moderate. While desktop virtualization has helped in reducing the ability to store information locally, the fact that avenues may still exist for which users can transfer data to their personal systems makes the overall risk still very high.

A look at Smartphone vulnerabilities and solutions

In addition to both the corporate owned and employee/vendor owned laptops, I also briefly explored applying similar solutions to Smartphones.

Due to a lack of resources, this study only looked at threats associated with communication security from an iPhone running iOS 5. Like the laptops, sniffing ftp traffic was

quite easy and provided the same level of information as the laptops with regards to usernames, passwords and content.

The iPhone however does benefit from a central application deployment solution through the Apple App Store. With this, security administrators can choose to deploy either a full IPSec VPN solution or an SSL VPN depending on the apps downloaded to the user's phone. With this, I deployed both solutions on the iPhone and tested their effectiveness.

With the IPSec VPN app I was able to connect to the site and secure traffic in the same manner as the IPSec client on the corporate owned laptop as the hacker system only ever saw ESP packets leaving the phone.

However, unlike the IPSec Solution on the corporate owned laptop, I was not able to force the routing of all traffic through the gateway as can be seen in the below image showing a traceroute from the iPhone to cnn.com. Using a traceroute app I could see that the first hop was to my external firewall rather than the firewall.

With the SSL VPN solution, users are limited to only web apps, preventing them from using any of the native applications that benefit from the IPSec VPN application. Only those apps defined as Web apps are allowed. No other access may be granted.

Solution Limitations

While the two solutions provided in this paper for both corporate owned and employee/vendor owned laptops were successful in lowering the risks associated with both communication security and device security, they do come with some limitations.

The centralized deployment for this lab was chosen for its simplicity and practicality but has benefits to real-world deployment as well. Khoo Boo Leong (2009) in an article in Network

World Asia states that the multi-layered protection model of firewalls, VPNs, content filtering, access control and security incident and event management is necessary still, but solutions can be found where these security elements are integrated into a single device. Leong states, “Clearly, reducing the number of disparate security devices and consolidating them into fewer appliances will lead to lower power consumption and simpler management.”

This deployment, however, lacks redundancy. Since the solution provided requires that all traffic from the mobile computing system be routed through the firewall, if the firewall were to go down or suffer a failure, outside users would be prevented from performing many of their necessary job functions. To address this limitation, a form of redundancy should be considered such as clustering whereby if the primary firewall fails, a secondary unit takes over.

With the employee/vendor owned systems, a restrictive endpoint compliance policy could prevent users that lack the technical acumen necessary to correct the security weaknesses from connecting to the site as well. As such, corporate security professionals could benefit from training employees on basic security principles to assist them with securing their own systems.

Lastly, neither IPSec VPN nor SSL VPN fully addresses the risk of theft/loss of laptops. The risk associated with this threat remains moderate to very high depending on the system. As such, corporate security professionals should look to additional measures such as full disk encryption, mandatory complex passwords and the use of data loss prevention mechanisms to prevent data from being distributed to third-parties via email or other means.

Conclusion

Mobile computing has become an essential part of doing business in the digital world. As such companies are more susceptible to breaches in security. This study illustrated those risks in

the form of three categories including Device Security, Communications Security and Theft/Loss.

A risk assessment was performed on each of the devices for the three categories that indicated that the corporate owned laptop was more secure when compared to the employee/vendor owned laptop, rating low, moderate and very high in the three categories whereas the employee/vendor owned laptop rated very high in all three.

The paper provides a solution in mitigating these risks in the forms of IPSec VPN and SSL VPN to encrypt and secure the connections from the client system to the corporate network. While it was shown that both solutions are highly effective in reducing the risks associated with communication security and device security, they are not without limitations and do little to nothing to mitigate the risks associated with theft/loss.

Implications for future research

This study highlights the need for further research in the areas of risk mitigation for Smartphone devices in addition to risk mitigation solutions for the theft and loss of all devices. Future studies should focus on implementation of data loss prevention systems and how they can be used to provide further mitigation to the risks associated with these devices.

References

Chenoweth, T., Minch, R., & Tabor, S. (2010). Wireless security: Examining user security behavior on public networks. *Communications of the ACM, 53*(2), 134-138.

Culnan, M., Foman, E., & Ray, A. (2008). Why it executives should help employees secure their home computers.*MIS Quarterly Executive*, *7*(1), 49-56

Deeson, D. (2005). Time wasting is theft and bad management. *Management Services*

Friedman, J., & Hoffman, D. (2008). Protecting data on mobile devices: A taxonomy of threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management*, 159-180.

FTC: Data leaked to p2p networks. (2010, May). *Information Management*, 7.

Johnson, M. E. (2008). Information risk of inadvertent disclosure: An analysis of file-sharing risk in the financial supply chain. *Journal of Management Information Systems*, *22*(2), 97-123.

Ipsec. (2012, October 11). Retrieved from http://en.wikipedia.org/wiki/IPsec

Ipsec basics. (n.d.). Retrieved from http://www.amaranten.com/support/user guide/VPN/IPSec_Basics/Overview.htm

Kalkbrenner, J., & McCampbell, A. (2011). The advent of smartphones: A study on the effect of handheld electronics on personal and professional productivity. *Journal of Applied Global Research*,*4*(8), 1-9.

Leong, K. B. (2009, August/September). Simplifying security in an age of collaborative and remote computing. *Network World Asia*, 14-17.

Loo, A. (2008). The myths and truths of wireless security. *Communications of the ACM*, *51*(2), 66-71.

Mayo, M., Pastor, J., Gomez-Mejia, L., & Cruz, C. (2009). Why some firms adopt telecommuting while others do not: A contingency perspective. *Human Resource Management*, *48*(6), 917-839.

Oien, S. (2008, June). Primary remote access: Consider ssl vpns. *Network World Asia*, 18 & 20.

Ponemon, L. (2008). Airport insecurity: The case of lost & missing laptops. *Ponemon Institute*.

Port 135 details. (n.d.). Retrieved from http://www.speedguide.net/port.php?port=135

Riaz Ahamed, S. S., & Rajamohan, P. (2011). Comprehensive performance analysis and special issues of virtual private network strategies in the computer communication: A novel study. *International Journal of Engineering Science and Technology*, *3*(7), 6040-6048.

Tan, D. (2002). Quantitative risk analysis step-by-step. *SANS Institute InfoSec Reading Room*

U.S. Department of Commerce, National Institute of Standards and Technology. (2011). *Guide for conducting risk assessments* (800-30)