

SANS

ADVISOR

CYBER NEWS YOU CAN USE

APRIL 2006

SANS INSTITUTE

VOLUME 2, NUMBER 1

In this issue: Instant Messaging

PAGE 2

Blackberry Deployment

**Configuring the Exchange 2003
Intelligent Message Filter**

PAGE 3

**Best Practices for Secure Wireless
PDA Operation**

PAGE 4

Secure Instant Messaging for Windows

**Secure Instant Messaging for OS X
Instant Messaging Security Tips**

PAGE 5

Terminal Server Forensics

Taking SNMP for a Walk

PAGE 6

**Service Oriented Architecture for
Web Services**

GSE Certification 2005

PAGE 7

Memory Forensics

Please Don't Decrypt My File

PAGE 8

**Guidelines for Choosing a Secure
Outsourced Exchange Solution**

TECHNOLOGY CORNER SECURITY TOOLS FOR YOUR WIRELESS DEVICE

There are many security issues to deal with when it comes to mobile messaging devices. Here are some software tools to help you make your PDA or Palm more secure. Best of all, they are FREE!

PAGE 3

INTRODUCING SANS ADVISOR

Welcome to the volume two, first edition of our newsletter. Our hope is to publish every six weeks. We offer short, pragmatic articles on what's new at SANS; as well as security, operations, audit and IT related legal topics. If you are interested in writing for the Advisor, contact stephen@sans.edu.

SANS has a new, exciting training track!

Management 524: Security Policy and Awareness.

This is a hands on course, you will learn how to write Security Policy by doing it. If your organization does not have policy, or if you need a tune up, this is the perfect course for you. The jewel of the course is the second part, we take you through everything you need to design and lift a security awareness program. If you are willing to be diligent and finish the labs, you will leave the class prepared to jump start your organization's awareness program. We even include a CD with example presentations and posters so you can use the skills you develop during the in-class exercises. In addition, when you certify we will allow you to teach our Awareness program, Security 351 which can be taught as instructor led, and also as an online course.

<http://www.sans.org/security06/description.php?tid=368>

"It's great to finally put all the pieces of the information security puzzle together."

Katrina Harris, PHH

BLACKBERRY DEPLOYMENT

If your company has decided to deploy the Blackberry solution by RIM, your security group has likely devoted a lot of effort to securely configuring the mobile handhelds. There are more than 100 security settings that can be configured centrally from the Blackberry Enterprise Server, all of them related to what users can or cannot do with their handheld device (e.g. screen lock, password policy, Internet browsing, etc.).

In addition to securing the handheld devices, your security group must also harden the central Blackberry Enterprise Server (BES). The BES will usually be located inside your company network and will be connected both to your corporate email server and to the Blackberry Routing Center through the Internet. This structure presents an interesting and threatening mix of internal and external connections.

The following three best practice tips, based on a defense-in-depth approach, are certainly not a comprehensive guide, but they will give you good advice for deploying a Blackberry infrastructure in a secure manner:

Server security: Keep your BES updated and patched, harden the underlying operating system, and check the BES logs (oper-

ating system and application level) periodically. BES logs are typically located in the *logs* subdirectory under the root installation directory.

E-mail server access security: Be aware that your BES will require admin rights in your corporate email server. This means that the BES server will have read/write access to all your Blackberry-enabled email accounts. Increase the monitoring level in your email server so you will have a better chance of detecting an attack more quickly.

Connectivity security: Best practices recommend using a proxy in your DMZ to handle HTTP communications between the Internet and your BES installed in your LAN. Your handheld policy should disable the *Blackberry Browser* to prevent split-tunnelling.

Remember, all emails sent or received by your Blackberry devices will go through one of the Blackberry Routing Centers. As a result, if you decide to use site-to-site email encryption, such as TLS, the messages will not be encrypted.

Alberto Partida, GSEC, GCFW, GCFA, CISSP, CISA

CONFIGURING THE EXCHANGE 2003 INTELLIGENT MESSAGE FILTER

Intelligent Message Filter (IMF) is Microsoft's offering to help reduce Spam on Exchange 2003 servers. IMF is free and can be downloaded from Microsoft's web site for Exchange SP 0 or 1 and is automatically installed with SP 2 for Exchange. It is disabled by default, and must be enabled before you can configure it successfully. IMF can be used to delete, reject, archive, or take no action on an e-mail that has the characteristics of spam. IMF also interacts nicely with Microsoft Outlook.

To configure IMF, there are two settings that have to be adjusted according to your organization's needs. The first, Gateway Blocking Configuration, allows you to decide what to do with a suspect e-mail at the Exchange level. It can be set to delete, reject, archive, or take no action, based upon the severity level (1-9) that you set for the sensitivity of the filter. The higher the severity level you select, the more likely that legitimate e-mails could be flagged as spam. It is considered best practice to set the severity level at 2 or 3. At this level, e-mails identified as spam

will not reach the users. It is also wise to configure the filter to archive e-mails that have been filtered. Review the archived e-mails weekly, and add the non-spam filtered e-mail addresses to the Global Accept list.

The next setting is Store Junk E-mail Configuration. This setting also has a 1-9 setting that will identify flagged junk mail. With the flag set, mail still passes the Exchange filter, but users can send it to the Junk Mail folder of the e-mail client. Set the junk mail flag a little higher, at 4 or 5. At this setting, users will be able to view flagged e-mails in their Junk E-mail folder, and have the opportunity to train their Outlook clients to direct legitimate e-mails to their inboxes in the future. Remember, because there is no perfect setting, it will take some time and practice to find the balance between legitimate and spam e-mails.

Charles Hornat, GCIH

BEST PRACTICES FOR SECURE WIRELESS PDA OPERATION

With so much talk about the security of Wifi, little attention has been given to securing other wireless communications that many of us use daily. Messaging devices, such as Blackberries and PDA-enabled phones (e.g. Treo and Ipaq) are becoming more and more common. Their processing power puts them on par with desktops systems of just a few years ago. The storage capacity is also amazing considering, with the addition of a thumbnail-sized SD card, I can add 1GB of storage to my PDA phone. The wireless capabilities, large file storage, and small physical size of such messaging devices present unique challenges for IT security departments trying to keep their key data inside the company. Here are some best practices for keeping your wireless devices secure.

1. Develop a Wireless PDA Policy.

Develop a clear policy on such devices and make sure all employees are informed of it. You may find you have more PDA phones in your company than you thought. The policy should cover the following items:

- **State whether PDA phones are or are not allowed. Many times PDAs fall outside the normal IT approval and procurement process.**
- **Define what type of employee is allowed to use them and for what purposes.**
- **Detail what information can be stored on them (e.g. contacts but no application data files)**
- **Specify the minimum level of security to which each device should be configured.**

2. Run Antivirus software on the devices.

Because they often sync with PCs and have Microsoft-like operating systems, PDAs can spread a virus within your organization. Employees should always run antivirus software on their PDAs, just as they do on their desktops. Both McAfee and Norton make versions of their antivirus software for the Palm and Windows Mobile operating systems.

3. Password-protect access to the device.

Users should password-protect the PDA functions of the devices. Setting a power-on password can be a hassle, but is your first line of defense should the device be lost or fall into the wrong hands.

4. Secure data stored on the device.

If your users store any data on their PDA, other than contacts and appointments, you should take additional steps to secure the data, especially if it is sensitive or confidential. Bypassing the power on password is trivial on some devices. Use a third party program such as *PGP Mobile* or *KeyCrypt* to encrypt the data.

5. Disable or secure short range wireless features.

Turn off or disable any Bluetooth or IR services if they aren't being used. Their interfaces could allow outsiders to access the device via a hacking process known as *blue-snarfing*. The first virus that spreads via Bluetooth has already been found. If you do use Bluetooth, make sure it is configured to connect only to your headset, car or whatever you are going to use it with. Not all models support these restrictions, unfortunately.

Tony Howlett, GSNA, CISSP

SECURITY TOOLS FOR YOUR WIRELESS DEVICE

There are many security issues to deal with when it comes to mobile messaging devices. Here are some software tools to help you make your PDA or Palm more secure. Best of all, they are FREE!

1. TuSSH (SSH client for PalmOS 4.0 and higher).

Have you ever wanted to log onto a server to check on something, but didn't have a computer nearby? You can do it securely from your Palm-capable cell phone using secure SSH. This program will allow you to connect to any SSH server. The terminal screen is a little small, so I wouldn't recommend any hardcore coding sessions; but it is just fine for checking a log file or making a quick change. <http://www.tussh.com/>

2. Keyring for PalmOS

This awesome program will store all your important accounts and passwords for different systems securely and in one place. (You don't still have the same password for all of them, do you?) Using Keyring is better than keeping your passwords on a paper system that could get stolen, lost, or destroyed in the rinse cycle. Keyring will even think up strong passwords that are easy to remember. Plus, unlike your little black book or laptop, Keyring and your wire-

less device are always with you. If the device is lost, all the data is encrypted using 112 bit Triple DES encryption. Most importantly, it is all backed up on your desktop when you hot-sync. <http://gnukeyring.sourceforge.net/>

3. Ministumbler (Windows CE, Pocket PC)

A part of the popular Netstumbler Windows wireless auditing program, this free software will allow you to audit your 802.11 wireless networks with your handheld. It is basically a fully functional version of the Windows program and is useful for doing wireless audits in hard to reach places, where a laptop would be difficult or awkward. I have used it to survey the perimeter of buildings and surrounding property, literally traipsing through field and stream, and for undercover audits of building lobbies and public spaces where a laptop might be too obvious. <http://www.netstumbler.com/downloads/>

There are lots of other pieces of software that may be valuable to you. Google on your wireless device model to see what is available for your platform.

Tony Howlett, GSNA, CISSP

SECURE INSTANT MESSAGING FOR WINDOWS

Gaim (<http://gaim.sourceforge.net>) is an instant messaging (IM) client that can be used with many different protocols. Users can also add to the feature-set of Gaim by installing additional plug-ins. One such plug-in is Gaim-Encryption (<http://gaim-encryption.sourceforge.net/>). The plug-in is very easy to install and supports RSA 512-4096-bit keys. Once Gaim-Encryption is installed, you generate a public and private key pair that will be used to encrypt communications with others. It is very important to note that both users communicating must install the plug-in and generate the keys. Once installed and active, your Gaim chat window will tell you if the communication is secure, using TX and RX lock icons. Public keys of users you are communicating with will be saved and you will be warned if the keys have been changed. You can view screenshots of Gaim with the plug-in active on the Gaim-Encryption website.

Should you have a requirement for secure IM communications, this is an excellent solution to utilize. Gaim, combined with the Gaim-Encryption plug-in, can be used to secure your communications with little effort on the part of the end user.

Richard Biever, CISSP, GSEC

“As a 15 year veteran of System Administration, the depth of knowledge learned was exceptional.”

Jerome Radcliffe, Internet Security Systems

SECURE INSTANT MESSAGING FOR OS X

In a multi-platform environment it is important that all operating systems in use have the ability to adhere to the security policy. Apple's OS X operating system is equipped with some of the latest security technologies, either included by default or available as an add-on package. If your policy states that all chat communications should be encrypted, as it probably should, there are some excellent options to accomplish this in OS X.

Adium (<http://www.adiumx.com/>) is a great, free, program that allows you to use several different instant messaging (IM) protocols. It also includes OTR (Off-The-Record), a tool that uses public and private key pairs to encrypt chat communications between clients. It is very easy to configure, however you must be certain that both parties to the chat communication have configured their clients. To configure your system using Adium, go to Preferences > Advanced > Encryption. You will then see a pull-down menu option for each account that you've created. To create your keys click the **Generate** button for each account. When you initiate a chat session, Adium will attempt an encrypted connection, provided the other party has configured OTR (in either Adium or another chat client).

Another alternative is to use OTR Proxy (<http://www.cypherpunks.ca/otr/>), which allows any chat program in OS X to take advantage of encryption. Its configuration is similar to that of Adium's, with the exception that you have to point your chat client at a local proxy.

If encrypting IM is required by your policy, the above two options will help you encrypt your messages using OS X. Even if you already have a secure messaging solution, encrypting a third party service could serve as a good backup.

Paul Asadoorian, GCIA, GCIH

INSTANT MESSAGING SECURITY TIPS

The instant messaging (IM) revolution keeps growing bigger and bigger. What was once the domain of IRC geeks, the desperate, and the dateless has become a communications tool for both personal and corporate use. Among the many IM networks you will find AIM, ICQ, IRC, Yahoo Messaging, and MSN Messenger.

Trillian is a front-end client for the above mentioned networks. Instead of installing multiple Instant Messaging (IM) clients, Trillian allows you to set up a connection for each network through a single interface. Irrespective of which IM system you use, hackers and malware use IM as an attack vector to compromise computers.

The following IM security tips are generic and can be applied to all IM network implementations irrespective of client type:

- Make sure you are using the most up-to-date version of your IM software and ensure that all security patches have been applied.
- As more and more Trojans propagate via IM, it is imperative that you keep your antivirus signatures up-to-date. This should mitigate the majority of malware-based risks.
- Never communicate sensitive or confidential information over IM networks.
- Ensure hackers and Trojans cannot “phone home” to isolate problems on your network and be sure you stop ongoing threats. You can take both of these steps by implementing a strong egress filtering (i.e. outbound) policy on your firewall.

Paul Leiao, GSEC

TERMINAL SERVER FORENSICS

Most fraud cases involve employees from within organizations. Do you know what a particular individual has done for the last months? In ordinary disk forensics an employee has a computer. The evidence on this computer, such as user-activity, deleted documents, and webmail can be gathered from the bit-copy of the hard drive. You probably will be able to reconstruct the contents of the hard-drive for a period of time, essentially an audit trail with content. But what if your client has a secure terminal service environment with thin-clients or is using a remote desktop? You won't be able to obtain much from the image. So you start looking at the network logging and finally the terminal servers. If you're lucky, the option `HKEY_LOCAL_MACHINE \ SOFTWARE \ Microsoft \ Windows NT \ CurrentVersion \ Winlogon \ DeleteRoamingCache` is not switched on in the group policy, and user profiles are stored on the terminal servers. Typically, that's where the evidence gets stored on disk temporarily. But what if your client has 25 or even more terminal servers with profiles of the suspect? Acquiring all those servers can be time-consuming and is not a realistic option. The evidence gathered from a terminal server is, in general, disappointing because of its multiuser role and I/O file operations of such a server. So, how can you make sure that user sessions are being logged and recorded for

a period of time? There is no cheap answer. However, you can take a few simple steps to store some contents and logs on the terminal server.

- **Use the appropriate security event logging. Who is logging on at what time and what applications he or she is activating are important for time line analysis.**
- **Make sure that you use cached profiles on your terminal servers.**
- **Use some cheap deletion-aware software that enables you to recover deleted files from users with potential evidence.**

But the best way is ensure that you can gather the evidence you need is to build an auditable terminal server environment that includes additional software that will record user sessions for a period of time. Citrix is currently developing the *IRIS Project* (ICA Recording ICA Surveillance), where user sessions get recorded and can be replayed. Another option is to install software called *AdminGuard* on the terminal servers. With either of these tools you will be able to reconstruct the past and find potential evidence of the fraud. These software packages can also be useful for analyzing compliance and liability in case a multi-million dollar server just crashed. You can determine if an administrator did or did not make a mistake.

Robert-Jan Mora, GCFA, GREM, EnCe, LPIC

TAKING SNMP FOR A WALK

A manager once told me, "We do not need strong SNMP community strings because they are passed in the clear." At this point I shook my head and moved onto the next issue. The truth is, I know how much of a mistake ignoring SNMP can be to the overall security of a device and network. Managing perimeter devices can be a time-consuming chore that SNMP positively impacts. Unfortunately, if SNMP is not implemented correctly, the effects can be damaging and lead to compromising everything it should be protecting.

When SNMP is enabled on a device it is generally available from all interfaces. This means that the device will respond to queries that contain the correct *read* or *write* community string. When the *read* community string is known, the device's information can be *walked*, meaning that much of the device's network configuration information can be obtained remotely. If the *write* community string is known, then the entire configuration file, which contains the administrator's password, can be downloaded and changes can be made to the device.

Follow best practices to avoid poor configurations. Be sure to use router Access Control Lists (ACLs) to control the source and destination of SNMP traffic and strong community strings pro-

tect SNMP access. Great sources for securing Cisco router configurations are *Securing Cisco Routers: Step-by-Step and Hardening Cisco Routers*.

A great example of network compromise through SNMP was written by Mati Aharoni and William M. Hidalgo and published in SecurityFocus in September, 2005. Other tools that can be used to test SNMP configurations include Net-SNMP (SNMP tools for Windows and Linux), ADMsnmp (SNMP brute forcer - Linux), Foundstone's SNScan (SNMP brute forcer - Windows), and Brutus (word list generation).

Don C. Weber, GSEC, GCUX, GSNA, GAWN, CISSP

For Further Reading:

Securing Cisco Routers: Step-by-Step – https://store.sans.org/store_item.php?item=70

Hardening Cisco Routers – <http://www.oreilly.com/catalog/hardcisco/>

Cisco SNMP configuration attack with a GRE tunnel – <http://www.securityfocus.com/infocus/1847>

Net-SNMP – <http://net-snmp.sourceforge.net/>

ADMsnmp – <http://adm.freelsd.net/ADM/>

SNScan – <http://www.foundstone.com/resources/freetools.htm>

SERVICE ORIENTED ARCHITECTURE FOR WEB SERVICES

Service Oriented Architecture (SOA) and Web Services are two of today's common catchphrases. A *Service-Oriented Architecture* is a collection of services that communicate with each other. A *service* in an SOA is a self-contained function that does not depend on underlying technology, exposing only what is needed to communicate with another service—similar to a class in an object oriented language. Communications range from simple (passing data from one database application to another) to extremely complex (coordinating patient treatment activities in a hospital).

Web Services form one set of technologies that connect the end points where SOA services reside in a service-oriented architecture. Two major consortiums, the W3C and OASIS, have created a series of XML-based standards that define Web Services, a principle one being the Web Services Description Language (WSDL).

The Simple Object Access Protocol (SOAP) referenced by WSDL, is an XML-based messaging standard defining the structures and rules for how Web Services messages are passed across a network. SOAP messaging is commonly implemented using HTTP, SMTP, or RPC, although other message transports such as .NET, Java Message Service (JMS), and WebSphere MQ are available. What does this mean for information security in general and messaging in particular?

Your SOA should be built to accept W3C and OASIS standards as they become available. These standards organizations are grappling with related Web Services security issues. The emerging standards range from enhancements to SOAP

that will ensure message integrity and confidentiality to XML-based standards for encryption, key management, and authentication. Standards influence product development within the security marketplace. Keep up-to-date on these standards.

Become familiar with available XML security products. XML has created a market for a class of security-related products that protect internal systems using Web Services. Traditional firewalls offer protection at the packet level and don't normally examine message content. Specialized XML firewalls examine message content (i.e., SOAP headers and XML content) and permit authorized content to pass through the firewall. Message routers and message adapters are available, some of which embed additional security controls for messaging.

Be proactive in planning for capacity and availability. While Web Services promise superior integration, they also present significant performance and availability challenges. The increasing use of XML-based messaging creates network and processing overhead that is a major hindrance to Web Services performance. Become familiar with the products that address XML-related performance, management, and security, such as XML accelerators.

Adhere to the basic tenets of good network security. SOA, Web Services, and messaging still rely on information flowing across a TCP/IP based network. The terminology will change, the tools evolve, and the challenges increase, but the basic tenets of good network security engineering remain as important as ever.

Barbara Filkins, GSEC, GHSC

“I learned more in one day than I could learn on my own in six months.”

Steven Wujek, Arthrex, Inc.

GSE EXAM 2006 SCHEDULE

The SANS Institute is pleased to offer you an opportunity to earn the GIAC Security Expert (GSE) certification, the highest level of Information Security certification and a recognized requirement of DoD 8570. Additionally, we announce the inaugural offering of two brand new GIAC Platinum certifications, GIAC Security Malware (GSM) and GIAC Security Compliance (GSC). We invite every qualified candidate to participate in the two day GSE, GSM or GSC certification exam at SANS Network Security 2006 in Las Vegas, Nevada on October 6-7, 2006. Please visit <http://www.giac.org/certifications/gse.php> for GSE and <http://www.giac.org/certifications/gsm.php> for GSM.

MEMORY FORENSICS

For years the primary focus of digital forensics has been the use of disk-based forensics to collect evidence. Now a relatively new field called *memory forensics* is arising. From the physical memory a lot of potential evidence may be extracted regarding actual intrusions. This is because intrusions are getting more advanced everyday with attackers using stealthier rootkit techniques, such as shadow walker and futo, to cover their tracks. These methods leave fewer traces of the intruders on the file systems used. Imagine, as an example, a memory resident rootkit being used by attackers on your servers. A lot of tools are available to check if rootkits are installed by the intruder. But can the output from these tools be used in court? Are these findings reproducible? No. When investigating these intrusions you have to acquire evidence that will hold-up in court.

In the case of an advanced intrusion, incident responders or forensic examiners often acquire both the physical memory and the hard drive from a hacked server. Until last year, however, we didn't know much about how to analyze the acquired memory. In the past a forensic-disk approach was used to examine the acquired memory image. This approach involved string searches or using data carving to look for specific headers or footers in the memory image. Unfortunately, the only conclusions that could be made indicated that the information was found in the physical memory of the server. You could not determine if a piece of malware or a rootkit was actually active at the time of the acquisition.

On Linux/Unix systems the physical memory is represented by the device `'/dev/(k)mem'`. On Windows systems the physi-

cal memory is represented by a section object, `device\PhysicalMemory`. The physical memory on both operating systems may be acquired in a forensically sound manner with the `'dd'` and `'netcat'` commands.

What kind of evidence can be obtained from a Windows-based memory image? On Windows-based systems active processes and system modules are kept in memory in doubly linked lists called `'PsActiveProcessHead'` and `'PsLoadedModuleList'`. When a process is activated, a creation time for that process is kept in memory. The memory image also contains the owner of a process, as well as the read, write and execute permissions of page table entries, and much more. A memory image frequently contains extracted file contents. You could say that the memory structure is like a file system, but more brief. Even hidden processes using rootkit-hiding techniques, such as hooking or DKOM, may be found in the memory image. You may also see from the obtained memory image if the process was active at the time the physical memory was acquired. All this information may be gathered from the image using a *hex-editor*. Since finding these artifacts of evidence can be a time-consuming process, the *Kntlist* program was introduced during last year's Digital Forensic Research Workshop 2005 (DFRWS) by GMG Systems, Inc. With this software, the acquired memory image may be quickly analyzed offline. Combined with a hex-editor or the Forensic Acquisition Utilities, *Kntlist* will enable you to understand what happened and find evidence about the intrusion.

Robert-Jan Mora, GCFA, GREM, EnCe, LPIC

PLEASE DON'T DECRYPT MY FILE

Pete Seeger once said, "A productive mistake is: (1) made in the service of mission and vision; (2) acknowledged as a mistake; (3) learned from; (4) considered valuable; (5) shared for the benefit of all."

With that in mind I have a confession to make, that will hopefully benefit others. I recently sent some important information to a colleague via e-mail. Because the information was sensitive I decided to encrypt it. I checked our company's keyserver and, when I did not find the recipient's public key, I encrypted the file with my private key and sent the file. This was a huge mistake because by encrypting the file with my private key, it can only be decrypted with my public key. Being a public key, everybody can decrypt the file.

To further the mission and vision of encryption I offer the following steps to anybody new to file encryption. These steps assume that the user has correctly installed GnuPG and has created a private and public key pair. If you need more information on GnuPG, please visit: <http://www.gnupg.org>.

First, make sure that you have the public key for the recipient.

```
user@gentoo ~ $ gpg --list-keys
```

Next, search a keyserver for the recipient's public key.

```
user@gentoo ~ $ gpg --keyserver pgp.mit.edu --search-keys fedora@redhat.com
```

Once you identify the correct public key, import it using the key ID.

```
user@gentoo ~ $ gpg --recv-keys 4F2A6FD2
```

Then, make sure the key imported correctly.

```
user@gentoo ~ $ gpg --list-keys
```

Finally, encrypt the file with the person's public key and sign the file with your private key to ensure non-repudiation.

```
user@gentoo ~ $ gpg -se -r fedora@redhat.com new_source.tgz
```

These steps are all it takes to start protecting sensitive data. Please, learn from my mistake and, hopefully, my shame will help me learn as well.

Don C. Weber, GSEC, GCUX, GSNA, GAWN, CISSP

