Global Information Assurance Certification Paper

Case Study: Spam Blocking, Content Filtering, Virus Scanning and Attachment Blocking in a Novell GroupWise Environment With Guinevere, SpamAssassin and Symantec (Norton) Anti-Virus Corporate Edition

Douglas Hitchen

GSEC Practical Assignment 1.4b (amended August 29, 2002)

Abstract

This case study details the implementation of Guinevere, a Spam blocking, content filtering, virus scanning, and attachment blocking solution, for a mid-size company running a Novell GroupWise 5.5 e-mail system.

This study details key aspects of the project including:

- A description of the computing environment both before and after the deployment of Guinevere
- An overview of the requirements and product selection
- Implementation of Guinevere in our environment
- An assessment of the effectiveness of the solution
- A Perl script and CGI code to Parse the Symantec Anti-virus Log Files and dynamically create web pages with blocked virus statistics
- Additional thoughts

1.0 Problem Definition

Our company has a central headquarters and 29 remote branch offices. We support about 250 e-mail users on a Novell GroupWise 5.5 e-mail system. This internal system connects to the Internet via the Novell GroupWise Internet Agent (GWIA), which provides no inherent filtering technology. We utilize Network Associates McAfee VirusScan 4.5.1 SP1 on all desktop machines. The virus definition files are updated weekly via automated processes and network login scripts.

Serendipitously, running GroupWise spared us from many of the Microsoft-targeted worms and viruses over the past few years. However, as these viruses grow smarter and stealthier, the need for multiple layers of protection increases. And, while spared from some of the viruses, we were not immune from the ever-increasing load of unsolicited e-mail (Spam). Users began complaining to our Help Desk, after some started receiving 20 – 30 Spam messages a day.

Spam falls into one of three categories:

- Trash: The e-mail's return address is invalid (the originating account closed after the message was sent) or the e-mail contains content deemed objectionable by the recipient. Cultural or regional idioms in a marketing e-mail may be considered offensive by those outside the culture or region and, therefore, also deemed to be Spam.

- Chain letters and hoaxes: These include such items as pyramid schemes and virus hoaxes. [To determine if a virus warning is hoax, check with your anti-virus vendor, or check Hoax Busters at this URL: http://www.hoaxbusters.org/].

- Unsolicited commercial e-mail: The e-mail is sent without the recipient's permission (opt-in) and without a method to stop future mailings (opt-out). (Caplan)

To combat this ever-increasing threat, I decided to research filtering and scanning solutions available that would integrate with our GroupWise 5.5 environment.

2.0 Requirements and Product Selection

There were several design goals for this project. We needed a product to scan and filter all e-mail entering or leaving our system for Spam, content, viruses, and potentially malicious attachments. The product should integrate cleanly into the Novell GroupWise environment and must be easy to install, configure, and maintain. Like any smart business, we also wanted the most cost efficient solution.

Initial online research yielded two potential products that integrate into the GroupWise environment, Guinevere and GWAVA.

Novell Technical Information Document # 10024073 indicates that server-based virus scanning solutions SHOULD NOT scan the GroupWise Post offices and GroupWise Domains.

> Why? The GroupWise message store is encrypted. Encryption renders virus scanners useless. When you point your server-based virus scanning solution at GroupWise you cause needless processor overhead because the virus scanning software is scanning files that it can't possibly detect viruses in.
>
> Perhaps a user might place a file into the e-mail input queues in an effort to sabotage the e-mail system. Even if someone were to place a file in one of the GroupWise queues in an effort to somehow route the virus into the e-mail system, the GroupWise agents would just throw the file away. The agent would throw it away because it would see that they file was not in the correct format, virus or no virus. The file would not be routed to the administrator either.
>
> Another good reason to keep anti-virus software away from the GroupWise message store is that it can cause timing-related problems. Virus scanning software seems to have difficulty related to the speed in which files move from one GroupWise queue into the next. They'll exert a lock on a file, but never release the lock for example. Do yourself a favor, use Client/Server connections to the GroupWise message store, and steer your server-based virus scanning solution away from your GroupWise System. (Novell TID # 10024073)

2.1 Effective Methods of Handling Internet E-mail Viruses Coming Into GroupWise

Armed with the knowledge of what not to do, I pressed on to find Novell's recommended approach to this type of scanning and filtering.

> One of the biggest threats to your computing systems are the Internet propagated e-mail viruses. The best way to stop these viruses is at the entry point from the Internet. The GroupWise Internet Agent is the entry portal for Internet e-mail into the GroupWise System.
>
> There are two approaches to providing an e-mail virus scanning solution. They are:
>
> 1. SMTP mail hosting with a virus scanner
> 2. GWIA third-party queue integration
>
> Novell Technical Information Document # 10007320 explains how to configure your GWIA for both of these solutions.

2.1.1 SMTP Mail Hosting

Mail hosting means that the GWIA is not sending or receiving SMTP mail with Internet SMTP hosts. Another SMTP device, the "host" is hosting the mail for the GWIA. The host receives e-mail from the Internet. In the case of virus scanning mail hosts, the host scans the messages for viruses and then forwards them back to the GWIA via the SMTP protocol. Outgoing e-mail from the GWIA can be configured to relay it's outgoing e-mail to the mail host. The mail host then scans outgoing mail for viruses on their way out onto the Internet.

2.1.2 GWIA Third-Party Integration Queues

When the GWIA receives messages from the Message Transfer Agent (MTA), it converts the message to ASCII format. The GWIA typically spools these files up to its internal SMTP Daemon. The GWIA can be configured so it spools these files into a different "third-party" directory. The third-party software will then scan the files in the third-party queue for viruses. The third-party software must then move the files to an input directory for the GWIA.

Many third-party solutions are written in such a manner that they work for many e-mail systems as a virus scanning solution. (Novell TID # 10024073)

Please see the following links for information on two third-party virus products written specifically for GroupWise.

- Guinevere
  http://www.openhandhome.com/guinevere/default.html

- GWAVA
  http://www.beginfinite.com/html/products.html

Other non-GroupWise specific products, most of which act as an intermediary SMTP gateway between your local mail server and the Internet, were also reviewed briefly. These included:

- CS MailSweeper™ for SMTP: Anti-spam Edition
  http://www.mimesweeper.com/products/antiSpam/Msw/default.asp

- MailMarshall
  http://www.marshallsoftware.com

After reviewing features and pricing, I decided on Guinevere. Its architecture utilizes the third-party queue feature of GWIA to process all e-mail entering or leaving the gateway. GWIA is reconfigured to filter all e-mail through the Guinevere queues rather than the standard queues.

Guinevere inherently provides the following features: signatures, filters, attachment blocking, archiving, oversize message handling, return receipts, and management.

> Guinevere provides integration with one of the best (and free) utilities in the world to find Spam – Spam Assassin. This product was developed on Unix, but it works on Win32 – with some modifications, all of which are fully described in the installation documents.
>
> So SpamAssassin is truly wonderful. It works by applying about 500 rules, mostly text checks, but also RBL lookups, DNS checks, and other sophisticated algorithms. It totals up the score from each of these, and if the sum exceeds a pre-defined threshold, marks them as Spam. (Bell, *User* Manual 41)

Follow these instructions thoroughly and test SpamAssassin before enabling this feature within Guinevere.

Anti-virus Scanner Selection

According to Michael Bell, Guinevere relies on a third party anti-virus product installed on the same box to perform the virus scanning. Since we already use Network Associates VirusScan 4.5.1 SP1 on client desktops, I chose to layer my approach to virus defense by deploying a different scanner here. Running different anti-virus products at the gateway and on the workstations adds to our "Defense in Depth" strategy, ensuring that a virus that makes it by one scanner is seen and hopefully caught by the other (SANS Institute). This configuration benefits from two signature bases and two heuristic approaches from two different companies.

Several independent organizations test the effectiveness of the scanning engines. The ICSA Labs (http://www.icsalabs.com) test and certify security related products, including anti-virus systems, as does West Coast Labs (http://www.check-mark.com) and Virus Bulletin (http://www.viursbtn.com). They provide an independent view on the abilities of products to perform to high standards.

After reviewing the test methods, results and certifications, I selected Symantec (Norton) Anti-virus Corporate Edition 7.61. Symantec is another leader in the anti-virus arena and this product has received favorable reviews and/or certification from the independent testing organizations.

For testing and certification results, please visit:

ICSA Labs Certified Products: Anti-virus Scanner
http://www.icsalabs.com/html/communities/antivirus/certification/certprod.shtml

> The goal of ICSA Labs' Anti-Virus Product Certification is to significantly improve commercial computer trust and security. While recognizing that perfect computer security is unattainable, ICSA Labs' Product Certification Program provides assurance to the user community that anti-virus products attaining the ICSA CERTIFIED rating reduce security risks caused by viruses and other malware consistent with a set of publicly vetted and industry-accepted criteria. (ICSA Labs)

Checkmark System Information: Anti-virus Checkmark Level One
http://www.check-mark.com/checkmark/ph_symantec.html

> For a product to be certified to Anti-Virus Checkmark, Level One the product must be able to detect all those viruses which are "In the Wild". This gives a clear and independent indication to end users of those anti-virus products that can be relied on. (Checkmark System Information)

Checkmark System Information: Anti-virus Checkmark Level Two
http://www.check-mark.com/checkmark/ph_av2_symantec.html

> For a product to be certified Anti-Virus Checkmark, Level Two the product must comply with Anti-Virus Checkmark, Level One and, in addition, disinfect all viruses on the "in the wild" list which are capable of disinfection. (Checkmark System Information)

Virus Bulletin: VB 100%
http://www.virusbtn.com/vb100/archives/products.xml?symantec.xml

> The VB 100% logo is awarded to anti-virus products that:

- Detect all In the Wild viruses during both on-demand and on-access scanning in Virus Bulletin's comparative tests
- Generate no false positives when scanning a set of clean files. (Virus Bulletin)

Guinevere and Symantec Anti-virus met all the requirements at a very reasonable price. Guinevere actually provided a wealth of features I hadn't even considered in my initial requirements analysis. In the Guinevere 2.0 Feature List, Michael Bell describes Guinevere's features as including the following.

2.2 Guinevere's Features

- Antivirus scanning of inbound and outbound Internet e-mail
- Centrally administered signature/disclaimer messages
- Powerful mail filters, allowing you to delete, archive, forward, CC, etc. various e-mail messages
- Return Receipt capability

2.2.1 Anti-Virus

- UniversalAV (tm) - Improved anti-virus integration supporting virtually any real-time scanner
- Integrations included for virtually every AV scanner on the market, including Mcafee, NAV (Symantec), Inoculan, Sophos, Trend Micro, F-PROT
- Support for CLEANING (not just blocking) messages containing viruses (Requires Mcafee or NAV)

2.2.2 Spam Protection

- SpamAssassin integration, allowing heuristic Spam analysis and RBL (Relay Black List) lookups (Requires Windows NT/2000/XP)
- Anti-relay protection
- Mail Filters (see below), allowing blocking by address or partial address

2.2.3 Signatures

- Signatures can be configured in both plain text and HTML
- They can be positioned at the top or the bottom of a message
- Improved signatures, multiple signatures, dependent on various criteria (wildcards ok)
- Allows you to suppress signatures conditionally

2.2.4 Filters

- Filter by incoming or outgoing message flow, by FROM or TO address, or by SUBJECT (wildcards ok)
- Actions include DELETE, FORWARD, ARCHIVE, STRIP, CC, and combinations thereof
- FORWARD/CC can be as encapsulated attachment or preserve original message structure
- REPLY filter, allowing you to create auto-reply messages
- Configurable user exceptions to Mail Filters

2.2.5 Attachment Blocking

- Block by extension or partial filename
- Block dependent on direction of message flow
- Auto-block common virus threads such as VBSCRIPT, double-extension filenames, etc.
- Finger Printing technology. Guinevere can now analyze individual files and determine their type regardless of extension. It's now nearly impossible for any file type to pass into your system that you don't want.
- Configurable user exceptions to Attachment Blocking
- Recursion
- Manual build of Attachment Blocks no longer needed

2.2.6 Archiving

- Archive messages using the Mail Filters, by direction of mail flow, or by event (such as infection)
- Compress archives automatically
- Archive viewer to conveniently read, search, print your archives

2.2.7 Oversize Messages

- Block messages exceeding a specified size
- Defer outgoing messages over a specified size until a particular time window

2.2.8 Return Receipts

- Request Return Receipts via MDN or RRT
- Always Request Return Receipts
- Outgoing Mail Analysis, allowing you to know exactly what's going on with that e-mail you sent

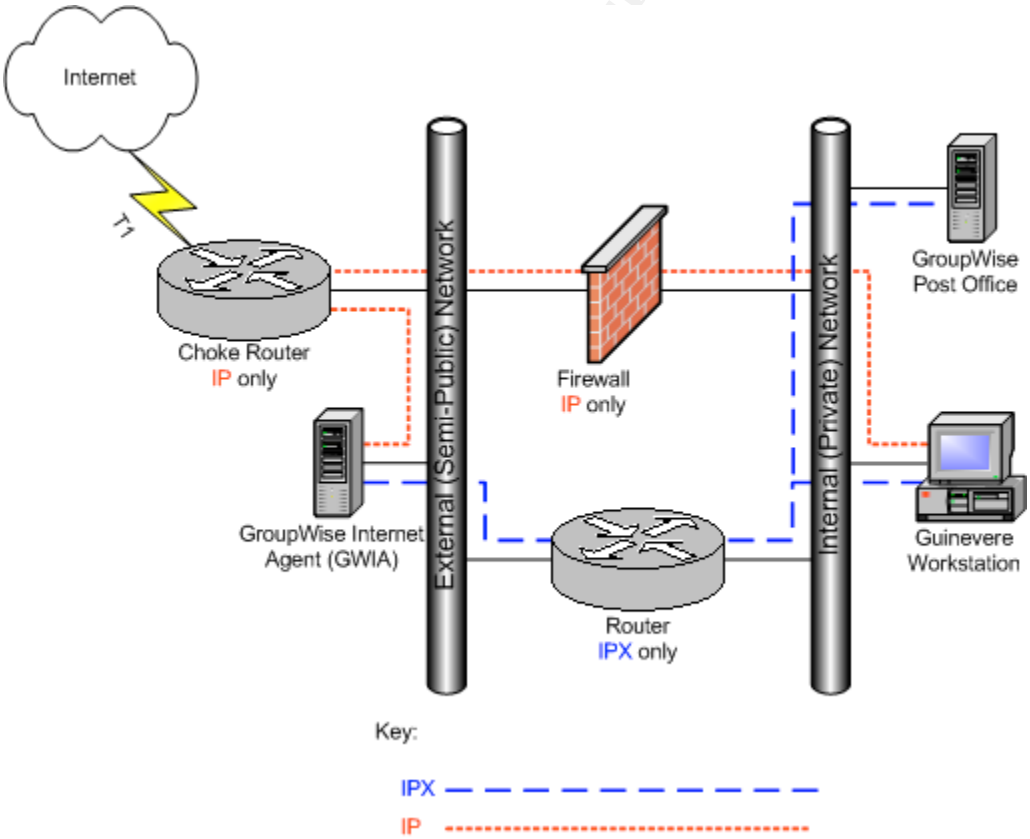
2.2.9 Management

- SNMP support
- Full, detailed logging
- Event Logging, offering a convenient way to create reports, and parse logs
- Vastly improved configuration program
- Preserve statistics upon reload
- Dynamic configuration reload
- Pause processing (Bell, *Feature List*).

3.0 Implementation

I installed Guinevere on a 1 Ghz PC with 512 MB RAM running Windows 2000 Workstation. The workstation communicates with the GWIA via a mapped-drive connection over IPX and uses TCP/IP to download anti-virus updates from Symantec. I loaded TightVNC 1.2.8 to allow remote controlling the box as it is in a locked server room, distant from support staff (TightVNC). I also tunnel TightVNC over SSH for access from the Internet (AT&T Laboratories). The figure below illustrates how I integrated Guinevere in to our environment.

Figure 1: Guinevere Integration in Our Environment



The IP and IPX protocol separation provides an additional layer of defense in our overall security architecture. Inbound IP is very restricted and is not allowed to pass through the firewall. This helps ensure that if the GWIA box gets compromised, the damage is contained at that point and not allowed to ride freely into our private network over IP.

3.1 Guinevere Installation and Configuration

I installed the following software on the Guinevere workstation:

- Windows 2000 with current service packs and hot-fixes
- Microsoft Client Service for NetWare
- Guinevere 2.0.8a – 2.0.13 beta
- Symantec Anti-virus Corporate Edition 7.61
- ActiveState Perl 5.6.1 build 635
- SpamAssassin 2.42
- Apache 2.0.44 (not required, used for dynamic virus count web pages)
- Novell GroupWise 5.5 client

I enabled features in Guinevere over a period of a few days to ensure that each change worked correctly before tweaking the next setting. Anti-virus took honors as the first feature enabled, followed by attachment blocking, then filtering, and finally the SpamAssassin integration. My initial filter set was very basic, containing unacceptable or offensive language in the subject and e-mail from known offenders. After following the support newsgroup on Yahoo, I found a far more comprehensive filter list (Mayer). I downloaded and reviewed the list. After cleaning it up a bit, I integrated it with my existing list, using a filter merge utility written by one of the newsgroup participants. This newly merged list was much more aggressive so I monitored for false positives a few days and either modified the filters or created exceptions as appropriate.

I upgraded Guinevere four times since the original installation. I started with version 2.0.8a and have since upgraded with version 2.0.9, 2.0.10, 2.0.11, and 2.0.12. I also applied 2.0.13 beta to fix problems related to the recent MiMail virus (CERT® Incident Note IN-2003-02).

I have not upgraded SpamAssassin since the original installation. I am currently running version 2.42. There are some appealing features in the newer (2.50 and higher) versions of SpamAssassin, like Bayesian Spam analysis (SpamAssassin).

Next I will review the various Guinevere configuration settings I enabled or tweaked and describe why each setting was chosen. This represents my current configuration.

3.1.1 Virus Scanning

> This screen is where you enable or disable virus scanning, select a virus integration method, and adjust some UniversalAV parameters. Virus Scanning,

like most settings, is disabled by default to allow testing of mail flow and verifying that GWIA is passing files back and forth correctly through the new third-party queues. (Bell, *User Manual* 30)

After testing mail flow and configuring Symantec Anti-Virus per the Guinevere User Manual, I unchecked both "Don't scan for viruses in incoming messages" and "Don't scan for viruses in outgoing messages" to enable this highly desired feature. I chose these settings to enable virus scanning for both incoming and outgoing e-mail. I selected UniversalAV for the "AV Program" because it is faster and more flexible. I configured the following Symantec Anti-virus settings, which are required for UniversalAV integration.

1. Norton Antivirus services must be loaded
2. Go to Configure/File System Real Time Protection
3. Enable file system real-time protection, and select ALL files
4. Set these actions for both macro and non macro viruses:
   first action: Delete, second action: Quarantine
5. Uncheck network drives (important, or the computer may scan the GWIA)
6. Uncheck Display Message on Infected Computer
7. Check the Exclude Files/Folders, and configure it to exclude c:\guin2 and subdirectories (Bell, *User Manual* 89).

3.1.2 Attachment Blocking

"This is where you can prevent specific filenames or extensions or file types from entering/exiting your e-mail system" (Bell, *User Manual* 32). I modified the included sample file, BLOCKIT.SMP, to arrive with the following list of blocked extensions:

> ADE, ADP, BAS, MSC, BAT, MSI, CHM, MSP, CMD, MST, COM, PCD, CPL, PIF, CRT, REG, SCR, HTA, INF, URL, INS, ISP, VBE, VBS, JSE, PPA, WSC, SCT, LNK, WSF, WSH, SHS, SHB, EMF, HLP, MDB, OCX, DLL, EXE

I chose this list to protect our users from potentially dangerous file attachments. Our Electronic Communications Policy prohibits users from downloading or running such programs anyway. Enabling this feature helps enforce that policy.

I also enabled Finger Printing and selected "Block all forms of DOS and Windows executables."

> Finger Printing works by actually opening each attachment and analyzing them for unique file signatures. This makes it extension-independent.
>
> Fingerprinting is a new (and optional) technique for blocking specific types of files. It was introduced because of these limitations of the standard attachment blocking technique:

1. You have to rely on the extension to determine the file type. This can be unreliable, and for a knowledgeable user, easy to bypass by renaming.

2. You can only check the main directory. If the attachment contains an archive with a directory structure, you'll miss those files with standard Attachment Blocking (Bell, *User Manual* 35).

3.1.3 Mail Filtering

As mentioned earlier, I first started out with a short and very basic filter list, until I discovered a more comprehensive list in the Guinevere General Discussion List on Yahoo (Mayer). I cleaned up the list and added several new entries and now have a filter list with 495 entries. It is helpful to block as much Spam as possible this way as it is never handed off to SpamAssassin and is thus less processor intensive.

> Use Mail Filtering to perform special actions upon messages with specific criterion. You can filter by FROM, TO, and SUBJECT. You can configure specific user exceptions to the Mail Filters in the User Exceptions section of the Configuration Program (Bell, *User Manual* 36).

3.1.4 SpamAssassin

This is another critical element to configure correctly to get the most usefulness out of Guinevere. Configuration is not for the feint-hearted, but the instructions provide ample detail to get this up and running.

> It works by applying about 500 rules, mostly text checks, but also RBL lookups, DNS checks, and other sophisticated algorithms. It totals up the score from each of these, and if the sum exceeds a pre-defined threshold, marks them as Spam. (Bell, *User Manual* 41)

SpamAssassin utilizes the following techniques:

> **header analysis:** Spammers use a number of tricks to mask their identities, fool you into thinking they've sent a valid mail, or fool you into thinking you must have subscribed at some stage. SpamAssassin tries to spot these.
>
> **text analysis:** Spam e-mails often have a characteristic style (to put it politely), and some characteristic disclaimers and CYA text. SpamAssassin can spot these, too.
>
> **blacklists:** SpamAssassin supports many useful existing blacklists, such as http://mail-abuse.org, http://ordb.org or others (SpamAssassin).

3.1.5 Signature Files

This feature was not necessary to meet any of our stated requirements and is thus not enabled.

3.1.6 Oversized Messages

Michael Bell states that, while GWIA provides some built-in mechanisms to limit incoming and outgoing message sizes, these options are limited (*User Manual* 49). Guinevere addresses these shortcomings nicely. While also not necessary to meet any of our stated requirements, I did enable this feature as another layer in our overall protection strategy. This can prevent an availability outage that could be caused by someone overloading the gateway or e-mail server with excessively large messages or file attachments.

I configured Guinevere to block incoming messages exceeding 15,360 KB (15 MB) and to defer processing outgoing messages exceeding 20 MB until after 10:00 PM. The latter option prevents large outbound messages from bogging down the system during normal business hours.

3.1.7 Archiving

"It's useful to be able to archive messages passing through your GWIA. You may need them for disclosure or disciplinary reasons. Or you may need to check if a particular message is really infected" (Bell, *User Manual* 51). I configured this option to archive inbound and outbound messages only when infected or blocked. This allows me to put a message back in the queue if it is blocked unintentionally. I also set Guinevere to turn off archiving when disk space is below 500 MB to prevent a system outage due to the hard disk filling up with archive files.

3.1.8 Return Receipts

This feature was not necessary to meet any of our stated requirements and is thus not enabled.

3.1.9 User Exceptions

Here, you can set up specific users (or pattern matches) to be excluded from the Mail Filtering, Oversized Messages, Spam, and Attachment Blocking rules (Bell, *User Manual* 56). This provides a convenient way to override all the other rules for specific exception cases. Our Help Desk can also use this to quickly open a temporary "hole" in the rules to get a critical message in or out. They close the hole by quickly removing the exception after the message gets through.

3.1.10 Location of Files

"The Location of Files section is where you set many of the fundamental directory path locations for Guinevere. You can also re-run the Location Of Files Wizard if you choose" (Bell, *User Manual* 58). These settings were configured during the initial installation and required no additional changes.

3.1.11 Notification/Disposition

> This section is where you configure how infected or blocked message should be treated – whether the message should be destroyed or partially preserved, whether the sender and Administrator should know about the problem message, etc. (Bell, *User Manual* 61)

I set the disposition of infected or blocked messages to remove attachments, but preserve the text message. This passes information on to the original recipient as to the problem with the message. This is useful to our Help Desk in case an attachment was un-intentionally blocked and also to notify senders of possible virus infection.

I also used the "Send E-mail to" feature during debugging, but disabled this after the configuration was tested and stabilized.

3.1.12 Miscellaneous

This is where Michael Bell chose to place features and options that don't seem to fit anywhere else. There are some rarely used options here. There is also Logging, Event Logging, and SNMP support (Bell, *User Manual* 64).

I enabled preserve settings on exit to keep the statistics on the main Guinevere screen when exiting the program. "Otherwise, they are zeroed out" (Bell, *User Manual* 66). This was more of an issue with earlier versions of Guinevere, as there was no built in logging or reporting. However, newer versions provide very detailed logging and built-in (manual) reporting.

I still kept this enabled because it's nice to see the at-a-glance statistics on the main Guinevere screen.

I enabled logging to disk and set the log file size limit to 8192 KB (8 MB), set it to store logs for 30 days, and set it to allow for up to 5 log files per day.

I also enabled event logging, which stores important events in comma-delimited format. These files are the basis of the built-in reports and can easily be parsed to create custom reports.

Finally, I configured Guinevere to decompress all possible types of archive files. The default is to process only ZIP files (Bell, *User Manual* 67).

Processing all types is more processor intensive, but after monitoring I determined this not to cause a significant impact on the overall processing speed of the system. I set it to decompress ZIP, RAR, CAB, GZIP, and TAR files, as well as self-extracting flavors of all of these.

3.1.13 Advanced Tuning

This feature was not necessary to meet any of our stated requirements and is thus not enabled.

4.0 Assessment of Effectiveness

Overall I am very pleased with the effectiveness of the Guinevere solution and I rate the project as successful. It has nearly eliminated calls to our Help Desk from users who "accidentally" opened a virus-laden e-mail and infected themselves. It is also effectively blocking upwards of 90% of the Spam destined for our domain, and with very few false positives. The following three-month statistics snapshot shows that Guinevere stopped almost 67,000 unwanted messages from clogging our users' inboxes. That's nearly 38% of all our inbound e-mail. It also stripped out almost 5,000 potentially malicious file attachments and blocked a handful of oversize messages.

Table 1: Guinevere Statistics 05/01/2003 – 07/31/2002

E-Mail Total	E-Mail Sent	E-Mail Received			
257,959	80,451	177,508			
Viruses Blocked	**SPAM Blocked**	**(Deleted) Blocked by Filter**	**Attachments Blocked (extensions)**	**Attachments Blocked (oversize)**	**% SPAM**
4,274	40,958	25,980	4,987	6	37.71%

I also discovered a Perl script on the Internet that parsed the Guinevere log files and created dynamic web pages showing the number of times each virus was caught. I believe it originated at Texas A&M University. The design of this script required modifying one of the Guinevere batch files to log additional information about the viruses, as they were found. This would work going forward, but I wanted to pull statistics from the time we began using Guinevere. After some digging, I found the Symantec Anti-virus was doing the logging for us and its log file was in simple ASCII text format. I would like to thank Niles Mills, a veteran developer and security professional, who wrote me a Perl script to pull the data directly from these logs, and voila we now have all the virus statistics since the inception of this project. The virus names are hyperlinked to information about the virus on Symantec's web site. The following table shows the breakdown of viruses eradicated during the sample period.

Table 2: Viruses Caught by Guinevere during Sample Period

May

Virus Name*	Times Caught
W32.Klez.H@mm	1306
W32.Klez.gen@mm	4
W32.Magistr.39921@mm	2
W32.Sobig.A@mm	2
W32.Sobig.A@mm.enc	2
W32.Sobig.B@mm	1
W32.Yaha.F@mm	2
W32.Yaha.F@mm.enc	2

June

Virus Name*	Times Caught
W32.Klez.H@mm	1353
W32.Klez.gen@mm	1
W32.Magistr.39921@mm	2
W32.Sobig.A@mm	2
W32.Sobig.A@mm.enc	4
W32.Sobig.C@mm	3
W32.Sobig.E@mm	8
W32.Yaha.F@mm	2
W32.Yaha.F@mm.enc	10

July

Virus Name*	Times Caught
W32.Klez.H@mm	1538
W32.Klez.gen@mm	10
W32.Sobig.A@mm	4
W32.Sobig.A@mm.enc	5
W32.Sobig.D@mm	1
W32.Sobig.E@mm	10

Following is the Perl code used to parse the Symantec Anti-virus log files.

4.1 Perl Code Used to Parse the Symantec Anti-virus Log Files

```
# Usage: perl process.pl

$webdirectory = "c:/temp"; # for debug
$webdirectory = "d:/webrpt";

opendir(DIR, ".") || die "can't open virus log directory";

while ($filename = readdir(DIR))
{
        if ($filename =~ /^.+\.Log$/g)
        {
                # mmddyyyy.log

                $mm   = substr($filename,0,2);
                $dd   = substr($filename,2,2);
                $yyyy = substr($filename,4,4);

                open (LOGFILE,$filename) || die "can not open virus logfile: $filename";
                while (<LOGFILE>)
                {
                        chomp;

                        $fields = @_ = split(",");

                        if ($fields > 6)
                        {
                                $virus_name = $_[6];

                                # Skip if the record is a LiveUpdate or
```

```
                                # virus definition record.

                                if ($virus_name ne "" && $virus_name !~ /^EICAR.*$/)
                                {
                                        $period = "${yyyy}_${mm}";

                                        if (! exists $periods{$period})
                                        {
                                                $periods{$period} = 1;
                                        }

                                        $$period{"$virus_name"}++;
                                }
                        }
                }
                close (LOGFILE)
        }
}

closedir(DIR);

foreach (sort keys %periods)
{
  @yyyy_mm = split("_",$_);

  $yyyy = $yyyy_mm[0];
  $mm   = $yyyy_mm[1];

  $month = (JAN,FEB,MAR,APR,MAY,JUN,JUL,AUG,SEP,OCT,NOV,DEC)[$mm-1];

  $filename = "${month}${yyyy}.TXT";

  open (DATAFILE,">$webdirectory/$filename") || die "can not create
$webdirectory/$filename\n";

  $period = "${yyyy}_${mm}";

  foreach (sort keys %$period)
  {
    print DATAFILE "$_,$$period{$_}\n";
  }

  close (DATAFILE);
}

# End
```

Following is the CGI code used to display the results. Name this file default.cgi and place in the Apache CGI directory.

4.2 CGI Code to Display Virus Count Web Pages

```
#!c:/perl/bin/perl.exe
$| = 1;
  print "Content-type: text/html\n\n";
### Below is code to get the current date and time ###
   ($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) = localtime(time);
@nummonths = ("01","02","03","04","05","06","07","08","09","10","11","12");
@namemonths =
("Jan","Feb","Mar","Apr","May","Jun","Jul","Aug","Sep","Oct","Nov","Dec");
@numyears = ("2001","2002","2003","2004","2005");
if ($hour < 10) { $hour = "0$hour"; }
if ($mday < 10) { $mday = "0$mday"; }
if ($min < 10) { $min = "0$min"; }
$year=$year+1900;
$year_search = $year;
$sdate = "@nummonths[$mon]/$mday/$year";
$stime = "$hour\:$min";
($month_name_given_var, $year_given_var) = split /\&/, $ENV{'QUERY_STRING'};
($month_name_given_name, $month_name_given) = split /\=/,
$month_name_given_var;
($year_given_name, $year_given) = split /\=/, $year_given_var;
 if ($month_name_given eq "")
 {
$month_name = @namemonths[$mon]; # Define the month to search
 }
else
{
$month_name = $month_name_given;
}
 if ($year_given ne "")
 {
$year_search = $year_given; # Define the year to search
 }
$url_base = "http://www.symantec.com/avcenter/venc/data/";
print "<HTML><HEAD><TITLE>Guinevere Statistics for $month_name
$year</TITLE></HEAD>\n";
print "<BODY style=\"font-family: verdana, arial, helvetica, sans-serif;\">\n";
print "<META HTTP-EQUIV=\"pragma\" CONTENT=\"no-cache\">";
print "<META HTTP-EQUIV=\"Refresh\" CONTENT=\"300\">";
print "<table border=0 width=500 cellspacing=0 cellpadding=0><tr><td align=center>\n";
print "<p> \n";
```

```
print "<H2>Guinevere Statistics for $month_name $year_search</H2>\n";
$file = "D:/webrpt/$month_name$year_search.txt"; # File where the results are stored.
if (-e $file) # If the $file already exists...
{
print "<table border=\"0\" bgcolor=\"#ffffff\" cellpadding=\"6\" cellspacing=\"2\">";
print "<TR><TD bgcolor=\"#99cccc\" font color=\"#ffffff\">";
print "<B>Virus Name*</B></TD>";
print "<TD bgcolor=\"#99cccc\"><B>Times Caught</B></TD></TR>";
open (WEBPAGE, "<$file"); # Open the file for reading
while (($line = <WEBPAGE>)) # Read it line by line
{
($virus_name, $virus_count) = split (/\,/, $line);
$url_lc = "\L$virus_name";
print "<TR><TD bgcolor=\"#cccccc\"><a href=\"$url_base$url_lc.html\"
target=new_win>$virus_name</TD><TD
bgcolor=\"#cccccc\">$virus_count</TD></TR>";
}

}
else
{
print "No statistics are available for $month_name $year";
}
print "</TABLE>\n";
print "<form>\n";
print "<p>\n";
print "<select name=\"month_name\">\n";
foreach $month(@namemonths)
{
if ($month eq $month_name)
{
print "<OPTION selected>$month";
}
else
{
print "<OPTION>$month";
}
}
print "</SELECT>";
print "<SELECT NAME=\"year\">\n";
foreach $yearA(@numyears)
{
if ($yearA eq $year_search)
{
print "<OPTION selected>$yearA";
}
```

```
else
{
print "<OPTION>$yearA";
}
}
print "</SELECT>";
print "<input type=submit value=\"View Month **\">\n";
print "</FORM>";
print "<p>* Writeups are not available for all viruses.";
print "<br>You will get a \&amp;quot;Not Found&amp;quot; error when a virus writeup is not
available.";
print "<p>** Statistics available from December 2002 - present.";
print "<br>(updated every 15 minutes)";
print "<p>Check out the <a href=\"topten.htm\">Sophos Virus Top Ten Lists</a>";
print "</td></tr></table>";
print "</BODY></HTML>";
```

I created a batch file to process the virus logs and update the web reports every 15 minutes. While, not quite real-time, it provides us timely enough information to be quite useful. This batch file is run from the Startup group and should be left running at all times to update the web reports.

4.3 Batch File to Update Virus Count Web Pages

```
@echo off
rem d:\webrpt\process.bat
rem Run this from the Startup group and leave running at all times
:loop
cls
echo Updating antivirus web statistics every 15 minutes...
echo !!! DO NOT TERMINATE THIS PROCESS !!!
echo.
c:
cd  "\Documents and Settings\All Users\Application Data\Symantec\Norton AntiVirus
Corporate Edition\7.5\Logs"
rem perl d:\webrpt\process.pl
d:\webrpt\process.exe
rem Sleep for 900 seconds (15 minutes)
sleep 900
rem Then wake up and do it all over again
goto loop
```

I also created an HTML page on our corporate intranet that displays Top Ten Virus Lists from feeds provided by Sophos, another industry leader in anti-virus solutions (Sophos). The Guinevere Statistics (dynamic virus counts) pages and this Top Ten list provide additional tools for our Help Desk to quickly find information on current virus threats.

For information on how to add these feeds to your web site, please visit Sophos at the following URL: http://www.sophos.com/virusinfo/infofeed/.

Table 3 shows a sample of this Top Ten page as modified to fit the scheme of our corporate intranet.

Table 3: Output from the Sophos Top Ten Virus Lists HTML Code

Latest 10 virus alerts	
6 Aug	W32/Lovgate-L
5 Aug	W32/Mimail-A
5 Aug	Troj/Autoroot-A
1 Aug	Bat/Boohoo-A
31 Jul	W32/Gruel-M
31 Jul	W32/Cidu-A
30 Jul	W32/Randon-R
28 Jul	Troj/Mimail-A
28 Jul	W32/BabyBear-A
25 Jul	Troj/QQPass-A
Source: Sophos Anti-Virus	
Add this info to your website	

Top 10 viruses in July 2003	
1	W32/Sobig-E
2	W32/Bugbear-B
3	W32/Klez-H
4	W32/Sobig-A
5=	W32/Parite-B
5=	W32/Sobig-B
7	W32/Ganda-A
8=	W32/Opaserv-G
8=	W32/Sobig-D
8=	W95/Dupator
Source: Sophos Anti-Virus	
Add this info to your website	

Top 10 virus hoaxes	
1	Bill Gates fortune
2	Hotmail hoax
3	JDBGMGR
4	Meninas da Playboy
5	WTC Survivor
6	Bonsai kitten
7	Budweiser frogs screensaver
8	A virtual card for you
9	Frog in a blender/Fish in a bowl
10	Irina
Source: Sophos Anti-Virus	
Add this info to your website	

5.0 Conclusion and Final Thoughts

This project yielded immediate positive results by nearly eliminating inbound e-mail viruses and by eradicating nearly 90% of our Spam. I am pleased to have had the opportunity to work on this project and I hope that by sharing my “lessons learned” others will benefit from this knowledge.

A dynamic system like this will continue to evolve over time. I will continue tuning it to increase our ability to weed out the unwanted chaff, while minimizing false positives.

The following lists a few additional short-term tasks that should increase the overall effectiveness and usability of the system.

- Upgrade SpamAssassin and implement Bayesian Spam analysis
- Research Guinterface, a web-based front end enabling you to administer Guinevere blocked messages and GroupWise undeliverable messages

- Write Perl scripts to parse Guinevere statistics log files and produce dynamic web reports (Guievere already has built in reporting, but these must be run manually)

In closing, I would like to thank the SANS Institute and all its contributing members for the tremendously beneficial services and the wealth of information provided to the public.

Works Cited and Additional References

ActiveState. “ActivePerl Download.” 5.6.1 build 635. Aug. 21, 2003 <http://www.activestate.com/Products/Download/Download.plex?id=ActivePerl>.

Apache. “Apache HTTP Server Project.” Aug. 21, 2003 <http://httpd.apache.org/download.cgi>.

AT&T Laboratories. “Making VNC more secure using SSH.” 1999. Aug. 21, 2003 <http://www.uk.research.att.com/vnc/sshvnc.html>.

Beginfinite, Inc. “GWAVA.” Home Page. Aug. 21, 2003 <http://www.beginfinite.com/html/products.html>.

Bell, Michael. “Guinevere FAQ.” July 11, 2002. Aug. 21, 2003 <http://www.openhandhome.com/guinevere/faq.htm>.

---. “Guinevere 2.0 Features List.” Aug. 21, 2003 <http://www.openhandhome.com/guinevere/precis.htm>.

---. “Guinevere 2.0.11 User Manual.” March 2003: 30, 32, 35, 36, 41, 51, 56, 58, 61, 64, 66, 67, 89. Aug. 21, 2003 <http://206.187.17.75/g2/userman2.exe>.

---. “Using SpamAssassin with Win32.” Feb. 5, 2003. Aug. 21, 2003 <http://www.openhandhome.com/howtosa.html>.

---. “Guinevere Announcements Discussion List.” Aug. 21, 2003 <http://groups.yahoo.com/group/guinevere-announce>.

Caplan Grey, Maurene. “Commentary: Price of Spam too high for struggling ISPs.” Nov. 8, 2000. Aug. 21, 2003 <http://news.com.com/2009-1023-248303.html>.

Carnegie Melon University, CERT® Coordination Center. “CERT® Incident Note IN-2003-02.” Aug. 4, 2003. Aug. 21, 2003 <http://www.cert.org/incident_notes/IN-2003-02.html>.

Checkmark System Information. “About.” Aug. 21, 2003 <http://www.check-mark.com/checkmark/aboutcm.html>.

---. “Anti-virus Checkmark Level One.” June 2002. Aug. 21, 2003 <http://www.check-mark.com/checkmark/ph_symantec.html>.

---. “Anti-virus Checkmark Level Two.” March 2002. Aug. 21, 2003 <http://www.check-mark.com/checkmark/ph_av2_symantec.html>.

Clearswift. “CS MailSweeper™ for SMTP: Anti-spam Edition.” Aug. 21, 2003 <http://www.mimesweeper.com/products/antiSpam/Msw/default.asp>.

Guinterface Software. “About.” Aug. 21, 2003 <http://www.guinterface.com/guinterface2_about.htm>.

Hoax Busters. “The Big List of Internet Hoaxes.” Aug. 21, 2003 <http://www.hoaxbusters.org>.

ICSA Labs. “Certified Products: Anti-virus Scanner.” Dec. 16, 2002. Aug. 21, 2003 <http://www.icsalabs.com/html/communities/antivirus/certification/certprod.shtml>.

Mayer, Matt. “Guinevere Filters.ini.” May 2, 2003. Aug. 21, 2003 <http://groups.yahoo.com/group/guinevere-discuss/message/3244>.

netiQ. “MailMarshall.” Home Page. Aug. 21, 2003 <http://www.marshallsoftware.com>.

Network Associates. “McAfee System Protection VirusScan® Enterprise.” Aug. 21, 2003 <http://www.nai.com/us/products/mcafee/antivirus/email/vs.htm>.

Novell. “GroupWise 5.5 Documentation.” Aug. 21, 2003 <http://www.novell.com/documentation/lg/gw55/index.html>.

---. “Novell Technical Information Document # 10024073.” GroupWise And Viruses, possible solutions. Feb. 7, 2003. Aug. 21, 2003 <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10024073.htm>.

---. “Novell Technical Information Document # 10007320.” How to configure GWIA to allow a third-party virus scanner to scan Internet messages. Feb. 17, 2003. Aug. 21, 2003 <http://support.novell.com/cgi-bin/search/searchtid.cgi?/10007320.htm>.

SANS Institute. “SANS Security Essentials II: Network Security Overview.” 2003: 1-2.

Sophos. “Virus and Hoax Information Feeds.” Aug. 21, 2003. <http://www.sophos.com/virusinfo/infofeed>.

SpamAssassin. “Welcome to SpamAssassin™.” Aug. 21, 2003 <http://useast.spamassassin.org/doc.html>.

Symantec. “Symantec AntiVirus™ Corporate Edition.” Aug. 21, 2003 <http://enterprisesecurity.symantec.com/Content/ProductLink.cfm>. Path: Symantec AntiVirus Corporate Edition.

---. “Security Response.” Aug. 21, 2003 <http://securityresponse.symantec.com>.

The WildList Organization International. “WildList FAQ.” Aug. 21, 2003 <http://www.wildlist.org/faq.htm>.

TightVNC. “Download TightVNC.” Aug. 21, 2003 <http://www.tightvnc.org/download.html>.

Virus Bulletin. “VB 100% Award for Symantec Anti-virus Products.” Aug. 21, 2003 <http://www.virusbtn.com/vb100/archives/products.xml?symantec.xml>.

Yahoo! Groups: Guinevere-Discuss. “Guinevere General Discussion List.” Aug. 21, 2003 <http://groups.yahoo.com/group/guinevere-discuss>.

Last Updated: November 18th, 2017

Upcoming Training

SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive
SANS Cyber Defense Initiative 2017	Washington, DC	Dec 12, 2017 - Dec 19, 2017	Live Event
SANS Cyber Defense Initiative 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Dec 14, 2017 - Dec 19, 2017	vLive
Community SANS Orlando SEC401	Orlando, FL	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Nashville SEC401	Nashville, TN	Jan 08, 2018 - Jan 13, 2018	Community SANS
Community SANS Honolulu SEC401	Honolulu, HI	Jan 08, 2018 - Jan 13, 2018	Community SANS
SANS Security East 2018	New Orleans, LA	Jan 08, 2018 - Jan 13, 2018	Live Event
Mentor Session - SEC401	Memphis, TN	Jan 09, 2018 - Mar 13, 2018	Mentor
SANS Amsterdam January 2018	Amsterdam, Netherlands	Jan 15, 2018 - Jan 20, 2018	Live Event
Northern VA Winter - Reston 2018	Reston, VA	Jan 15, 2018 - Jan 20, 2018	Live Event
Mentor Session - SEC401	Minneapolis, MN	Jan 16, 2018 - Feb 27, 2018	Mentor
SANS Las Vegas 2018	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	Live Event
Las Vegas 2018 - SEC401: Security Essentials Bootcamp Style	Las Vegas, NV	Jan 28, 2018 - Feb 02, 2018	vLive
Community SANS Chantilly SEC401	Chantilly, VA	Jan 29, 2018 - Feb 03, 2018	Community SANS
SANS Miami 2018	Miami, FL	Jan 29, 2018 - Feb 03, 2018	Live Event
SANS Scottsdale 2018	Scottsdale, AZ	Feb 05, 2018 - Feb 10, 2018	Live Event
Community SANS Madison SEC401	Madison, WI	Feb 05, 2018 - Feb 10, 2018	Community SANS
SANS London February 2018	London, United Kingdom	Feb 05, 2018 - Feb 10, 2018	Live Event
Southern California- Anaheim 2018 - SEC401: Security Essentials Bootcamp Style	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	vLive
SANS Southern California- Anaheim 2018	Anaheim, CA	Feb 12, 2018 - Feb 17, 2018	Live Event
Community SANS Columbia SEC401	Columbia, MD	Feb 12, 2018 - Feb 17, 2018	Community SANS
SANS Dallas 2018	Dallas, TX	Feb 19, 2018 - Feb 24, 2018	Live Event
SANS Secure Japan 2018	Tokyo, Japan	Feb 19, 2018 - Mar 03, 2018	Live Event
SANS New York City Winter 2018	New York, NY	Feb 26, 2018 - Mar 03, 2018	Live Event