Bits & Bytes

No. 175 RZG Computer Bulletin October 2003

Computer Center of the Max Planck Society and the Institute for Plasma Physics*

IBM p690 Supercomputer

In July, the IBM Regatta system "psi" was upgraded to the latest level of compilers (xlf 8.1.1) and operating system (AIX 5.1-04).

There is now a migrating GPFS file system /r available that will automatically migrate files to tape when the file system gets filled up. As soon as the user accesses the files again, they will be automatically retrieved from tape. Currently, this file system is under testing. General availability is scheduled for October 03.

The installation of the new "Federation" switch as a fast interconnect between the "Regatta" nodes is in progress, a two node system has been in test operation since early September. A larger 16 node system will be set up in October/November. Later on in December, all nodes will be connected to the new switch.

Ingeborg Weidl

Notes on virus attacks

The latest virus attacks (Blaster, Sobig, Bugbear, ...) to Windows-based PCs changed the role of the central PC-Service to a disinfecting group, leaving no more time for improvements (testing software and hardware, deploying new concepts). Therefore it is mandatory to give you some hints how to deal with these nasty beasts to reduce the risk of getting infected.

In order to establish effective policies, it is important to know the common virus entry points:

Internet access
As IPP is permanently connected to the Internet theoretically any application (based on so-called ports) can attack any host inside our intranet. Two well-known applications are email and WWW:
Email An overwhelmingly large proportion of infections today are caused by infected email attachments. The ease with which a user can click on an attachment and launch an application is a significant factor in the spread of email-borne viruses. If the email content is sufficiently inviting (e.g. "kindly check the attached LOVELETTER coming from me") and the visible attachment extension sufficiently innocent in the eyes of the user (e.g. "LOVE-LETTER-FOR-YOU.TXT.vbs – text files cannot carry an infection, can they?"), the temptation for a user can become overwhelming. The danger of infection through attachments is, of course, not confined to email. Newsgroup postings are also capable of carrying attachments.
World Wide Web The web is full of sites carrying virus-infected material. Desktop access to the Internet is viewed as an "expected" in today's workplace, meaning that downloading potentially infected files is too easy.

Floppy disks and CDs
The use of floppy disks has decreased radically with the advent of networks, but all IPP-PCs still come with a floppy drive. 0.5 % of all infections are due to boot sector viruses, which shows that floppy disks are not dead (yet). CDs (especially magazine cover CDs) have also been shown to be relatively frequent virus carriers.

How to deal with these threats?

First of all, it should be stressed that 100 percent security means zero percent functionality. Therefore the aim is to minimize the threats by applying actions (central and desktop based) and enhance the sensitiveness for risks (user based). This, of course, cannot be a one-stage process, but needs the cooperation of users and IT-professionals.
Central actions (RZG-based)
Two actions are already in place for some time: First, our common Internet-gateway acts also as packet filter firewall protecting the IPP intranet from risky and unused applications. Second, any email addressed to a user inside our network is checked against viruses, and – if infected – quarantined.
Mandatory user actions:

- Any network-attached PC needs anti-virus software to detect, report and disinfect viruses. Keep this software up-to-date with the latest virus identities.
- It is strongly recommended that you apply the patches that Microsoft makes available for its suite of operating systems to fix known vulnerabilities exploited by viruses.

However, without automating these desktop actions, we will not have success: Therefore "Lager-PCs" are installed with a preconfigured version of Sophos Anti-Virus, which meets all the points above: it detects and reports viruses; updates with virus identities will be done every three hours. With the new Windows XP the Software Update Service (SUS) can be adopted, which

*Max-Planck-Institut für Plasmaphysik, Boltzmannstraße 2, D-85748 Garching bei München, tel.: +49(89) 3299-01, e-mail: benutzerberatung@rzg.mpg.de, URL: http://www.rzg.mpg.de/
Editorial: Dr. Roman Hatzky, Tel. -1707

automatically applies all the relevant patches for security leaks of the operating system. Normally, this service contacts a Microsoft-Server in the Internet to download the patches. As this is for several reasons not accepted, the SUS for a "Lager-PC" is configured to contact instead a server located at the GWDG (Gesellschaft für wissenschaftliche Datenverarbeitung), which is member of the MPG.

What about notebooks?

For notebooks the situation is slightly different: They are not permanently attached to our network, but for traveling users temporarily hooked up to hot spots at airports or hotels or other perhaps unsecured parts of the Internet. In this way they are subject of great interest for viruses. Should a virus manage to penetrate all the defenses put in its path, the notebook will be reattached to the IPP network and is now a potential risk of infecting other PCs (as was the case for the Blaster virus a few weeks ago). With this in mind, all the notebooks should be the PCs with the highest level of security.

Mandatory user actions:

- Be always aware of the risk getting infected by a virus (see the entry points above).
- Check your PC if an actual version of Sophos is installed and properly configured.
- If running Windows XP, activate SUS.
- If not running XP, check your PC if an upgrade to the latest version of Microsoft Windows is possible.

For checking and upgrading, and if you have any questions, please contact your local IT-representative or the PC-Service (ext. 1872).

Anton Hackl

Active Directory

One of the most significant new components of the Microsoft operating system is a new directory service, called Active Directory. A directory service stores information about all network resources and makes that information available to administrators, users and applications. Using Active Directory, administrators manage a directory service with only one management interface for many directory service tasks.

Active Directory builds on the familiar architecture of the Windows NT operating system with the addition of primary network services such as "DNS" and "LDAP" to access Active Directory features. By implementing Active Directory we take advantage of advanced security features, such as support for Kerberos, smart cards, public key infrastructure (PKI), and x.509 certificates.

Active Directory uses logical components – domains, organizational units (OU), domain trees, and domain forests – and physical components – sites and domain controllers – to build a directory structure that meets the needs of our organization. For example, the domain administrator defines several OUs and delegates the administrational control of them to sub-administrators. The resources stored in the directory, such as user data, printers, servers, databases, groups, computers, organizational units, domains, and security policies, are known as objects.

A computer that stores a replica of the domain directory (Active Directory) is running Windows Server 2000 or Windows Server 2003, and is called domain controller (DC). It manages all aspects of user domain interaction, such as locating Active Directory objects and validating user logon attempts. Because a domain can contain one or more domain controllers, all domain controllers in a domain have a complete replica of the domain. DCs in a domain automatically replicate all objects and changes to each other. Having more than one domain controller in a domain provides fault tolerance. If one DC is offline, another DC can provide all required functions. DCs can be placed in different sites. Where a site is a set of subnets, that allows administrators to easily configure the Active Directory access and replication topology to take advantage of the physical network.

All objects in the Active Directory are protected by Access Control Lists (ACLs). ACLs determine who can see the object, which type of attributes each user can see, and what actions each user can perform on the object. Administrators also use Group Policy (GP) to manage desktop configurations for groups of computers and users. Group policies are collections of user and computer configuration settings that can be linked to computers, sites, domains, and OUs. For example, using GP's the administrator can determine the programs that are available to users, the programs that appear on the user's desktop, and "Start" menu options.

At this time the administrators of the IPP domain are planning and implementing the Active Directory as the default directory service.

Vitalijus Bludov

Mozilla as substitute for Netscape

Since Netscape has discontinued its support for a lot of operating systems, RZG decided to offer Mozilla as new supported browser. Mozilla is a fully-featured substitute for Netscape based on original Netscape-sources. It is available on all newer Solaris, AIX and Linux-Platforms. It is in the default PATH, so you can simply call it "mozilla" instead of "netscape". Doing so for the first time should configure your new Mozilla-environment converting your old Netscape setup and copying the files to a new .mozilla subdirectory in your home-directory. RZG will also install Mozilla as the default-browser on the Windows-PCs step by step during upgrades of the Operating-System.

Andreas Schott