OS/390 UNIX Security Overview

Prepared by

IBM Global Services

April 1999

Table of Contents

List of Figures

Preface

Although this document was written with emphasis on security, it contains is a lot of OS/390 UNIX information summarized and presented for a person with MVS (and not UNIX) experience. This document contains information and analogies, mostly summarized from IBM redbooks and product manuals, that a person familiar with MVS can relate to. Some information (e.g. thread level security), although interesting and important, was intentionally left out to keep the document from being too technical in nature.

Several references are made to a "Information Security Controls" document. This document, previously called GSD331, is used to provide a guideline to establish security implementation practices and procedures for the protection of IBM Global Services and the customer. This template document is to be customized for each customer account when applicable.

1.0 Introduction

This document examines, from a security perspective, some of the features available in OS/390 Version 2.6. OS/390 UNIX provides security mechanisms that work with the security capabilities offered by the OS/390 system. In short, OS/390 UNIX provides the traditional UNIX security mechanisms and also eliminates some "security holes" contained in other UNIX systems. As such, some of the classic hacker attacks on traditional UNIX do not work on OS/390 UNIX. For example, hackers will often seek to obtain the /etc/passwd file and attempt to crack the passwords. Since OS/390 UNIX relies on RACF for authentication, it does not have an /etc/password file and is therefore immune from that attack.

2.0 A Few Words About OS/390 UNIX

This part of this document is intended to establish a baseline of information about OS/390 UNIX and make some comparisons with traditional MVS concepts.

2.1 Compatibility With Other UNIX Systems

UNIX capabilities have become an integral part of OS/390. Over time, the following names have been used to describe UNIX capability on IBM mainframes.

- Open Edition MVS
- OS/390 with OpenEdition MVS installed
- OS/390 UNIX System Services
- OS/390 UNIX

X/Open branded OS/390 as a XPG4 UNIX system which means that OS/390 UNIX supports all the C functions and command interfaces in the X/Open Company's Single UNIX Specification also known as the X/Open Portability Guide (XPG) Version 4, Issue 2.

OS/390 UNIX can be thought of as another UNIX platform similar to other well known UNIX platforms (e.g. Solaris, HPUX, AIX) with the performance, reliability, scalability, and security benefits inherent in S/390.

2.2 UNIX Concepts

The following information is provided to establish a baseline of knowledge. The concepts discussed below are often referred to later in the document. In addition to the concepts listed here, a table comparing UNIX, MVS, and OS/390 UNIX is provided in Appendix A.

2.2.1 Kernel

The UNIX kernel is the low-level system code running at the heart of a UNIX system. It sends instructions to the processor, schedules work, and manages I/O. There is only one kernel on a single UNIX system.

2.2.2 Shell

Users normally interact with the shell which is a protective layer built around the kernel. It protects the users from the complexity of the kernel and vice versa. The users make requests to a shell which interprets the requests and passes them on to the kernel.

2.2.3 Daemons

A daemon is process that runs in the background and is not associated with any particular user. Daemons usually run with superuser authority and can issue authorized functions (e.g. change the user identity associated with a process).

2.2.4 Hierarchical File System (HFS)

OS/390 UNIX files are, as in other UNIX systems, organized in a hierarchy that is conceptually similar to the organization of DOS or Windows NT files. By convention, the highest level of the directory structure is called the root directory. Other directories branch off from the root and generally follow a well known naming convention.

MVS views an entire file hierarchy as a collection of HFS data sets – a new kind of data set. Each HFS data set is a mountable file system. The root file system is the first file system mounted and subsequent file systems can be mounted or un-mounted on any directory within the hierarchy. The following rough analogies exist between MVS data sets and the HFS:

Concept	**OS/390**	
	MVS implementation	**UNIX implementation**
High level storage organizer	Catalog	Root directory (/)
User's storage space	MVS data set user prefix (SMITHA.)	User directory (/u/smitha)
Subdivision of user's storage space	Partitioned data set (SMITHA.TEST.C)	User subdirectory (/u/smitha/test)
Low level container of data	Partitioned Data set member SMITHA.TEST.C (PROGRAMA)	File within subdirectory (/u/smitha/test/programA.c)

Within the HFS, file and directory names can be longer than traditional MVS data set names. Like other MVS data sets, HFS data sets can be allocated, backed up, restored, and deleted. Figure 1 illustrate that a directory structure can be contained within an HFS data set.

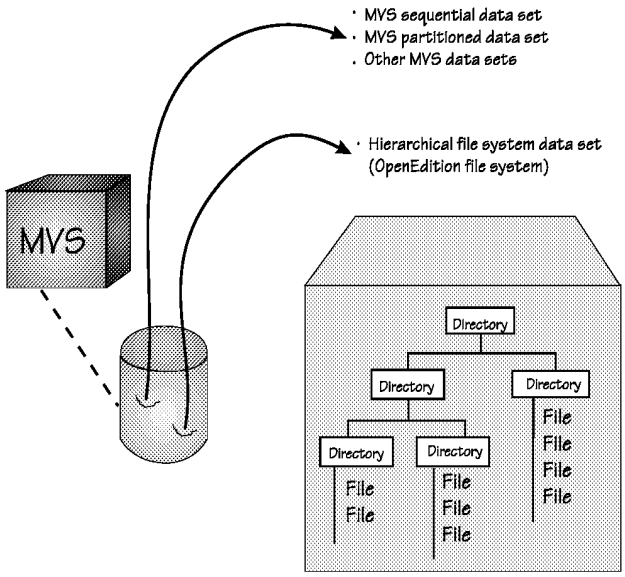


Figure 1 MVS perspective of how OS/390 UNIX files and directories are stored in HFS data sets

2.3 Interoperability Between MVS and OS/390 UNIX

There is a high degree of interoperability between MVS and the OS/390 UNIX:

- Data can be moved or copied between MVS data sets (stored in EBCDIC format) and the HFS (stored in ASCII format).
- TSO/E commands, shell commands, or the panel interface of the ISPF shell can be used to work with the HFS.
- You can write MVS job control language (JCL) that includes UNIX shell commands.
- To edit HFS files, you can use the ISPF/PDF full-screen editor or one of the editors (vi or ed) available in the shell.
- Using OS/390 UNIX extensions to REXX, you can run REXX programs from TSO/E, batch, the shell, or a C program.
- You can run a non-interactive UNIX shell command or shell script from the TSO/E READY prompt and display the output to your terminal.
- The same application program can access both traditional MVS data sets and files in the HFS.

2.4 Selecting and Maintaining a Security Level

In a UNIX system it is common for one person to have full administrative or superuser authority (i.e. UID = 0). In an OS/390 system, it is common for these administrative authorities to be divided among several people. OS/390 UNIX provides the ability to separate some of the authorities commonly granted to a single superuser on a traditional UNIX system.

If the BPX.DAEMON FACILITY class profile is not defined, the system has UNIX-level security. With this security level, both daemon programs and superusers have superuser privileges including the ability to change identity.

If the BPX.DAEMON FACILITY class profile is defined, the system has OS/390 UNIX level security which provides greater control over OS/390 resources that daemons / superusers can access. Specifically, a daemon can change identity only if:

- The daemon's / superuser's identity is permitted to the BPX.DAEMON FACILITY class profile.
- All programs running in the address space have been fetched from a security product controlled library.

Kernel services that change a caller's identity require the target OS/390 user identity to have an OMVS segment defined. Extra control can be obtained by not defining OMVS segments to certain privileged OS/390 users.

Other security mechanisms, similar to the BPX.DAEMON FACILITY class profile, are provided which allow privileged server applications to have fine grained control over the user identity of small pieces of work or threads of execution.

3.0 OS/390 UNIX System Services

3.1 Accessing OS/390 UNIX

OS/390 UNIX system services allows interactive users a choice to use either traditional MVS interfaces or traditional UNIX interfaces:

- Mainframe users can logon through the TSO/E interface using the OMVS command
- Mainframe users can logon through the ISPF panels.
- Users with TCP/IP installed on their workstation can login by using telnet or rlogin commands.

3.2 Users and Groups

3.2.1 Setting-up users

Each user has a user ID (UID) that is set in the RACF OMVS segment. The user's default RACF group needs a group ID (GID) set in it's OMVS segment. Alternatively, a default OMVS segment may be defined for users who need access to a limited set of OS/390 UNIX services. A user needs to have a UID defined or a default set up to obtain OS/390 UNIX services.

3.2.2 Superusers

A superuser is one of the following:

- A user with a UID of 0
- A started procedure with a *trusted* or *privileged* attribute defined in the RACF STARTED class or added to the RACF Started Procedures Table. Although the procedure must have a UID, that UID can be of any value.

Superusers can:

- Pass all security checks to access any file in the HFS file system
- Manage processes
- Change identity from one UID to another
- Increase system limits for a process created by a superuser

However, superuser status is not related to being in a supervisor state, PSW key 0, and using APF-authorized instructions, macros, and callable services.

A traditional UNIX system, grants superuser privileges based on a UID = 0. In addition to this traditional method of defining superusers, OS/390 UNIX also provides a more controlled method of granting superuser privileges via a BPX.SUPERUSER FACILITY class profile to which all users needing superuser privileges may be permitted. This class profile allows non-UID 0 users to become UID 0 users.

Additional control over superusers can be obtained by defining a BPX.DAEMON FACILITY class profile as described previously.

3.3 HFS Files and Directories

3.3.1 Controlling access

Security for files in the HFS is provided through OS/390 System Authorization Facility (SAF) interfaces used by RACF. The system verifies that an OS/390 UNIX user can access a directory, a file, and every directory in the path to the file. Every file and directory has security information which consists of:

- File access permissions
- UID and GID associated with the file
- Audit options

3.3.2 Running Programs Stored in the HFS

The entire HFS is considered to be an unauthorized library. Individual programs within the HFS may be APF-authorized by setting the APF-extended attribute. HFS programs that are APF-authorized behave the same as other programs that are loaded from APF-authorized libraries.

3.4 Auditing Options

Auditing functionality provided by RACF is tightly integrated with OS/390 UNIX. An SMF record can be written at each point where the system makes security decisions. As much or as little auditing as desired can be performed of system and resource accesses. The security auditor uses reports formatted from RACF system management facilities (SMF) records to check successful and failing access to files and kernel resources.

Fine-grain audit control is available for files stored in the HFS. Both the file owner and a security administrator have the ability to separately specify auditing options (successful, failed or all) for read, write, and execute access attempts.

One characteristic of OS/390 Unix services is that whenever you use RACF to control access, you can use RACF to perform logging.

- For example, if you set the auditing (logging) on the BPX.SUPERUSER profile to audit(all(read)), every attempt successful or unsuccessful to use root authority will be logged.
- If you use RACF to control login authority (RACF as the SAF- System Authorization Facility), RACF can audit all logins no matter what service, Unix or TSO or other, the user accesses.

There are some generally accepted auditing guidelines as well as platform specific guidelines that can be met by RACF. The base auditing guidelines for all systems, unless specifically exempted, are:

1. Log all system access attempts (e.g., login).

2. Operating System Resources (OSR) are those data objects which are part of: (1) The system control program and its access control mechanism (2) Subsystems and program products supported by the Provider of Service

- All update attempts to OSR's should be logged, successful or unsuccessful.
- If an OSR needs to have a universal access of NONE, then all READ attempts should be logged.
- If execution of OSR programs would assist the user to bypass systems controls, then execution should be restricted to authorized users. If feasible, the execution attempts should be logged.

4.0 Relevant OS/390 Features

4.1 Security Server

4.1.1 RACF

RACF manages system and data security in OS/390 UNIX by allowing general users to:

- Log on to the system

- Access resources on the system
- Protect their own resources and any group resources to which they have administrative authority

Access control is integrated with the SAF interface to call RACF (or similar security product). File access control information is stored with each individual HFS file. A user is identified by a UID which is kept in the RACF user profile OMVS segment and a GID which is kept in the RACF group profile OMVS segment. RACF program control can be placed on individual files in the HFS.

Digital Certificate Support

RACF will accept digital certificates and associate them with a specific userid. The DIGTCERT general resource class contains the digital certificate and related information. An administrator can use the RACDCERT command to associate a certificate with a RACF user ID thereby enabling user authentication to a webserver (or other SSL enabled application) without providing a RACF password.

Alternatively, an automatic registration web page can be setup allowing users with appropriate privileges to associate a certificate with their RACF user ID. When the user clicks on the registration box, a secure session is set up using SSL and the user's digital certificate. Successful establishment of an SSL session implies that the validity of the user's digital certificate is established. The user's RACF user ID and password is prompted for and passed from the webserver, through OS/390 UNIX, to RACF. RACF verifies the user ID and password and associates the certificate with the user ID that provided it.

A de-registration function is also provided to allow the certificate to be disassociated from a RACF user ID.

4.1.2 LDAP Server

The Lightweight Directory Access Protocol (LDAP) Server is part of the OS/390 Security Server. An LDAP server is a directory server which is similar to a database but the information is generally read more often than it is written. Everyday examples of directories include phonebooks, yellow pages, TV guides and library card catalogs. Computer and network directories such as the LDAP server provide dynamic, flexible, secure and even personalized access to directory entries. Examples of other computer directories are:

- RACF
- Novell NDS
- Windows NT Server as well as Microsoft planned Active directory

LDAP is actually an Internet Engineering Task Force (IETF) standard for accessing directories. The purpose of the standard is to ensure that client programs can store or

retrieve information in an LDAP compliant directory without regard to differences between vendor platforms. IBM's OS/390 LDAP server version 6 is compliant with the IETF LDAPv2 standard.

The real advantage of an LDAP directory server is that it can provide a centralized and common repository for information such as centralized registry of all enterprise users, applications and data.

Enterprise directory strategy and the design and deployment of LDAP directories is beyond the scope of this document but two useful references are listed in the references section of this document.

Some of the advantages of the OS/390 LDAP server are:

- Takes advantage of the performance, reliability and scalability of the OS/390 platform.
- Use of DB2 database to store entries.
- LDAP server 2.7 provides integration with RACF.

The LDAP server normally installs in /usr/lpp/ldap directory. LDAPSRV is normally the userid that runs the LDAP server. LDAP server may run as a started task or under the Unix shell.

Note that LDAP server can provide the ability for the eNetwork Communication server to have a large key size for their certificates.

The protection of the LDAP server is actually in two parts:

- LDAP native security (access lists, etc.)
    - SSL server security
- Protection of the DB2 database

LDAP Security

There are four basic components to secure access of an LDAP server:

- **Administrative access**

The administrator domain name (adminDN) and password (adminPW) is specified in slapd.conf. This user has complete authority to add, delete, and change entries and access control lists (ACL). The administrative user's (adminDN) password should be changed with the same interval as the password for other administrative users. This password is defined in the slapd.conf and changing the password requires LDAP be stopped and restarted.

- **Distinguished Names and User Authentication**

Every entry in the directory has a distinguished name (DN). The DN is the name that uniquely identifies an entry in the directory. A DN is made up of attribute:value pairs, separated by commas. These distinguished name entries can relate to users:

cn=John Smith, ou=downtown, o=Big University, c=US

If a password is defined for the distinguished name, the user may access the directory using simple authentication. LDAP has plug-in modules to support other methods of authentication. LDAP provides for password authentication and for SSL client authentication using certificates.

- **Access Control Lists**

Access control lists provide rich options for controlling access to LDAP entries. Access lists provide a rich set of attributes to control access including **owner, ownerPropagate, inheritOnCreate, acl and aclPropagate.** Users may be put into groups using **group: cn=Anybody** ACL entry. Each of the LDAP access permissions is discrete. One permission does not imply another permission.

- **Secure Sockets Layer (SSL)**

SSL (Secure Sockets Layer) provides the ability to establish an encrypted session between the server and the client. As with any SSL enabled application, proper certificate management, such as password protecting the file containing private keys, is required to ensure security is not compromised.

Properly setting up the security of the LDAP server requires careful planning. The diversity and significance of the LDAP entries can vary greatly. Some entries may be used to define access to general applications or provide generally available information such as telephone numbers, while other entries may define access to the most sensitive applications and data in the enterprise.

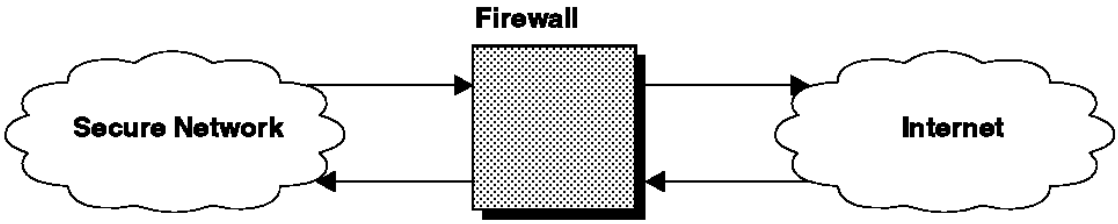
4.1.3 Firewall

OS/390 Firewall Technologies add firewall features to the OS/390 platform. The purpose of a firewall is to prevent unwanted or unauthorized communication into or out of the secure network. The firewall has two jobs:

1. The firewall lets users in your own network use authorized resources from the outside network without compromising your network's data and other resources.
2. The firewall keeps users who are outside your network from coming in to compromise or attack your network.

A firewall is used when communications being passed between an internal trusted or secure network such as a customer’s internal network and an untrusted or insecure network such as the Internet. The diagram below shows a typical configuration:

Figure 2 Typical firewall configuration



OS/390 Firewall Technologies includes functions provided by the OS/390 Security Server as well as functions provided by the eNetwork Communication Server for OS/390.

Functions Included in OS/390 Security Server

1. **Proxy FTP Server** - A proxy server is a secure server that runs on the firewall and performs a specific TCP/IP function as a "proxy" for a network user. A proxy server is, in essence, an application gateway -- a gateway from one network to another for a specific network application. The FTP proxy server intercepts all file transfers and information requests made via the FTP protocol that would cross between your network and the Internet. The user contacts the FTP proxy server using FTP and optionally provides a valid user ID and password. The FTP proxy server then asks the user for the name of the remote host to be accessed. The FTP proxy server makes contact with that remote host as a proxy for the actual user.

2. **Socks Server** - Intercepts all TCP/IP requests, from a socksified client, that cross between your network and the Internet. However, a Socks server provides a remote application program interface so that the functions executed by client programs in secure domains are piped through secure servers at the firewall. As with the proxy server, the Socks server intercepts the request, checks for authorization to come into or go out of the secure network, and either denies the request or pipes it through the firewall.

3. **Logging Server** - Records the activity of the firewall services. As users try to access hosts in your secure network through the various firewall services, the logging server records this activity according to rules that you establish. Logging data can help you to audit the traffic on your firewall and to discern usage patterns and anomalies that may have implications for your network security. (The OS/390 Firewall Technologies logging server is a replacement logger for the UNIX services TCP/IP syslog server.)

4. **Other Servers** - Two other servers, fwlogd and fwtimernat are shipped with the OS/390 Security Server. fwlogd assists in the filter and Network Address Translation (NAT) logging process, and fwtimernat manages NAT timeouts.

Included in eNetwork Communication Server for OS/390

1. **Network Address Translation** - Allows internal IP addresses to be hidden from the non-secure network, either for security reasons or because an intranet is using non-registered IP addresses. NAT maps the internal IP addresses to registered addresses, allowing UDP and TCP traffic to flow freely. IBM provides NAT for any routed TCP or UDP application packets. In addition, FTP is supported by providing translation of the IP address in the port command.

2. **IP Filters** - Provides intranet/Internet access control by using a set of administrator-defined rules to determine if a packet arriving at or departing from the TCP/IP stack should be allowed to pass.

3. **IP Tunnels** - (IPsec, or Virtual Private Network) Allows you to define a secure pathway across the Internet or an intranet to another host. The data traveling across this pathway can be encrypted and provided with authentication information at the source, and decrypted and authenticated at the destination.

Using OS/390 Firewall Technologies

There are many Internet firewalls on the market today, including IBM's eNetwork Firewall which runs on a number of platforms including OS400, AIX, and Windows NT. The question is whether the OS/390 Firewall Technologies can be used to replace or supplement the use of other firewalls. There are several considerations:

1. Isolation of the firewall – Generally the best approach is to isolate the firewall in a separate device. With OS/390, the installation can put the firewall in its own LPAR. This allows the firewall installation to remove any services that are not required by the firewall. The next best alternative, and possibly most reasonable approach, is to direct all incoming traffic (from the Internet) through the stack running the firewall. This allows applications such as Telnet and FTP to be activated, but becomes subject to the filtering rules defined on the firewall.

2. Limited Proxy Server Functions – Either a proxy server, socks server, or state based filtering is needed to control user access to or from the untrusted network. The OS/390 Firewall technologies only provide an FTP proxy and a socks server. Socks requires that the user install special socksified version of all of their Internet client programs.
3. VPN Functions – The VPN functions in the OS/390 Firewall Technologies are only designed to establish secure communications between itself and another compatible firewall. The OS/390 VPN functions do not currently provide the ability to link to remote users such as employees.
4. Access Control – The OS/390 firewall technologies has only limited capabilities to control access by user access. The filters are designed to control based on IP address or type of service.

Depending on the specific requirements, OS/390 Firewall Technologies may be best used to supplement but not replace the use of other firewalls and technologies. OS/390 Firewall technologies may be used to enhance protection for services such as Web based applications when accessed from the insecure or untrusted network.

4.2 E-Network Communications server – TCP/IP Services

TCP/IP is a set of protocols and applications that allow you to perform certain computer functions in a similar manner independent of the types of computers or networks being used. With the popularity of the Internet, TCP/IP has become the network protocol of choice. Since most systems and applications are designed to communicate using TCP/IP, it makes it much

easier to interconnect systems and share data. Not only is TCP/IP well known but so are many vulnerabilities, often associated with TCP/IP and the Internet. Many of the vulnerabilities in TCP/IP are related to TCP/IP enabled applications.

Weaknesses in TCP/IP applications

Beyond any problems with the use of TCP/IP protocol, there could be problems with the applications communicating using TCP/IP.

OS/390 Unix services provide safeguards to eliminate many of the typical exposures associated with TCP/IP applications. IBM has eliminated the use of one of the most dangerous features of traditional Unix internetworking, the use of trusted host facilities.

In many Unix systems, the system administrator may create a file "hosts.equiv" of "trusted systems". Alternatively, each user may create a file ".rhosts" of hosts that the particular user trusts. In either case, the trusted host designation means that userids on another hosts may login using rlogin or issue remote shell commands without specifying a password. While this feature may be convenient in some cases, often mistakes are made which leave systems and servers open to penetration. IBM has eliminated this potential problem for its OS/390 Unix services.

4.2.1 telnet

In most Unix systems, the standard telnet service allows the user to connect to the host and emulate a DEC vt100 or similar terminal. In the case of OS/390 Unix, the default is to have the standard telnet port emulate an IBM 3270 terminal. The installation may choose to change this option or enabled the standard telnet service on another port.

4.2.2 rlogin

rlogin is often used referenced in the OS/390 Unix manuals in place of telnet. The reason is that the default setting for OS/390 Unix is to have the standard telnet port set to emulate IBM 3270. As mentioned above, OS/390 UNIX does not use the .rhosts file that is used on most other UNIX systems to indicate the remote hosts and users who are allowed to access your system without specifying a password. A password is always required to rlogin to an OS/390 UNIX system.

4.2.3 sendmail

Sendmail is an application that has been plagued with many security holes. Depending on the customer's environment, sendmail may not be needed. Therefore, SMTP on port 25 may not need to be enabled.

4.3 LAN services - LANRES

4.3.1 LANRES

LANRES provides a number of features to support NetWare LANs and LAN administration including:

- Administration through LANRES of multiple NetWare servers.
- One login to the network provides access to data on multiple servers in the tree.
- Both host users and NetWare workstations can print data or documents.
- Host users can manage files and directories.
- NetWare workstation users can store data on host direct access storage devices.

Administration through LANRES

With minimal training, an OS/390 administrator can easily function as the LAN administrator for an almost unlimited number of LANs connected by OS/390 LANRES. This administrator can quickly and easily:

- Add and delete LAN users
- Modify trustee rights
- Change users passwords
- Administer print queues and print servers
- Limit the amount of disk space available to users
- Create and delete directories
- Create and delete NetWare NFS** group and user mappings
- Display user bindery, identification, and trustee rights information
- Start a chain of commands
- Save and restore the NetWare bindery
- Rename groups, users, print queues, and print servers
- Limit the number of concurrent user logins
- Set password limits

One Login for Access

LANRES provides the ability to integrate network access either by:

1. Providing the ability for host users to print data or documents
2. NFS users to access or print data or documents on Novell LAN volumes including OS/390 LANRES volumes. The administrator can map the NFS user IDs of the NFS UNIX clients to an existing NetWare user. This means, anything a NetWare user can do, the NFS user can do.

Host Users and NetWare Workstations Can Print Data or Documents

The use of LANRES provides both host users and NetWare workstations with increased printing options:

- Host-to-LAN Printing - Host users can print to Novell LAN based printers.
- LAN-to-Host Printing- Both host and LAN users can print to printers attached to OS/390 (e.g, host based Advanced Function Printing (APF*) page printer).

Host Users Can Manage Files and Directories

The distribution function of OS/390 LANRES lets authorized OS/390 users perform a variety of centralized tasks, such as:

- Distribute company forms from the host to various LANs
- Route output from host based batch processing to servers
- Consolidate reports on the host
- Copy important LAN data on the host
- Copy important host data on the NetWare server
- Distribute messages to NetWare users
- Create, delete, rename, and display NetWare files and directories
- Display NetWare server volumes, directories, and file information
- Compress data on the S/390

Disk Serving of OS/390 LANRES

Normally add data for Novell LAN's are stored on workstations or servers. OS/390 LANRES disk serving provides the ability to create disk images that can be accessed from the Novell LAN's. They appear to be harddisk images but in reality the data is stored in OS/390 datasets.

LANRES Security and Trust Relationships

The trust relationship between the Novell LANs and LANRES is established using passwords. These passwords take two forms:

- Component Passwords - These passwords are established when the NLM's are loaded on the NetWare side and then used on the OS/390 side to bring up the various LANRES components, such as the administrator functions.

- Individual NetWare Logins and Passwords – When the host users initiate user functions such as printing or managing files, they must enter their individual NetWare login and password.

LANRES provides a number of convenient functions but has a weak security functions for two reasons:

1. Single passwords to bring up the LANRES components does not provide for individual accountability for the use of administrative authority.

2. LANRES apparently does not provide the ability to fully integrate the NetWare login with the OS/390 user logins.

4.4 Network Computing Services

4.4.1 WebSphere Application Server

The WebSphere Application Server includes common webserver capability, including Secure Sockets Layer (SSL) functionality, and support for Java-based

servlets. The webserver can serve out data from HFS files or MVS datasets. The webserver can be configured to perform any desired level of RACF based security checking when a client attempts to access a specific file or resource. Three protection options can be used to control access to MVS or HFS resources available to the webserver:

- Password protection - the server provides options to use an existing MVS user ID and password, and to allow RACF to perform password verification.
- IP address or host name protection – password protection rules can be activated for a request based on the originating IP address (or host).
- Secure Sockets Layer (SSL) *client authentication* – the webserver can be configured to request a certificate from all clients making an https request. The server will establish a secure connection if the client has a valid certificate and deny the request if the client has a certificate that has expired, if the certificate is signed by an untrusted CA, or if the client does not have a certificate. (This option is not to be confused with the more common *server authentication* which requires the server, not the client, to have a certificate.)

In addition to the authenticated webserver protection options listed above, mechanism's are provided to allow guest or anonymous users access to designated resources available to the webserver.

As with any other webserver, proper administration is required to control access of information to authorized individuals.

Extending Webserver Functionality

Webserver functionality can be extended to retrieve DB2, IMS, CICS, or other data and present this data to a client browser. The term "web connector" is sometimes used to refer to this "glue code" that connects the webserver with DB2, IMS, CICS, or other resources.

Examples of how to extend webserver functionality, using Common Gateway Interface (CGI) scripts, are provided with OS/390 for access to:

- DB2 via DRDA protocols for remote data access
- IMS via the APPC/IMS interface
- CICS via the CICS external call interface (EXCI)

Programs (CGI scripts) that extend functionality will typically take some action based on user input provided to a webserver from a client's browser. As with any other webserver, care must be taken to ensure that bugs in the extended functionality programs do not create new vulnerabilities and allow unauthorized access.

5.0 Relevant OS/390 Products

5.1 eNetwork Host On-Demand

Host On-Demand allows Java-enabled browsers to emulate TN3270E and other types of mainframe sessions through a dynamically downloaded emulator. A Java applet, capable of a subset of the functionality a traditional, full featured emulator provides, is served from a webserver to a browser where it is executed.

No new access points to the mainframe are introduced to support Host On-Demand. However, web browsers need be configured with Java enabled which may be a security concern depending on the security policy in effect.

6.0 Conclusions

Based on available OS/390 UNIX security information and knowledge of the customer's IT environment, some conclusions can be reached. The following list includes both specific recommendations and suggestions for follow-on activity:

1. Comply with relevant recommendations made in the OS/390 UNIX section (Appendix A1.11) of IBM's Information Security Controls document.
2. Do not allow users to update OMVS fields in their RACF profile.
3. Be selective about purchased UNIX programs that are installed so they will not compromise the security level.
4. Ensure "strong" passwords are maintained on system level userids (e.g. BPXROOT, OEDFLTU, and OMVSKERN).
5. Determine specific auditing requirements. In order to provide good security auditing, the following may be appropriate:
   - evaluate the need to implement the RACF auditing controls to meet the general auditing requirements for OSR's (see section 3.4) as well as for add-on products and customer specific applications. The evaluation should be based on the actual deployment of the OS/390 Unix services.
   - implement audit(all(read)) for profiles which control administrative authority such as BPX.SUPERUSER, BPX.SERVER, and BPX.DAEMON.
6. The LDAP directory may become a central point of access control to the most sensitive data as the use of directories and directory enabled networks (DEN) become more prevalent. For this reason, a project may be needed to carefully define directory requirements including access control requirements. From these requirements, specific standards can be developed for how to properly secure access to the directories using the OS/390 LDAP security controls.
7. Develop one or more trial functions or applications to help demonstrate OS/390 UNIX related capabilities and how they can benefit the customer.

Appendix A - A comparison of UNIX, OS/390, and OS/390 UNIX

Category	"Traditional" UNIX	OS/390 (MVS)	OS/390 UNIX
User identity	Users are assigned a unique 4-byte integer UID and user name.	Users are assigned a unique 1 to 8 character user ID.	Users are assigned a unique user ID with an associated UID.
Security identity	UID	User ID	UID for accessing traditional UNIX resources and user ID for accessing traditional OS/390 resources.
Login ID	Name used to locate a UID	Same as the user ID	Same as the user ID
Special user	Multiple user Ids can be assigned a UID of 0.	RACF administrator assigns necessary authority to users.	Multiple user Ids can be assigned a UID of 0 or users can be permitted to BPX.SUPERUSER.
Data set access	Superusers can access all files.	All data sets controlled by RACF profiles.	Superusers can access all HFS files; data sets controlled by RACF profiles.
Identity change from superuser to regular user	Superuser can use system functions to change the UID of a process to any UID.	APF-authorized program can invoke SAF service to change identity.	There are two options: • If the BPX.DAEMON FACILITY class profile is not defined, the superuser can use system functions to change the UID of a process to any UID. • Or, the superuser must be permitted to the BPX.DAEMON FACILITY

Category	"Traditional" UNIX	OS/390 (MVS)	OS/390 UNIX
			class profile in order to change UIDs.
Identity change from regular user to superuser	**su** shell command allows change if user provides root's password.	No provision for unauthorized user to change identity.	**su** shell command allows change if the user is permitted to the BPX.SUPERUSER FACILITY class profile or if the user provides the password of a user with a UID of 0.
Identity change from regular user to regular user	**su** shell command allows change if user provides password.	No provision for unauthorized user to change identity.	**su** shell command allows change if user provides password.
Terminate user processes	Superusers can kill any process.	MVS operator can cancel any address space.	Superuser can kill any process.
Multiple logins	Users can login to a single user ID multiple times.	Users can only log on to TSO/E once per user ID.	Users can login multiple times to a single user ID and logon once to TSO/E at the same time.
Login daemons	**inetd** daemon processes user requests for login. A process is created with the user identity (UID).	TCAS and VTAM process user requests for logon. A TSP/E address space (process) is created with the user identity (user ID).	Users can log on to TSO/E or login using the **inetd** daemon. In all cases, an address space is created with both an MVS identity (user ID) and a UID.

Appendix B – References

The following IBM references are useful for understanding OS/390 UNIX related security issues:

1. IBM # SC28-1890-06 OS/390 V2R6.0 UNIX System Services Planning
2. IBM # SC28-1891-05 OS/390 V2R6.0 UNIX System Services User's Guide
3. http://ww.s390.ibm.com/products/oe The OS/390 UNIX System Services web page
4. Understanding and Deploying LDAP Directory Services, Timothy A. Howes, Mark C. Smith, MacMillan Technical Publishing, 1999
5. IBM # SC24-5861-01 OS/390 V2R6.0 Security Server: LDAP Server Administration and Usage Guide
6. IBM Information Security Controls IBM Global Services template document customized for a specific account