Global Information Assurance Certification Paper

"Remote Access To The Corporate Intranet Without Compromising Your Security"

James Nierle
GIAC Security Essentials Certification (GSEC)
1 April 2004
Practical Version 1.4b Option B (Case Study)

ABSTRACT/SUMMARY

Remote access to the corporate intranet is in high demand as we transition from a completely wired networking environment to a predominantly mobile computing environment. The challenge for security personnel is to engineer solutions that allow legitimate mobile users access to data and services without jeopardizing the integrity, confidentiality, and availability of those data and services. This paper describes how this challenge was met in the European regional headquarters of a government agency. The solution was a combination of remote access methods, including the addition of *BlackBerry* wireless devices using General Packet Radio Service (GPRS) and Global System for Mobile Communications (GSM) networks, addition of a dial-up hardware virtual private network via the international wired public telephone network, and configuration improvements to the existing Outlook Web Access service. The result was faster, more reliable, more available, and more secure communications for the staff of the regional headquarters.

1. INTRODUCTION: THE CHALLENGE

The 150 person staff of the European regional headquarters spend much of their time out of the office, traveling throughout more than 80 countries in Europe, Africa, and Central Asia. As the Euro gained strength against the U.S. dollar, the cost of this business travel skyrocketed, which gave management a sense of urgency for finding means to make the staff more productive while on the road. Greater access to information was determined to be the key, and specifically the ability to send and receive email, surf the web, and gain access to data on the intranet, no matter where the staff member was physically located.

As the Information Assurance Manager for the European region, my challenge was to facilitate enhanced access to information services while neither violating the stringent information security policies directed by higher echelons of the government, nor compromising the security of our regional headquarters network.

This is a fundamental dilemma for information technology professionals: maintain adequate security while providing better communications capability (usually expressed by the user as more openness to data and other users). Since the network and the data it contains exist to facilitate business processes, security of the network and data is not an end in itself. Rather, objectives of the information security program are to provide levels of Confidentiality, Integrity, and Availability that are affordable and acceptable in view of the risk to those data and network services. The goal is to manage the level of risk to which you are exposed. Risk is in fact a key decision factor in how much and what kind(s) of security to implement. The SANS Security Essentials course teaches that risk is related to threats and vulnerabilities and the impact if information assets were compromised (the asset "value") in the following way:

Risk = Threat x Vulnerability x Impact (or value)[1]

[1] SANS Institute, pg 833.

This formula will be used later in the paper to explain why some of the technologies were chosen despite some vulnerability associated with each.

Due to the small size of the Information Technology department of this regional headquarters, some people do both IT engineering and information assurance/security work. To address this remote access problem, I formed a small team of network engineers and network administrators to develop alternatives, assess the risks and costs involved with each, identify the best achievable solutions and the policies that must accompany them, and then carry the technical and policy implementations of those chosen through to completion. While playing a personal role in all of these steps, my focus was assessment and selection of the technology and the security features to be implemented, and the development and implementation of policy. Technical installation was left to the network engineer and the administrators.

The goal was to introduce the new technology without increasing the overall level of risk to the existing network. We did so by weaving both technical security features and policy and procedures into the plan from the outset, using a security-as-an-independent-variable approach to the problem. Security was not ***the*** all-important variable, but nor was it treated as an appliqué, addressed only after satisfying the performance requirement. Truly effective security must be built into the network's technical design and the user and administrator procedures.

2. BACKGROUND: GENERAL DESCRIPTION OF THE NETWORK

The European regional headquarters network supports 150 users, one third of whom are typically away from the headquarters on official government business travel at any given time. While not a completely homogenous Microsoft Windows 2000® environment, it is nearly so. Only a few servers for special systems or applications run on variants of UNIX. All workstations are Win2K. Wide area network connectivity is provided via a global government enterprise network of leased circuits. Many Internet connection points exist in the enterprise, so the wide area connection leaving the regional headquarters is protected with a Cisco screening (filtering) router, a Cyberguard firewall, an intrusion detection system (IDS), and internal router and LAN. A rough sketch of this network is shown in Figure 1.

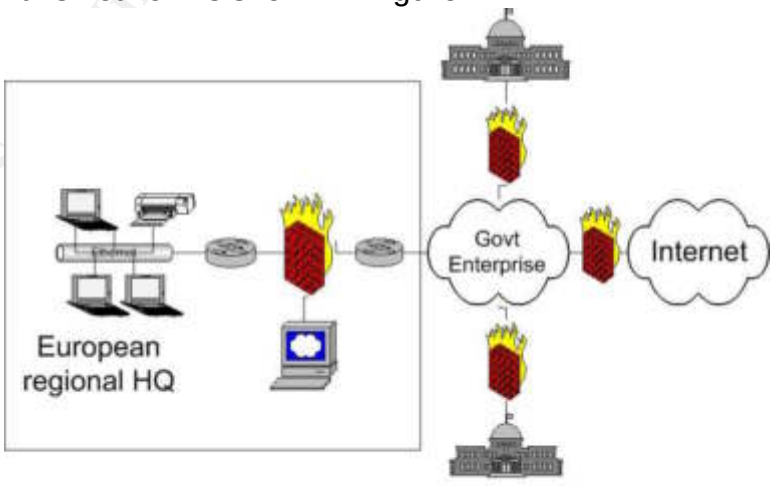

Figure 1. European Regional Headquarters Network

It is important to note that there is only one firewall. There is a "service network", on which sits the web server, but it is not a true demilitarized zone (DMZ). However, since remote access is the focus of this case study, the perimeter security systems will only be discussed in their relationship to remote access. Another important concern is the network described herein is not used for information related to national security matters. That highly sensitive and classified information is processed on a completely physically separate network.

While the project's genesis was to satisfy additional remote access requirements, we started by examining the existing remote access capabilities and architecture. These were found lacking in security, so improvements to those services were rolled into the project.

3. THE PROBLEM SPACE: BEFORE SNAPSHOT OF REMOTE ACCESS

Two types of remote access into the regional network were provided: access to email via the Outlook Web Access and dial-up access into the local area network (LAN) via the public switched telephone network (PSTN). The security and performance concerns of each of these are discussed below.

3.A. OUTLOOK WEB ACCESS (OWA) AND ITS ASSOCIATED RISK

OWA at the regional headquarters had been implemented to allow traveling employees to read and send email while visiting other government facilities around the globe, or to occasionally work from home (not telecommute). The configuration was a simple one. A hyperlink on the regional headquarters' main web page redirected the client side browser to a server on the intranet (inside the firewall) that was running the OWA service. This "front end" server authenticated the user by his/her username and password (same username/password used for the wired headquarters LAN), and then set up a secure socket layer (SSL) connection with the browser on the client machine. The front end server then pulled the relevant email data from the regional headquarters' main email server and served it up via HTML to the user on his/her client workstation browser.[2] The versions of software being used were Microsoft Internet Information Service® version 5.0 (IIS 5.0) and Microsoft Exchange® 2000.

Going back to the formula for risk for a moment, we look at a few of the threats and vulnerabilities of this OWA implementation and the impact if the assets were compromised.

One of the major threats to OWA was the unauthorized user trying to exploit the communication with the OWA server in order to penetrate the intranet and steal, destroy, or corrupt the data on the local network, or to compromise the regional headquarters network as a jumping off point to launch further attacks elsewhere in the government network. Another threat was the keystroke logger who captures the username and password of a legitimate OWA user during a legitimate OWA session and then uses those credentials to gain "insider" access to the network to conduct further exploitation. There are many such threats on the Internet targeting government

[2] Oppliger, pg 3.

networks, although perhaps not this regional headquarters specifically. Nevertheless, the possibility of my network being used as a springboard for attacks on other government agencies leads me to conclude that the threat is high.

The vulnerability that was of most concern was the ability of anyone on the Internet to communicate with our OWA server on the intranet. The web server was outside the domain, but it served no security function in regulating access to the OWA server. Since most of the website's information is releasable to the general public, access to the web server through the screening router and firewall is only denied by exception. Unless the user was coming in from a known malicious or suspicious IP address or range, or attempting unusual types of communications, he/she could hit the email logon hyperlink, and thus communicate with the OWA server inside the firewall. Once a valid username and password were supplied, the user had access to information on the Exchange® server. Given the multitude of vulnerabilities and avenues of attack that exist (many of which we do not yet know), we assumed that any hacker able to penetrate or circumvent the OWA authentication process would be able to do extensive damage to the entire intranet.

Although a secure socket layer (SSL) connection was used for OWA, this in and of itself did not prevent unauthorized access to the network. SSL does prevent a third party from intercepting the logon credentials in transit and then using them in a replay attack.[3] But in our implementation no client side certificates were required, and thus no authentication of the distant end computer was taking place. All authentication at the machine level was on the server side. The server provides the client a certificate with its public key, the client generates a session key, and sends it back to the server encrypted with the server's public key. Then the SSL connection is established with the session key. [4] So, all data communicated during the session, including the logon credentials, are protected from eavesdropping by third parties. But nothing within this SSL handshake established that the client or the user is an authorized OWA user of the regional headquarters network. That still rests solely on the logon script presented by the OWA server, and the username-password pair.

Several policies were put in place to mitigate the vulnerabilities described above. The Outlook Web Access feature was denied by default on all email account profiles, and permitted by exception for those users specifically authorized this service. Strong passwords consisting of at least 12 characters, a mix of numbers and letters, upper and lower case, and at least one special character were required by the system. These passwords were changed at least every 90 days. Only three incorrect login attempts were permitted before OWA for that account was suspended, with a 30-minute "cooling off" period before being re-enabled. Finally, the global enterprise imposed a policy prohibiting OWA from non-government client computers in public places, such as cybercafes, kiosks, and libraries. The intent was to counter the threat of passwords and government data being captured by keystroke logging or other eavesdropping mechanisms at the client side. This policy proved nearly impossible to enforce at the system level. As stated OWA was controlled at the account level, so if a user's account

[3] Oppliger, pg 3.
[4] SANS Institute, pp 551-553.

profile had OWA enabled, the user could physically access OWA from any client not specifically blocked by the perimeter.

Assessing the impact of loss of data or service is sometimes hard to quantify, especially in the government where costs of labor are not closely tracked and the data is not tied to revenue generation. The backup plan for the regional headquarters was good, and recovery from a complete loss of intranet data could be accomplished within 48 hours. The loss of availability of the data and network connectivity is the major concern in this organization. Certainly the lost productivity of two days without network access would be in the tens of thousands of dollars, just considering salaries. Continuity of operations plans do exist for this eventuality, but are beyond the scope of this paper. Considering the existence of the COOP and backup plans, I considered the impact of loss due to compromise of OWA to be moderate.

Considering the threats, vulnerabilities, and impacts, I was not comfortable with the security posture of OWA and knew that it could be improved for reasonable investment of time and money. Namely the ability to penetrate to the intranet via OWA needed to better controlled.

3.B. DIALUP REMOTE ACCESS

The dialup network access in the before situation could be described as "plain old dialup access." Several phone lines from the local (foreign owned and operated) public switched telephone network (PSTN) connected to 56Kbps modems which connected to a server on the intranet running Microsoft Remote Access Service (RAS). Utilizing government laptops, users dialed into one of these connections and logged into the headquarters domain. Of course unlike Outlook Web Access, with dialup the client computer is acting as part of the local domain, with full access afforded to the profile of the user who logged in.[5]

The threats and impacts with RAS are very similar to those for OWA. A major vulnerability is the reliance on a username and password as the sole defense for entering the LAN. Passwords were, again, required to be strong, but if you can defeat or circumvent the logon process, you own the network. The risk associated with this implementation of RAS with its lack of defense in depth were inconsistent with the level of security provided at the perimeter and elsewhere, and therefore needed to be tightened up.

4. THE "DURING" PHASE: CONSIDERING THE ALTERNATIVES AND DECIDING ON IMPROVEMENTS

4.A. SECURING OUTLOOK WEB ACCESS

OWA was revalidated by the users as a required service, so shutting it off was not an option. A couple of alternatives surfaced: use strong authentication for access to the service, and/or move the front end server outside of the intranet. [6]

[5] Davies, pg 1.
[6] Oppliger, pg 4.

Both of these seemed like good moves from a purely security point of view. But the absence of a second firewall to protect the intranet from the web server and the front end server made the option of moving the OWA server less attractive. Acquiring a second firewall was not feasible due to both the additional hardware and software costs and the enterprise wide restrictions placed on firewall configurations. These latter restrictions necessitate extensive coordination with higher echelons and a lengthy approval process to add a firewall. An architecture incorporating a second firewall is still being developed, but it was not going to get implemented during the timeframe of this project.

Strong authentication, however, was achievable without the red tape and added cost. The agency had already developed a public key infrastructure (PKI) plan using asymmetric cryptography for digital signatures, encryption of email, and authentication. Yet this plan had not been implemented to protect OWA. Since there was an existing program, there was no additional cost to use this technology for securing the OWA service. All users were already getting PKI certificates in both software and hardware forms. So, it was decided to utilize PKI certificate based authentication as a defense in depth measure, added to the existing username-password logon process.

PKI is an application of asymmetric key cryptography.[7] In symmetric key (or private key) cryptography, the communications end points share the same key. Therefore, they must have some secure means to distribute those keys, because anyone who gets the key will be able to read the traffic encrypted with that key. Digital Encryption Standard (DES) is an example of a symmetric key. [8]

Asymmetric key cryptography employs pairs of keys also, but each one of the pair are related but different. In PKI the pair consists of a public key and a private key. Each user is issued a unique public key and private key pair (also called certificate). Data encrypted with a user's public key can only be decrypted using that user's private key. This maintains confidentiality and integrity, as no third party can alter or read the data while in transit. And data encrypted with the private key can only be decrypted with the corresponding public key. This ensures identity (authenticity) and non-repudiation since only the person associated with that private key could have signed that data. [9]

In our agency's implementation of PKI each user received a key pair (hardware certificate) on a hardware token called a smart card. Some users also received different certificates on floppy diskettes (software certificate). The certificate uniquely identifies that user, and only that user has the password to his private key. The users' public keys and certificates were then stored in a central certificate server at the enterprise level. Other users in the enterprise could then obtain another user's trusted public key and then encrypt an email to that user employing that public key. The public key is available to anyone, while the private key is held solely by the user. [10]

[7] SANS Institute, pg 914.
[8] Ibid, pg 951.
[9] Ibid, pp 914-916.
[10] Ibid, pp 1013-1015.

A major advantage of the hardware token PKI is that it adds an authentication factor. The username-password pair used for OWA is a single factor authentication. You only need to "know" something, in this case the username and corresponding password. The usernames are often quite easy to guess or ferret out. The passwords, even when "strong", can be cracked using programs readily available for free on the Internet.[11] PKI added a second authentication factor that the user must "have," i.e. the smart card. [12]

The principal security vulnerability identified in our PKI implementation is the safety (secrecy) of the user's private key and password to that private key. Someone trying to penetrate the PKI encryption or spoof a legitimate PKI user must have both of those. Our policies and procedures prevented users from writing down their PKI passwords, and their certificates were loaded on smart cards that also served as physical identity and access cards, which therefore had to be carried on their persons at all times.

Each workstation on the network had to be outfitted with a smart card reader. Since this PKI program was implemented across the enterprise, all workstations on the global enterprise network were also being outfitted with smart card readers. This would allow the users to access OWA from any workstation on the global enterprise using his/her smart card. Support for use of certificates was already built into the enterprise wide browser, Microsoft Internet Explorer® 6.0. Training was provided to all users on the use of their smart cards with the browser for authentication, as well as with their email client for signing, encrypting, and decrypting of email. Development of this training was not time consuming or difficult, but it must be part of any plan to implement new security features.

Implementing PKI on the server side was only a bit more involved. The goal was restrict access to the OWA server logon solely to authorized users of the regional headquarters. One option considered was to have the web server do the PKI authentication before redirecting the client to the OWA server. However, since the OWA server was setting up SSL connections with clients outside the firewall, the OWA server's domain name and IP address were easily discoverable. Therefore, it would be a somewhat simple matter for a hacker to bypass the web server anyway and communicate directly with the OWA server. PKI authentication was implemented only on the OWA server to simplify the implementation.

To restrict access on a by-user basis required the storage of each authorized user's PKI public certificate on the OWA server. When the user hit the OWA link on the web server, he/she was redirected to a PKI authentication screen vice the previous username-password logon dialog. When the identity PKI certificate is requested, the browser presents the user with a choice of those certificates already installed. The user must select one and provide the key password in order to authenticate himself to the server. If the user's private key matches the public key already stored on the OWA server, the user is presented the email username-password logon screen. If not, access is denied and no domain logon attempt is permitted.

[11] Maguire, pg 1.
[12] Abbott, pp 10-11.

Another consequence of implementing this PKI solution was the system level enforcement of the enterprise wide policy on where OWA is allowed. Since very few public area computers currently provide support for smart cards, the necessity to use the PKI smart card for authentication effectively prevents OWA from those places.

PKI is not simple or cheap to implement. It required a major investment of resources across the entire agency. The creation and maintenance of a certificate authority hierarchy alone is a daunting task.[13] Introducing PKI solely to protect OWA at the regional headquarters would not have made financial sense. But since the agency had already introduced it for email (and planned for network logon) it was available for use at little to no addition cost, and therefore the cost-benefit was very favorable.

4.B. SECURING PLAIN OLD DIALUP REMOTE ACCESS

PKI was also considered for authenticating users for the plain old dialup access, and would have been selected had another more secure option not been available. To control access for a high security network within the agency, two hardware encryption based systems had been purchased several years before. The requirements for numbers of access lines had been overestimated at the time of purchase, and therefore one of the two systems was not in use on that high security network. I decided to reuse that system to secure the dialup access to the regional headquarters intranet.

The system is sold by Kasten Chase Limited under the product name *RASP Data Security*™. The two principal components of the system are the *Optiva*™ secure remote access server and the *Palladium*™ secure PCMCIA modems. The basic configuration of this system is shown in Figure 2 below. [14]

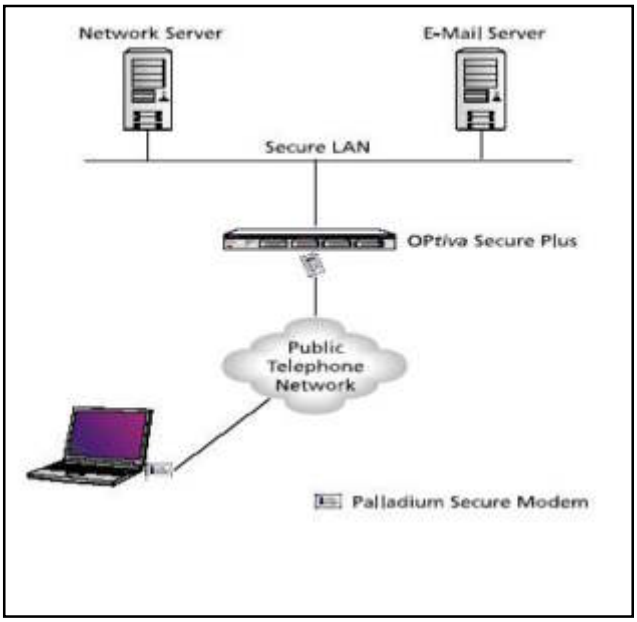

Figure 2. RASP Data Security™ Basic Configuration
© 2003 Kasten Chase Applied Research Limited

[13] SANS Institute, pp 1013-1015.
[14] Kasten Chase Limited. http://www.rasp4secret.com/

The OP*tiva*™ server was installed on the regional headquarters intranet LAN, with one *PALLADIUM*™ modem per each incoming telephone line from the local public switched telephone network provider. The number of phone lines and modems installed was based on local historical dialup remote access usage and input from users on expected use going forward.

Travelers wishing to use dialup remote access must have a laptop with a *PALLADIUM*™ modem in one of the PCMCIA slots. The IT section provides the user with the modem and it's unique password. The user simply dials in to one of the *OPtiva*™ phone lines using the native DialUp Networking function within Windows 2000. The client is authenticated based on the X.509 certificate loaded on the modem, and then granted access to the network logon screen for the regional headquarters LAN.[15] After supplying a valid domain username-password pair, the user is virtually made part of the LAN with access to all data and services, albeit limited performance-wise by a low speed analog telephone connection.

PALLADIUM™ contains a type of encryption called FORTEZZA® that was developed by the National Security Agency (NSA) for protection of U.S. Government communications.[16] Therefore, it was considered to be very secure in terms of protecting the confidentiality of the data communicated across the phone lines. It must be noted that the data is encrypted/decrypted at the modems for transmission only. There is no encryption of the data while it's on the laptop or the intranet.

RASP™ is a form of two-factor authentication. The user must have the *PALLADIUM*™ modem (uniquely identifiable by the certificate to the Op*tiva*™ server), and must know the password to unlock the encryption.[17] All of this makes the *RASP*™ a very secure solution for ensuring that only authorized users of the intranet are permitted dialup access, and that data exchanged is not subject to eavesdropping.

RASP™ is not cheap to implement. Besides the hardware costs, there is a requirement to manage the certificates for the modems. For government use, this requires access to a Certified Authority Workstation (CAW) that is capable of creating a FORTEZZA® certificate on the PCMCIA modem card. It is non-trivial for a small organization to maintain this capability in-house, as special equipment, training, and accreditation is required. But as was the case with PKI, the agency already had a sunk cost in this technology, so there was no additional outlay of money upfront. Reusing the technology to improve security added very little cost, but added significant defense in depth.

5. ADDING SECURE *BLACKBERRY* WIRELESS DATA SERVICES

The previous two sections discussed how additional security was added to existing services, which reduced vulnerabilities in these services in turn reducing the risk to the network. However, these improvements added no additional capabilities for the user. Performance of dialup access via international telephone lines was spotty, marked by

[15] Kasten Chase Limited. http://www.rasp4secret.com/
[16] Ibid.
[17] Abbott, pg 10.

lengthy synchronization times (achievable data rates of only 14.4 or 19.2 Kbps) and frequent disconnects due to noisy lines. OWA policies severely restricted the locations from which travelers could access their email. The users demanded a better mobile data solution. This section describes how that problem was solved.

The practical solution to more accessible communications was not difficult to come by. There existed very few options in Europe, and *BlackBerry* was an easy choice due to its small size, relatively high bandwidth, and broad penetration in the European market through the roaming agreements existing among the major cellular phone companies.

5.A. *BLACKBERRY* BACKGROUND

BlackBerry is the trade name of a proprietary wireless technology developed by the Canadian firm Research In Motion (RIM) Limited. It has been available in the U.S. market for several years, debuting in Europe in 2003. One very high profile customer of the system is the U.S. Congress. The *BlackBerry* Wireless Handheld™ can be thought of as a combination personal digital assistant (PDA) and cellular phone with email and Internet access capability. *BlackBerry* uses existing Global Packet Radio System (GPRS) networks for transport of data, and Global System for Mobile Communications (GSM) for cell phone voice service.[18] While it is possible to purchase devices and service directly from the cellular providers, this would involve user's having email accounts with the commercial provider. This was not acceptable for the regional headquarters from a security policy standpoint. The agency has a long-standing policy of not using commercial or free email accounts for official business. The more appropriate solution was to set up a virtual private wireless network using the *BlackBerry* technology and a commercial GPRS provider for transport.

The major components of the *BlackBerry* system implemented at the regional headquarters are depicted in Figure 3 below. In addition to the handheld devices carried by the travelers, a *BlackBerry* Enterprise Server™ (BES) was required on the regional headquarters intranet. The BES is linked to the existing intranet Microsoft Exchange® 2000 server via Messaging Application Programming Interface (MAPI). RIM proprietary protocols are used to extend email from the user's Microsoft Exchange® intranet email inbox to the *BlackBerry* device across the Internet and GPRS transport network, no matter where he/she is located. Likewise, all email generated by the user from the handheld transits the GPRS network and Internet back to the BES and Exchange® servers. The user has a wireless extension of his email account, and no one else need know that the user is not physically located at the regional headquarters. [19]

5.B. ASSESSING AND IMPROVING THE SECURITY OF THE *BLACKBERRY* SERVICE

Before purchasing and implementing *BlackBerry* it was necessary to evaluate the security of the system. This evaluation focused on specific security concerns for the regional headquarters LAN and the agency enterprise.

[18] Research In Motion, "BlackBerry Wireless Solution for GPRS/GSM Networks," pp 3-4.
[19] Research In Motion, "BlackBerry Security for Microsoft Exchange," pp 3-7.

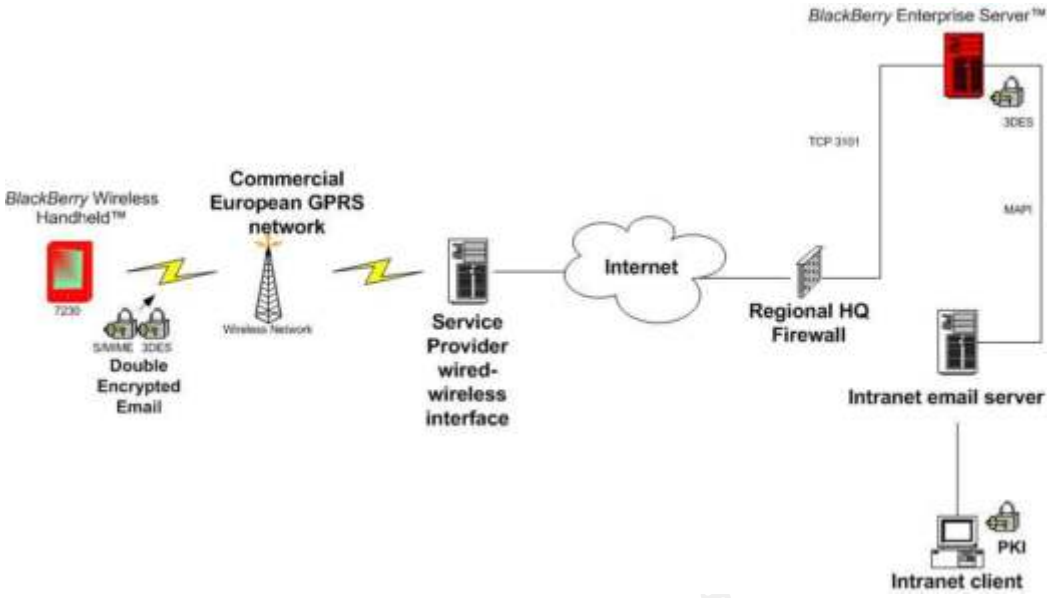

Figure 3. Regional Headquarters BlackBerry Data Service Installation

EMAIL CONFIDENTIALITY

The first security concern was the protection of data from eavesdropping while it transits the public networks between the BES and the handheld. Agency policy prohibited the use of this network for national security information, but the official government business transacted on the network is still a matter of sensitivity as not all information can be disclosed to the public. Confidentiality is provided with the out-of-the-box *BlackBerry* solution by Triple Digital Encryption Standard (3DES) encryption between the handheld and BES.[20]

Triple DES is a symmetric encryption key, so both endpoints of the encrypted communication link must share this same private key. Prior to placing a handheld in service, it must be registered with the BES by synchronizing it on the intranet. At that time a unique 3DES key is created for that handheld and stored on the BES. Each time the handheld comes up on the network and communicates with the BES, this unique 3DES key is used to encrypt/decrypt all data.[21]

In order to comply with global agency policy on protection of certain sensitive information, it was necessary to implement an end-to-end encryption capability beyond the inherent 3DES capability of *BlackBerry*. As described earlier, an enterprise wide PKI system existed, and this was extended to *BlackBerry*.

Adding this additional security to the out-of-the-box product was not trivial. A problem immediately encountered was the lack of a commercially available smart card reader for the *BlackBerry* Wireless Handheld™. This meant that we could not implement the

[20] Research In Motion, "BlackBerry Security with the S/MIME Support Package," pg 4.
[21] Ibid.

exact same PKI system being implemented on the intranet. Rather than wait for the product to become available, it was decided to use software based PKI certificates for the handhelds instead of smart cards. This was a slightly less secure implementation. After the user's certificates were loaded onto the handheld, the user only had to "know" the password to the certificate. He/she did not have to both "have" the token (smart card) and "know" the password. The alternative was to not have the end-to-end encryption protection provided by PKI, and that was less acceptable.

Implementation of PKI on *BlackBerry* required the add on S/MIME Security Package software offered by RIM. Secure Multipurpose Internet Mail Extensions (S/MIME) is a standard promulgated by the Internet Engineering Task Force that enables the use of PKI certificates in email. Certificates can be stored locally on the handheld for the primary user, and for other users with whom the user communicates often. Public certificates of other users can also be looked up in the enterprise certificate authority directory and imported as necessary in real time. Using the intended recipient's public PKI certificate, the *BlackBerry* user encrypts and digitally signs the email. The PKI protects the message against third party eavesdropping from the handheld all the way to the destination, where the intended recipient, and only the intended recipient, decrypts the message with his/her own private PKI certificate. During the transit from the handheld to the BES, the message was protected by both 3DES and PKI.[22]

PHYSICAL SECURITY

A second security concern was the physical loss or theft of the handheld device(s). The data storage capacity of the handheld is small, so the impact of any loss of data was likewise limited. However, loss of a device that can gain access to a legitimate user's email account and access the Internet from behind the corporate firewall remained a concern. The out-of-the-box solution has a couple of features to mitigate this risk. One is an automatic lock out with a time period is adjustable up to 60 minutes of inactivity. Once locked the device requires the PIN or password to be entered. A maximum of 10 login attempts is allowed, after which all data on the handheld is automatically erased.[23]

We tailored these default features for additional security. Group policy was set up on the BES to push standard security settings to each handheld every time the handheld was synchronized. First, we disabled the PIN feature and forced the use of a strong password to unlock each handheld. The inactivity lockout was set to 20 minutes. These settings could not be changed on the handheld without administrator privilege, which was retained among only two personnel within the IT section.

The lockout features, coupled with the ability of the BES administrator to immediately and remotely lock out any handheld suspected of being lost or compromised, made the vulnerability of a lost device being used for access low. The impact of a lost handheld, was determined to be essentially the price of the device itself.

[22] Research In Motion, "BlackBerry Security with the S/MIME Support Package," pp 5-6.
[23] Research In Motion, "Wireless IT Policy and IT Administration," pg 3.

SECURITY FROM INTERNET INTRUSION AND MALWARE

A third security concern was vulnerability of the handheld device and the BES to attacks from the Internet. The built in browser allows the *BlackBerry* user to access the Internet via a commercial provider or via our own regional headquarters intranet, using the *BlackBerry* Enterprise Server™ as a proxy.[24] The latter method was chosen for several reasons.

Email to the handheld was protected from malware by the anti-virus software running on intranet mail server and on every client workstation across the enterprise. All email from outside the intranet was also screened through the firewall, which stripped off known dangerous file types and file names. Although *BlackBerry* Wireless Handhelds™ can accept email forwarded from multiple email accounts, we instituted a local policy, enforced by the system settings within the BES, to prohibit all but the users' agency accounts. So, there was little probability that malware would get to the handheld from the Internet via email.

But there was no anti-virus or personal firewall software available for the *BlackBerry* Wireless Handheld™ at the time of purchase. So, access from the handheld to the Internet had to be controlled through a network whose security posture we controlled, namely our own. Using the *BlackBerry* Enterprise Server™ as a proxy ensured that all agency policies regarding appropriate use of the Internet would be enforced on *BlackBerry* users in the same way those policies were enforced within the intranet and dialup remote access environments.

BlackBerry Enterprise Server™ on the intranet was, of course, protected from the Internet by the existing perimeter defenses described earlier. To further limit its vulnerability to intrusion or denial of service, communications to and from the BES was restricted to only legitimate and necessary devices, ports, and protocols. Only a legitimate registered *BlackBerry* Wireless Handheld™ can initiate communications from the Internet to the BES, and this communication takes place only on a specific high end port. The firewall had to be configured to allow this port open. [25]

A further policy implemented to prevent infections was a prohibition against connecting, i.e. synchronizing, the handheld to any computer other than the designated workstations on the regional headquarters LAN. This was enforced through group policy settings forced to the handheld from the BES and unalterable by the user, as well as firewall settings that prevented any synchronizing of a handheld via the Internet.

Applying these policies and features ensured that the *BlackBerry* Enterprise Server™ and the handhelds were just as secure against threats from the Internet as any other servers or workstations on the regional headquarters intranet. This met the goal of not increasing the level of risk by introducing the new technology. In fact no other systems on the intranet were made any more vulnerable by the presence of *BlackBerry*.

[24] Research In Motion, "BlackBerry Security for Microsoft Exchange," pp 8-10.
[25] Ibid.

CONFIDENTIALITY OF INTERNET BROWSING TRAFFIC

Many web servers on the Internet now advertise themselves as "secure." In most cases this means they have a verifiable authenticity certificate and use secure socket layer (SSL) connections to your client browser. As described earlier in this paper, SSL is a means of encryption that provides confidentiality of the data between browser and server.[26] The *BlackBerry* Wireless Handheld™ has the ability to do SSL from the built in browser, but there is a performance penalty. For this reason we decided to rely on the Triple DES encryption between the handheld and the *BlackBerry* Enterprise Server™ for confidentiality for that leg of the connection, and to let the BES set up the SSL connection with the destination web server as a proxy. For non-SSL web connections, the Triple DES still prevents eavesdropping on web traffic while it transits the GPRS network. Once on the Internet after leaving our firewall, of course, unencrypted web traffic is subject to capture and inspection by anyone.

DENIAL OF SERVICE CONCERNS

The Triple DES, PKI, and proxied Internet access described above provide good protection for the integrity, authenticity, and confidentiality of *BlackBerry* data communications. These also provide some insulation from the inherent security of the GPRS wireless transport networks over which *BlackBerry* operates. Even if the GPRS network were penetrated, none of our *BlackBerry* data could be compromised, i.e. decrypted and examined. There is some vulnerability to the complete loss of service due to attacks on the GPRS network. Given the inherent nature of *BlackBerry* there is really no alternative transport available for the handhelds should all GPRS connectivity be cut off. It was decided to continue the operation of OWA and dialup remote access to mitigate the risk of such a situation. Although they don't offer the speed of performance that *BlackBerry* does, OWA and dialup remote access utilize completely different transport networks thereby offering a form of defense in depth against denial of service.
While discussion of GPRS and GSM security is beyond the scope of this paper, readers interested in this topic should consult Buchanan[27] and Chang[28] papers in the references.

6. CONCLUSION: THE AFTER SNAPSHOT

Adding PKI strong authentication to Outlook Web Access enhanced the security posture of the network. The two-factor PKI authentication was a significant step up from to the existing single-factor username/password authentication requirement. Would be attackers cannot gain access to the logon screen without significant effort. This makes it exponentially more difficult for unauthorized users to penetrate the system via OWA. Use of a password cracking program does no good if the hacker cannot even get to the logon screen without presenting the hardware token and corresponding password to authenticate himself as an authorized user of the LAN.

---

[26] SANS Institute, pp 551-553.
[27] Buchanan, Ronald M. "The Internet in the Palm of Your Hand." SANS Institute. August 2001.
[28] Chang, Dung. "Security Along the Path Through GPRS Towards 3G Mobile Telephone Network Data Services." SANS Institute. January 2002.

While strengthened from its original state, improvements can be made. The OWA front end server should be moved to the service network or better yet, a newly created DMZ, with the web server, so that direct communication from the Internet to servers on the intranet is prohibited. Further, OWA must be S/MIME enabled so that individual email messages can be signed and encrypted using the PKI certificates. It was not specifically mentioned earlier, but Microsoft Windows 2000/Exchange 2000 does not have native S/MIME support for OWA. This is a promised feature within Exchange 2003, and will provide a major part of the business case for migration to 2003. The addition of PKI to the Exchange 2000 Outlook Web Access was done with almost no additional cost. During the period of this project, migration to Exchange 2003 was not viewed as an option due to the agency's to budgetary cycle, the relative immaturity of the software, and the time required for administrator and security training. However, migration is planned for the next fiscal cycle.

The security of the telephone dialup network access is substantially stronger due to the addition of the hardware encryption server and modems. By requiring the outside user to have a uniquely identifiable hardware modem that is protected by a strong password, this system makes it nearly impossible for an unauthorized user to intrude on the intranet via this dialup service. Further, the encryption provided by the modems protects all data from eavesdropping while in transit, an addition of confidentiality that did not exist in the original (before) configuration. As with the introduction of PKI into OWA, there was little added cost to implement this hardware encryption RASP™ solution. The existing equipment and management infrastructure was simply reused to satisfy a different requirement.

While the security of the dial in remote access was improved, the performance was not. An area that remains to be explored is the use of software virtual private networks and laptop data encryption to allow remote users to securely join their laptops to the regional headquarters LAN via broadband Internet connections, such as exist throughout Europe in hotels, airports, and business centers.

Finally, the addition of *BlackBerry*™ wireless services provided a faster, more available, and far more convenient means of remote access. These are the performance features that the users were really demanding. The user no longer needs to find a suitable location on the agency's enterprise network from which to access OWA. Nor must they find a wired telephone line with a compatible jack over which to dial into the modem bank, suffering through 14.4 Kbps and 19.2Kbps connections. One major security enhancement that must be introduced is hardware PKI, once the appropriate reader is commercially available. The cost of the entire system of 50 *BlackBerry* Wireless Handheld™ devices, server, and all software licenses was less than 30,000 Euros. The continuing cost of operation is not much more than regular GSM cellular service, but with much more capability. In fact the observed trend thus far is an offset of cellular costs as users prefer using the email when traveling which is much cheaper than placing international roaming cellular voice calls. The introduction of local policies coupled with local configurations of the *BlackBerry*'s security features allowed us to make the system as secure as the existing intranet. Thus proving that it is possible to allow remote access to the corporate intranet without compromising your security.

LIST OF REFERENCES

Abbott, John. "Smart Cards: How Secure Are They?" SANS Institute, 2002.
URL: http://www.sans.org/rr/papers/6/131.pdf

Buchanan, Ronald M. "The Internet in the Palm of Your Hand." SANS Institute. August 2001.
URL: http://www.sans.org/rr/papers/68/22.pdf

Chang, Dung. "Security Along the Path Through GPRS Towards 3G Mobile Telephone Network Data Services." SANS Institute. January 2002.
URL: http://www.sans.org/rr/papers/68/165.pdf

Davies, Joseph. Microsoft Remote Access Introduction and Overview. Microsoft Corporation, Redmond, Washington, 2002.
URL:
http://www.microsoft.com/technet/itsolutions/network/evaluate/featfunc/msrasov.mspx

Dornan, Andy. The Essential Guide to Wireless Communications Applications. Upper Saddle River, New Jersey: Prentice-Hall, 2001. 75-79.

Kasten Chase Applied Research Limited. "RASP Secure Access" Website, 2004.
URL: http://www.rasp4secret.com/

Liang, Qiao and Xiangsui, Wang. Unrestricted Warfare. Beijing: PLA Literature and Arts Publishing House, February 1999.
URL: http://www.terrorism.com/documents/TRC-Analysis/

Long, Mark. "Product Review: RIM's BlackBerry 7000 Series." NewsFactor Network, March 2004.
URL: http://wireless.newsfactor.com/story.xhtml?story_id=23335

Maguire, James. "Windows Passwords Cracked in Record Time." NewsFactor Network, 2003.
URL: http://www.newsfactor.com/story.xhtml?story_id=21952

McDonald, Tim. "Email Encryption: Why isn't everybody doing it?" NewsFactor Network. 2002.

Oppliger, Rolf. "Microsoft Outlook Web Access: Blessing or Bane to Security?" IT Professional January 2003.
URL: http://dsonline.computer.org/0304/f/fp1opp.htm

Ramsdell, B. "S/MIME Version 3 Message Specification." RFC 2633. The Internet Society, 1999.
URL: http://www.ietf.org/rfc/rfc2633.txt

LIST OF REFERENCES (continued)

Research In Motion Limited. "BlackBerry Wireless Solution for GPRS/GSM Networks." 2003.
URL:
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/278486/BlackBerry_Wireless_Solution_for_GSM_GPRS_Networks.pdf?nodeid=271442&vernum=0

Research In Motion Limited. "BlackBerry Security for Microsoft Exchange." 2003.
URL:
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/278286/278425/BlackBerry_Enterprise_Server_version_3.5_and_version_3.6_Security_White_Paper_for_Microsoft_Exchange?nodeid=340694&vernum=0

Research In Motion Limited. "BlackBerry Security with the S/MIME Support Package version 1.5." 2003.
URL:
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/348231/BlackBerry_Security_with_the_S_MIME_Support_Package.pdf?nodeid=348232&vernum=0

Research In Motion Limited. "BlackBerry Wireless Solution for GPRS/GSM Networks." 2003.
URL:
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/fetch/2000/7979/278486/BlackBerry_Wireless_Solution_for_GSM_GPRS_Networks.pdf?nodeid=271442&vernum=0

Research In Motion Limited. "Wireless IT Policy and IT Administration." 2003.
URL:
http://www.blackberry.com/knowledgecenterpublic/livelink.exe/Wireless_IT_Policy_and_IT_Administration.pdf?func=doc.Fetch&nodeId=340697&docTitle=Wireless+IT+Policy+and+IT+Administration

Russell, Deborah and Gangemi Sr., G.T. Computer Security Basics. Sebastopol, California: O'Reilly & Associates, 1991.

SANS Institute. SANS Security Essentials. February 2003.

Last Updated: July 23rd, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor