

DRAFT

LAYERED VIRUS PROTECTION FOR THE OPERATIONS AND ADMINISTRATIVE MESSAGING SYSTEM

Roger H. Cortez
Jet Propulsion laboratory
4800 Oak Grove Drive M/S 230-305
Pasadena, CA 91109

ABSTRACT

NASA's Deep Space Network (DSN) is critical in supporting the wide variety of operating and planned unmanned flight projects. For day-to-day operations it relies on email communication between the three Deep Space Communication Complexes (Canberra, Goldstone, Madrid) and NASA's Jet Propulsion Laboratory. The Operations & Administrative Messaging system, based on the Microsoft Windows NT and Exchange platform, provides the infrastructure that is required for reliable, mission-critical messaging. The reliability of this system, however, is threatened by the proliferation of email viruses that continue to spread at alarming rates. A layered approach to email security has been implemented across the DSN to protect against this threat.

EXECUTIVE SUMMARY

Computer viruses spread quickly and often contain a damage routine. They can destroy files, format hard drives, downgrade performance of a computer, or cause other damage. This results in increased labor costs and lost productivity, as DSN users would have to rely on other forms of communication such as voice lines and fax machines. These viruses use electronic mail as their major transport mechanism, and take advantage of social engineering techniques to manipulate end users into opening infected messages or attachments. Anti-virus software on the desktop lowers this risk, but a single layer of virus defense is no longer sufficient as their virus definitions are not always up to date, and they do not protect against unknown viruses.

A multi-layer approach to email security has been implemented to protect users from viruses originating within the DSN (intersite communication) or externally from the Internet. In addition to virus protection on the desktop, the Exchange mail server employs its own virus protection that automatically detects and removes viruses from both intersite and external mail. All intersite mail is therefore subject to two layers of security – virus protection at the desktop and virus protection at the mail server. Internet mail, which uses the Simple Mail Transport Protocol (SMTP), benefits from an additional layer of security. This third layer of security is critical as Internet mail is the primary transport mechanism of a virus into the DSN. An SMTP virus protection gateway has been deployed at each site to perform virus checking and filtering. Mail originating from the Internet is not only checked for existing viruses, but is also stripped of any attachments that can be executed. This added protection ensures that new viruses undetected by virus protection software will be stopped at the gateway.

The layered approach to virus protection significantly reduces the overall risk of a virus infection. Viruses are now being stopped both at the SMTP gateway and the Exchange server, before it can reach the end user. In addition, all Internet mail is stripped of any dangerous attachments, nearly eliminating the risk of infection from new, unknown viruses. The steps taken to protect the Operations and Administrative Messaging system from viruses has been a success in minimizing both virus infections and their inherent nature to spread, which reduces the risk to spacecraft operations.

1.0 BACKGROUND

The primary purpose of the Operations & Administrative Messaging (OAM) system is to send messages that support DSN operations across the Deep Space Network. These messages include operation directives, advisory messages, schedules, incident reports, and configuration change notices. The growth of email as a communication tool has resulted in the use of the OAM system not only for operations, but also for administrative purposes such as daily communication between users. DSN users not only receive email from other OAM sites, but also from individuals residing out on the Internet. It is imperative that the OAM and its users are protected from the threat of worms and viruses that originate on the Internet.

2.0 MESSAGING SYSTEM ARCHITECTURE

The OAM system consists of five mail servers geographically distributed across the Deep Space Network and the Jet Propulsion Laboratory. Mail messages between these servers are transferred via the Exchange site connector using Remote Procedure Calls (RPC), a session-layer application program interface that runs over TCP/IP.

Messages outside the OAM, however, are sent and received via the Internet Mail Service (IMS) connector. IMS is a Windows NT service that allows the Exchange Server to act as an SMTP host. Therefore, all mail destined for or originating outside the OAM organization uses the Simple Mail Transfer Protocol.

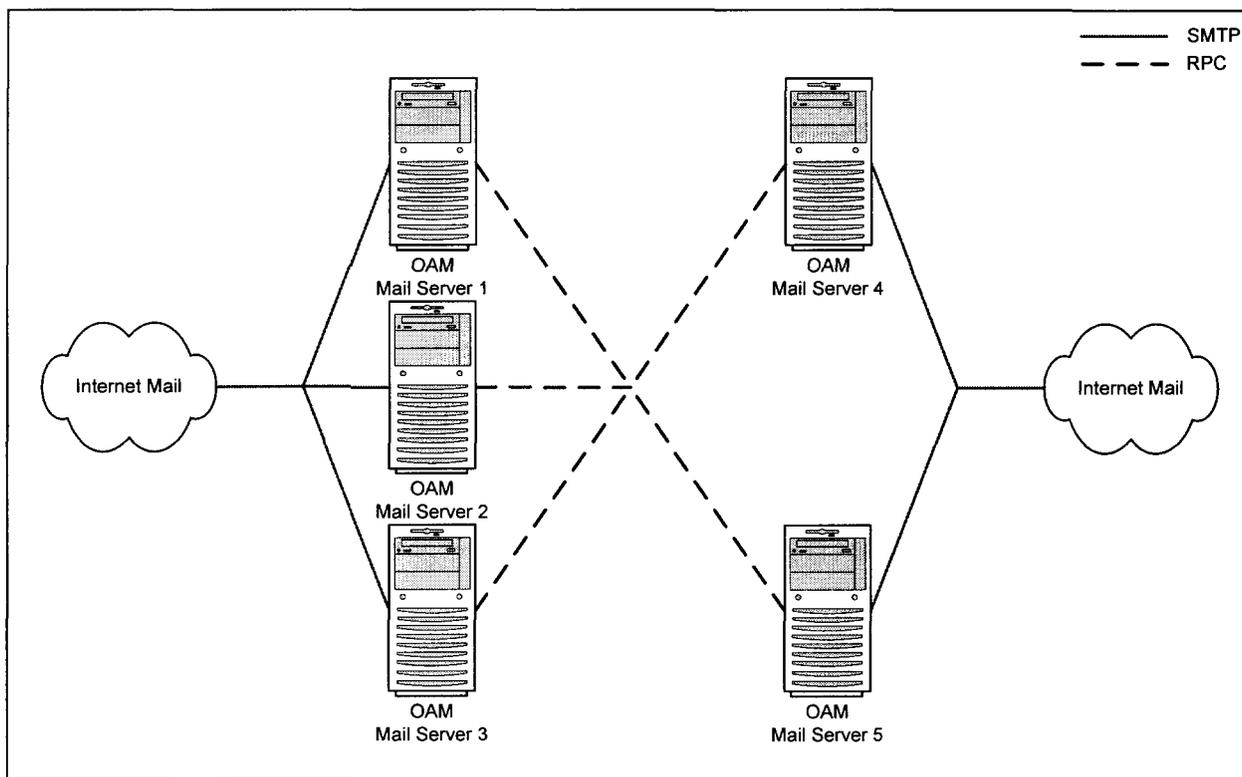


Figure 1 - Messaging System Architecture

The use of different messaging protocols is a key factor in choosing and implementing an anti-virus solution. Mail gateway anti-virus solutions generally support the industry standard SMTP protocol, but not the Exchange site connector and its use of RPC.

3.0 ANTI-VIRUS SYSTEM ARCHITECTURE

Virus protection on the OAM system consists of multiple layers that have been put into place over several years. This layered approach to combating worms and viruses was not implemented all at once, but became what it is today due to the proliferation and increased sophistication of malicious code. The OAM system offers three layers of protection against the threat of worms and viruses (in order of implementation):

1. Virus protection at the desktop
2. Virus protection at the mail server
3. Virus protection at the SMTP gateway

Due to the nature that the OAM processes intersite mail (OAM to OAM server) and Internet mail differently, not all mail messages are exposed to the three layers of protection. Mail messages transferred between OAM servers use RPC for communication and are therefore not exposed to the SMTP gateway for virus checking. The lack of a third layer for mail messages between OAM users is not critical since the majority of virus-infected messages received come from the Internet. All mail outside the OAM organization does use the SMTP protocol and is therefore exposed to all three layers of protection.

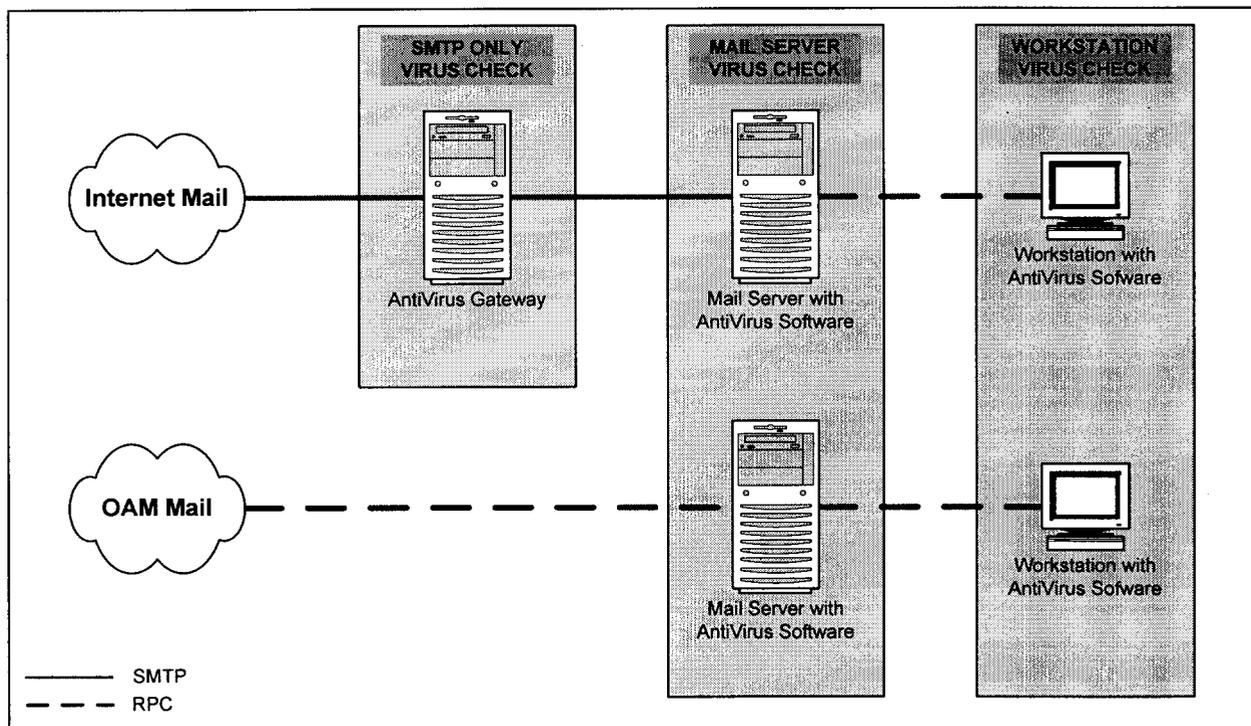


Figure 2 - Anti-Virus System Architecture

It is important to note that there is no correct way to define the first layer of protection versus the last, as it is dependent on the origin of a virus. For example, anti-virus software on the desktop would be the first level of protection against a virus originating at the user workstation due to the use of an infected floppy disk. If the anti-virus software at the desktop fails then the SMPT anti-virus gateway (if destined for the Internet) or the anti-virus software on the mail server (if destined for another OAM user) would become the last line of defense. Infected mail messages, on the other hand, would face the SMPT gateway or mail server first, with the user workstation remaining as the last level of defense.

3.1 VIRUS PROTECTION AT THE DESKTOP

Virus protection at the desktop consists of a commercial anti-virus product configured for file system real-time protection. The anti-virus client scans all files for viruses when they are accessed or modified to ensure the continued integrity of the system. Additionally, all clients are configured to perform weekly scans of the entire system.

Virus protection at the desktop, however, has several drawbacks. All have been observed on user workstations.

1. Software may be removed from the system
2. Software may be disabled or enabled “only when needed”
3. Virus definitions are not kept up to date
4. Lack of protection for recently discovered viruses

These observations signify the importance of not relying solely on desktop protection as users can easily modify the software and its settings, removing a critical layer of defense against worms and viruses. It has been found that users who remove or disable the software do so for performance reasons. This is generally attributed to weekly scans scheduled during regular working hours, which result in performance degradation while users attempt to perform their work. Most of the problems associated with virus definitions not kept up to date have resulted from a misconfigured client that does not update its definitions automatically.

The fourth problem observed is the lack of protection against recently discovered viruses. This is an inherent problem of anti-virus software as there will always be a window of time between virus discovery and the release of new virus definitions. Protection against this threat has not been implemented at the desktop level, but instead at the SMTP gateway.

To reduce user intervention with client software and improve desktop protection, managed anti-virus clients are being deployed across the DSN. Managed clients maintain communication between themselves and a central server to ensure the following:

- Client software cannot be removed or disabled without a password
- Virus definitions are kept up to date by pushing them to the client

The use of managed clients has significantly improved virus protection at the desktop level. The following table indicates the improvement seen at two DSN sites after implementation (based on a random audit of 20% of the computer systems):

	AV Software Installed & Operational (2001)	AV Software Installed & Operational (2002)	AV Software Virus Pattern Files Up-to-Date (2001)	AV Software Virus Pattern Files Up-to-Date (2002)
DSN SITE 1	98.3 %	100 %	91.7 %	100%
DSN SITE 2	79.2 %	100 %	33.3 %	82.3 %

3.2 VIRUS PROTECTION AT THE MAIL SERVER

A desktop only solution to the virus problem is no longer sufficient, as users can modify the software or its settings. There is also no guarantee that a new machine on the network will have anti-virus software installed and operational. One solution to combat these problems is to place anti-virus software on the mail server where infected messages can be intercepted before reaching the end user.

This solution has been implemented on the OAM system. A commercial anti-virus product, compatible with the Microsoft Exchange platform, was installed on all mail servers to add a second layer of protection against the growing threat of worms and viruses. The number of virus infections attributed to email was significantly reduced after implementation, but virus incidents did not stop. This was a result of the following:

- Anti-Virus patterns can only be updated automatically 10 times per month
- Manual updates must be forced by the Administrator outside the 10 times/month schedule
- Lack of protection for recently discovered viruses.

Once again, the lack of protection for recently discovered viruses is inherent of anti-virus software. The window between virus discovery and release of definitions will always exist – giving viruses and worms a window of opportunity to reach the unprotected user, resulting in infection and replication. Adding to this window is a second window of opportunity for possible infection – the time between the release of virus definitions and the manual update an Administrator has to perform. This second window of opportunity can be many hours depending on the time of release and the geographical location of the server.

One pattern across most virus incidents was that the infected mail message always originated from an outside user on the Internet. This led to the idea that in order to truly protect the OAM, messages from outside the OAM organization had to be targeted.

3.3 VIRUS PROTECTION AT THE SMTP GATEWAY

The need for virus protection at the SMTP gateway resulted from the following observations:

1. Nearly all virus-infected messages originate from the Internet
2. Virus definitions must be automatically updated within minutes of their release
3. Protection was needed against recently discovered viruses.

An enterprise-level email control product was deployed at the SMTP gateway as a solution to these problems. This product has been deployed across the DSN and is used to:

- Run a virus scanning product and update virus patterns within minutes of their release
- Block executable and dangerous attachments
- Block known worms and known virus attachments

At a minimum, all incoming and outgoing Internet mail is scanned at the SMTP gateway for viruses, executable files, dangerous attachments, known worms, and known virus attachments. Virus pattern files are updated within minutes of their release eliminating the second window of opportunity – the time it takes between the release of new virus patterns and their deployment.

DRAFT

More importantly, a solution was found for the problem of unknown or recently discovered viruses. A new mail policy was put into place eliminating the receipt of all executable files and dangerous attachments (e.g. screensavers) from the Internet. Rules have been added at the SMTP gateway to enforce this policy, resulting in zero virus infections since implementation. If virus-infected messages reach the SMTP gateway before its pattern files have been updated, the dangerous attachment or executable rule will block these messages from reaching the mail server and ultimately the end user.

4.0 CASE STUDY: FRETHEM WORM

The W32/Frethem worm and its variants is an Internet worm which uses its own STMP engine to spread. It attaches an executable file to all messages and attempts to use both IFRAME (a sub-window of the main browser window) and MIME (Multipurpose Internet Mail Extensions) exploits on systems that have not been patched, forcing the execution of the attached file when the user simply reads or previews the message. These vulnerabilities affect the Internet Explorer (IE) web browser but also have an effect on the Microsoft Outlook email client as it uses IE to render HTML messages. The Frethem worm served as a test case for the OAM and its use of the SMTP gateway.

During mid July 2002, all OAM mail servers were under heavy attack by the Frethem worm. One DSN site alone received over 240 infected mail messages. Not a single site reported an infection.

These results are attributed to the implementation of the STMP gateway and its enforcement of several rules. For purposes of this discussion the following rules were implemented at the time and executed in the order shown:

1. Block Virus
2. Block IFRAME Commands
3. Block Executable Files.

To reiterate, an inherent problem with anti-virus software is the window of opportunity between virus discovery and the release of pattern files. This window of opportunity was active during the receipt of infected mail messages. If the virus pattern files would have been updated before the receipt of the first infected message, all messages would have been stopped by the first rule: "*Block Virus*"; this was not the case.

Instead, a number of Frethem infected messages were stopped by the "*Block IFRAME Commands*" rule as it attempted to exploit known Microsoft bugs. Other infected messages not using IFRAME commands were stopped by the "*Block Executable Files*" rule. It was not until the pattern files were released and automatically updated that the "*Block Virus*" rule stopped the messages.

The case of the Frethem worm demonstrates the need for not only virus protection at the gateway, but also the need to protect against unknown worms and viruses. This is being accomplished across the OAM by placing in quarantine all executable and dangerous attachments, as well as implementing additional rules that look for hostile code attempting to exploit known vulnerabilities. Without the SMTP gateway in place, a high number of virus infections would have occurred as neither the anti-virus software running on the mail server nor the client software, would have received updated virus definitions on time.

5.0 CONCLUSION

A single layer approach to virus protection is no longer sufficient as the number of worms and viruses, and their complexity, continues to increase. The OAM system, used for sending operational messages across the Deep Space Network and the Jet Propulsion Laboratory, must be protected from both known and new virus threats. This has been accomplished by implementing three layers of protection:

1. SMTP Gateway that performs a virus check and quarantines all executable and dangerous attachments
2. Anti-Virus software on the mail server
3. Anti-Virus software on each workstation

The implementation of the last component, the SMTP gateway, took place nearly five months ago and not a single virus infection has been reported since. This can be attributed to a layered approach to virus protection and a new policy that restricts the receipt of executable and dangerous attachments. The latter has resulted in the protection against new and recently discovered viruses – maintaining the OAM system and its users virus free.

ACKNOWLEDGEMENT

I would like to thank all members of the Deep Space Network OAM Administrator team for implementing the many stages of this project. Special thanks to Ross Murray from the Canberra Deep Space Communication Complex for the original design of the SMTP gateway and for pilot testing many of our solutions along the way.