Global Information Assurance Certification Paper

Michael Walsh
SANS Security Essentials GSEC Practical Assignment Version 1.2f

Some of the Dangers of Connecting your AS/400 to a Network

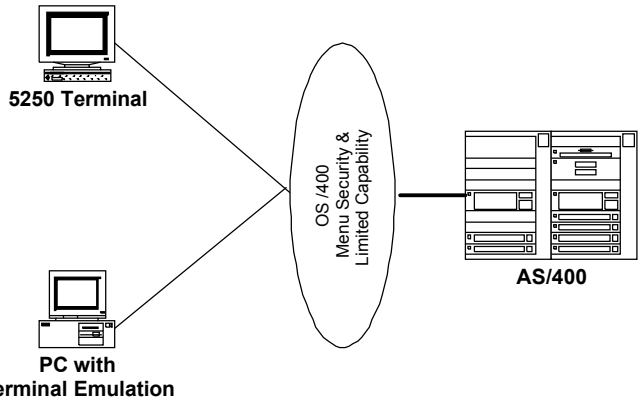
The AS/400 has evolved since its inception and with each change there have been associated security issues to resolve. The AS/400 in today's networked computing environment has several inherent security exposures that should be addressed.

Since its beginning the AS/400 computing platform has been one of the most successful systems used by businesses to hold and process their information and data. The AS/400 was designed from the beginning to securely store and protect data. The Operating System of the AS/400 was designed with security in mind and the AS/400 is thought by many to be the most secure system "out-of–the box".

The early AS/400 environment consisted of terminals direct connected through workstation controllers into the main system. Applications were accessed by users through terminals via a "green screen" interface. Access to applications is granted to users using "Menu Security". When the user logs on to the system the user is presented with a list of menu options for functions that the user is allowed to perform. Users were further restricted in what they could do by setting the user profile parameter *LMTCPB* to **YES* to prevent the entering of commands at a command prompt. If a user was allowed to enter/update data for a particular application, the user profile allowed object level authority to the associated production library by putting the library in the users library list. This was a secure scheme since the user could only access the data through a menu configured for his/her responsibilities.

Things changed when the Personal Computer (PC) came on the scene. Eventually users with PCs wanted the personal processing power of the PC for all the new applications they had not been able to do on the "mainframe". They still had their jobs to do and the information still resided on the AS/400 so it was either have a PC and a Terminal to clutter their desk or come up with a way to access the AS/400 from the PC.

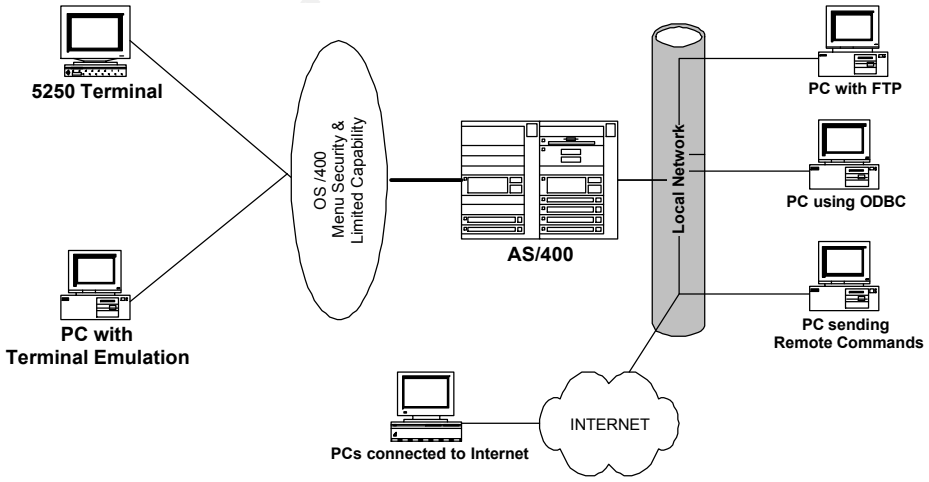
To solve this PCs were first connected to the AS/400 via twinax and asychronous workstation controllers with terminal emulation programs to provide users their familiar "green screen" interface. The OS/400 menu based security still provided protection.



The advent of computer networking added more communications capabilities for connecting to the AS/400 and along with it, additional security issues. The network protocol used alot today for connections to the AS/400 is TCP/IP, which now allows connection to the Internet opening even more security issues. These additional communication capabilities have added functions that do not go through a menu, thus bypassing menu security. They also don't require a command line to enter commands, thus bypassing the Limited Capability attribute. Some of the functions with vulnerabilities in this type of environment are:

Client Access
FTP
ODBC
DDM
TELNET

Our diagram now looks like the following:



In this environment, the dangers are from outside and inside the local network. Lets look at the potential dangers.

A Typical AS/400 Environment

A typical AS/400 environment consists of the operating system programs and utilities that come with the AS/400, and purchased third-party software applications to perform various business functions, i.e. payroll, accounting, manufacturing, distribution.

Third-party software vendors rely only on menu based security which leaves application data open to access via the functions already mentioned which bypass this type of security. Typically, a vendor installation process may create group profile(s) with access to the programs and data for the application. Users are set up with object level access to the application data based on their roles in the software application by making them part of the group profiles. Menu access is based on the group profiles established. If users have inquiry access via the application menu system, they have read-only access to the data. If they have update access via the application menu system, they have write access to the data. Users do not have access to a command line for command entry.

A typical environment uses TCP/IP for network connectivity to PCs and other hosts. A connection to the Internet is also commonplace. It is fairly easy for PCs or other remote systems to get around the menu security and access the data on the AS/400.

Client Access / Express

Client Access provides terminal emulation, file transfer, remote command, and printing to network based printers.

Besides providing 5250 terminal emulation for PC access to menu-based applications, Client Access provides a graphical user interface to interacting with an AS/400. It makes it simple for a user to transfer information up or down from the AS/400. A user that has inquiry authority via the menu system now is able to download that information to their PC for viewing and manipulation. A user that has write or update authority to the menu-based application can use Client Access to download data, manipulate it and upload it, potentially overwriting over the original information.

A knowledgeable user can even send CL (Command Language) commands to the system via the RMTCMD function in Client Access. The limited capability parameter on a user account profile is ignored because the command is not entered at a command line.

FTP

The use of TCP/IP allows the use of FTP (File Transfer Protocol). FTP is a method of transferring files between computers regardless of hardware or operating systems. Thus one can transfer from AS/400 to AS/400, or AS/400 to and from another type of computer. The AS/400 can serve as an FTP server or client. The security concerns here are similar to those for Client Access but with a few additional exposures. The basic FTP commands available on an FTP client accessing the AS/400 are:

- Logon
- File download from the AS/400
- File upload to the AS/400
- Directory navigation
- Execute CL Commands

To start a connection to an AS/400 FTP server a user must login to the service. If not configured to restrict Anonymous logins, anyone can logon to the AS/400 FTP server and download any public information on the AS/400. With Anonymous logins disabled, a valid user-id and password are required. A vulnerability with the login process is that encryption not is used during the login process to the FTP server. Passwords could be sniffed and compromised.

As with Client Access, if a user has account authority set up for Menu access they have the same access via FTP. Data could be downloaded, manipulated, and uploaded replacing the original data. There is no control on what and how much is uploaded the AS/400 potentially resulting in a denial of service by using up all disk space.

The AS/400 directory navigation functions present additional exposures. Without proper object authority in place, a hacker or unscrupulous user could create, rename, or delete directories and files causing real system problems.

The FTP client can also submit CL system commands even if the commands are restricted by the Limited Capability parameter in the users account. A hacker now has access to the AS/400 operating system.

To make matters worse, all the FTP functions mentioned, are not audited. There is no audit trail or history of what was done and by whom.

ODBC

ODBC is a tool that allows PC applications to have file and record level access to data on the AS/400. AS/400 applications are written to handle field level security within the application code. PC applications such as Microsoft Excel and Access can read data directly from AS/400 files and can access all fields in any file the user has READ access. Any user with *CHANGE authority to AS/400 files can update data or even delete records or files.

DDM

DDM (Distributed Data Management) is remote data access at the file and record level and can be run from PCs. The issue with DDM is the same as for ODBC. In addition system CL commands can be sent to the target AS/400 using the Submit Remote Command (SBMRMTCMD) command. Again commands are not restricted by the Limited Capability parameter since it is not from a command line.

TELNET

The AS/400 supports TELNET connections from remote TELNET clients and allows a user to interactively sign on and run applications on the AS/400. There are some serious exposures to the use of TELNET particularly if the AS/400 is connected to the Internet.

- When a user signs on to a TELNET session, the passwords are transmitted in clear text and are vulnerable to sniffing.
- TELNET automatically configures virtual devices for each session. The number of sign-on attempts is equal to the number of allowed sign-on attempts (*QMAXSIGN*) times the number of virtual devices that can be created. This gives a hacker more chances at password guessing and also can lead to a denial of service condition.
- TELNET session logging is limited.

Solutions

The question now becomes how to protect against these vulnerabilities? It would appear that there is a big hole left in the security of an AS/400 connected to a network and the Internet. The way to close the hole is to use multiple security layers to resolve the exposures.

Starting with the OS/400 built-in object based security capabilities, make sure that the correct level of granularity is used to secure objects.

- Limit the number of objects that users with **PUBLIC* authority have access to. Only make publicly available what is needed.
- Secure at least at the Library level, for the required access.
- Give users only the access required for them to do their job.
- Review the authority scheme implemented by 3rd party Application Vendors, contact them about problems and adjust.

Unless purposely using the AS/400 as a web server for open access from the Internet, disable anonymous FTP logins.

The best way to resolve the majority of security issues with Client Access, FTP, ODBC and DDM is by the use of "Exit Programs" to control and monitor their use from network connections. Exit Programs are programs that supplement existing security by monitoring, and allowing or rejecting requests. Fortunately, OS/400 provides "Exit Points" in the operating system that allows user-written programs to be called before a function executed. The Exit Program associated with a particular Exit Point, receives information from the operating system when a request occurs. The Exit program analyzes the information and determines whether the request should be allowed or rejected and sends a response back to OS400 which processes or rejects the request. The Exit Program can use the passed information to create a log the requests processed. This provides for an additional layer of control beyond object level security to restrict what users can do. IBM provides documentation for all the exit points.

If AS/400 system programming resources are available, writing exit programs to close all of the security exposures is definitely doable but it could take considerable time and effort to accomplish. Some organizations may find this a viable alternative if programmer resources can be freed up from other IT projects. Fortunately there is another alternative. Several 3rd party software vendors have identified the need and have developed packages of exit programs to plug the security holes. These vendors have invested considerable resources to develop the packages and have made them easy to install, configure and use. Some vendors have even made their packages so that the user can first install in a monitoring mode to determine what functions are already being utilized on the AS/400. The system can then configured to tighten the security without disrupting legitimate activity. Of course all activity is now logged for accountability, alert messages can be sent, and reports generated of allowed and disallowed accesses.

This is the recommended approach particularly for organizations with little or no available IT development resources.

Implement newer releases of the OS400 operating system. The newer releases of OS400 provide for enhanced security. One enhancement reduces the chance of denial–of–service attacks from a flood of FTP logins. V5R1 introduces a delay before the next prompt after an invalid password login attempt. Additional invalid password attempts result in longer delays.

The issue of clear text passwords being sent over the network (or Internet) can be resolved for FTP and TELNET by implementing supplemental security facilities recently introduced into OS400 and the appropriately configured client. Secure FTP can be used to implement SSL (secure socket layer) communication between an SLL FTP client and the AS/400 FTP server. The OS/400 secure TELNET server can secure TELNET sessions to the AS/400. In addition to the login process, the whole session is encrypted via SSL. Client Access Express is one of the TELNET clients that can provide secure 5250 emulation.

Conclusion

An AS/400 in today's networked and Internet connected environment can have many potential security holes that can be exploited from inside and outside the local network. These holes can be secured if implemented with a layered approach using the OS400 built-in object level security, Exit Programs, and additional supplemental security tools / programs.

References

International Technical Support Organization, Rochester Center "AS/400 Internet Security Scenarios: A Practical Approach", July 2000, Document Number SG24-5954-00

International Technical Support Organization, Rochester Center "AS/400 Internet Security: Securing Your AS/400 from HARM in the Internet", June 1997, Document Number SG24-4929-00

Green, Chris "ANJE Classics: Internet Security Part 5: Securing FTP and WSG" 12/23/99

URL: http://www.midrangecomputing.com/anje/article.cfm?id=281&md=19996

Woodbury, Carol "AS/400e Security"
URL: http://www.as400.ibm.com/tstudio/secure1/whitepapers//v4r4wp.htm

Woodbury, Carol "Securing FTP Communications Under V5R1"
URL:
http://www.as400network.com/resources/artarchive/index.cfm?fuseaction=viewarticle&CO_ContentID=10942

Evans, Wayne O. "Exit Programs Are Essential to Protect Your iSeries 400"
URL: http://woevans.freeyellow.com/ExitPrograms.PDF

McKelvey, Mark "Secure Internet Applications on the AS/400 system"
URL: http://www-1.ibm.com/servers/eserver/iseries/beyondtech/secure_internet_apps.htm