DATA COMMUNICATIONS MANAGEMENT

SECURE ACCESS TO MISSION-CRITICAL APPLICATIONS

David Johnson

INSIDE
Why Use the Internet? The Challenges; Network Integrity; Filtering Firewalls; Application Firewalls; Proxy Firewalls; SOCKS Firewalls; Authentication/Access Controls; Authentication Services; Access Controls; LDAP; Application Integrity

Every day, MIS departments in organizations around the world wonder how they can maximize the potential of the Internet. One of the biggest obstacles still holding them back is their concern over security. Organizations face new challenges when attempting to interface legacy systems with the Web. Whether it is an internal intranet or external access for employees or business partners over the Internet, a series of security measures and policies can be put in place to ensure secure access to these mission-critical applications. This article will look at several levels of security that companies should address to help alleviate concerns over utilizing the Internet for business-critical activities. Areas to address include network integrity, authentication services, communication integrity, and protection of the information flowing across the network.

WHY USE THE INTERNET?
In today’s information society, timely access to information can be critical. Many organizations adopted the IBM mainframe as their mission-critical computing platform for its reliability and transaction processing capability. Not only is processing the information key, but also getting it into the hands of those who can act on the information quickly. The Internet offers a low-cost network that can be used to share information with customers, business partners, or remote employees. That free flow of information can greatly increase a company’s compet-

PAYOFF IDEA
Mainframe systems are the repository of a vast amount of mission-critical data and applications. Organizations are grappling with how to leverage these data and applications to provide new Internet-based services to their business partners and customers. Security is obviously a major concern. This article describes the various types of security that should be addressed in order to keep mission-critical systems secure.
itive edge. Great care must also be taken to keep this business-critical information from unwanted eyes. With the right security measures in place, the risk of someone accessing unauthorized information can be greatly reduced. This article focuses on how to provide secure access to mission-critical applications predominately running on enterprise IBM mainframes. While IBM mainframe applications are the focus, the security discussions relate to almost all mission-critical platforms.

THE CHALLENGES

Companies face several obstacles in relation to older security models that have sufficed up until now. In the past, most organizations utilized leased lines for communication to mission-critical applications. Local area networks (LANs) were used only for sharing devices such as printers; 90 percent of mission-critical applications were in use on the IBM mainframe. The mainframe security model was simplistic in nature, but very powerful. Dumb terminals were attached directly to a communication controller that was in turn directly attached via a leased line or hardwire connection to the mainframe. A number of companies took this one step further and only authorized certain applications or user access from specific terminals. This is what is known as Logical Unit (LU) Nailing. A specific user’s session or ID was “nailed” to a specific terminal. The only way to eavesdrop on an application conversation was to physically tap into the leased line or controller. Physically tapping into a phone line, while not impossible, was difficult. The eavesdropper would also have to record the session and play it back through a special decoder program designed to filter SNA traffic. Because all terminal traffic for a given controller was multiplexed across a single line, it could mean hundreds or thousands of packets to filter through to find any usable information.

This communication or session level of security was coupled with a series of host-based security products such as Resource Allocation Control Facility (RACF), ACF-2, or TopSecret, to name a few. These host-based measures were centrally controlled and administered. They determined what resources a user or a program being run by a user could access. One user may be able to view records in a DB/2 table based on his or her authorization. Another may have complete read/write privileges over that same information. This access control could also be location dependent. In some instances, access to top secret information can only be done from the terminals physically located in a secure room. These central control facilities allow MIS staff to easily monitor any unusual activity and greatly protect assets from both other applications running on the mainframe, as well as unauthorized users.

While these security methods are still available, the majority of companies have moved away from terminals to networked PCs and from leased lines to switched networks based on frame relay, X.25, or asyn-
chronous transfer mode (ATM). Most users no longer use SNA all the way to the desktop. An SNA gateway converts the traffic to IP, IPX, or some other LAN-based protocol. Also, LANs use shared media. There is one physical wire that all the devices share. To help troubleshoot this shared media, numerous LAN-based protocol analyzers have been developed over the years. These analyzers make it quite easy to observe or record all the information flowing across the network.

Organizations have also developed remote access capabilities to support remote and mobile employees. Early solutions relied on user ID passwords and even dial-back methods to help protect the integrity of the network. With efforts to continue to reduce costs, many companies are looking to the Internet as a means of providing extremely low-cost dial-access and communications with business partners. Mobile employees using the Internet for a remote access network make traditional dial-back solutions unfeasible.

While there are a number of new concerns for MIS departments as the world moves into a network-centric infrastructure, there are methods available to “plug” potential security holes and open access to authorized users. To provide access to one’s mission-critical applications to business partners or other users via the Web, there are four main areas to focus on when providing access. These are:

- Network integrity
- Authentication/access control
- Application integrity
- Data protection

The remainder of this article takes a look at each of these areas in detail and provide an overview of the different options and methods to secure each area in the network.

Network Integrity

The first area to focus on is protecting the underlying network itself. Unauthorized users often try to gain access by locating and collecting information flowing over the network itself. While a number of companies have moved to dynamically assigning IP addresses to workstations, most servers and other fixed devices use a permanent IP address. This is often required so that users can always quickly find resources such as file servers, application servers, and printers. A fixed IP address also facilitates troubleshooting access to those systems. A skilled individual with access to a network can begin to learn the IP addresses of critical servers, sockets they communicate on, and other information.

Network integrity involves providing security at the network layer. For example, network integrity means preventing unauthorized users from
using an Internet connection to gain access to one's internal networks. Firewalls are the most typical deployed method to prevent unauthorized access to the network. Firewalls are available in several varieties. While some vendors combine several functions into a single offering, the most common functions provided by firewalls include:

- Filtering firewalls
- Application firewalls
- Proxy firewalls
- SOCKS firewalls

Some organizations have taken a shortsighted approach by effectively putting a Berlin Wall around their network and allowing no traffic in or out. While this might provide a sense of security, it is extremely limiting. The competitors of these shortsighted organizations are leveraging existing security solutions to provide access to information to business partners and customers. Those companies that do not provide access may feel safe, but they will suffer from competitors that offer better services to their customers.

**Filtering Firewalls.** Filtering firewalls are the most basic. They filter information packets based on a destination or a source address. A filtering firewall could be used to only allow outbound traffic from a certain IP or range of IP addresses. It could only allow inbound traffic from trusted IP domains. While filtering firewalls were useful when remote access and router networks were first established, they have become a bottleneck in today's network. With Dynamic Host Configuration Protocol (DHCP), remote access via an ISP, and other dynamic IP assignments, it is cumbersome — if not impossible — to update configurations to take into account all these new source or destination addresses. Most new solutions combine packet filtering with more advanced rules to protect the network.

**Application Firewalls.** A more advanced filtering firewall is an application firewall. Application firewalls are designed to only allow certain application traffic to pass its boundaries. They can be configured to allow different access, depending on whether the information is inbound or outbound. For example, a company may allow its employees to send files using File Transfer Protocol (ftp), but not allow anyone to receive files by the same manner. Other common application filters include telnet access, e-mail, and HTTP traffic. Each application can have a separate set of access rules applied to it. Application firewalls can prevent an unauthorized user from gaining access via a custom protocol. Users are forced to work within the confines of an allowed application protocol. Application firewalls can include the source or destination address as
part of the rules based access. Exhibit 1 shows an example of an application firewall, in which business partners can access the company’s mainframe via TN3270, but internal users cannot access external mainframes. External users can also send and receive mail (SMTP) and do Web transactions (HTTP), but they cannot telnet into the mainframe or do file transfers to or from it. Application firewalls typically do not provide authentication services.

**Proxy Firewalls.** Proxy firewalls begin to provide a level of authentication. Users are normally asked to provide an ID and password to access systems via the proxy server. The main function of a proxy server is to hide the IP addresses of internal users accessing outside systems and the IP addresses of internal systems. Most attempts at breaking into a system require the knowledge of its IP address. IP addresses are like telephone numbers: one needs to know how to contact the machine or person one wants to speak with.

Assume that a company allows its employees to send and receive files over the Internet using ftp via a proxy server. While each internal user has a unique IP address, all users collectively appear as a single IP address, that of the proxy server, to the outside world. Users requesting to do an ftp transfer are routed to the proxy server; the proxy server takes the user's requested transfer and replaces the source address with its own. The proxy server then sends the packets on to the destination. When the remote host sends the information back to the user, it uses the proxy server's IP address as the destination. The proxy server receives the packets and then forwards them on to the user's PC. Throughout the entire ftp transmission, the remote machine has never established a direct communications link with the internal user machine. The remote machine not only does not know the IP address of the actual user, but can-
not “piggyback” an attack on the communication because the proxy server is only sending valid ftp packets back to the user.

Proxy firewalls support most common applications, including ftp, telnet, HTTP, SMTP, etc. Companies can require their users to “log-on” to the proxy server, or preconfigure the connection in the browser. Both Netscape and Microsoft browsers support proxy configurations.

**SOCKS Firewalls.** Each successive generation of firewalls continues to build upon previous security systems. SOCKS version 5 is the latest generation of firewall technology. Not only does it support application, filtering, and proxy support, it also adds authentication services, encryption capabilities, and interoperability between different vendors' SOCKS firewalls based on RFC 1928. SOCKS firewalls are typically used to deploy Virtual Private Networks (VPNs). SOCKS firewalls can also be used to establish extranet communications between business partners. One of the biggest advantages of SOCKS firewalls over earlier implementations is that SOCKS v5 is a standard. Authorized SOCKS clients can dynamically negotiate through multiple firewalls. This reduces the complexity; prior to the standard, business partners had to statically configure their firewalls to match the configuration of each other.

Suppose there is a manufacturer that wants to allow its suppliers to access a mainframe application that tracks the purchase orders for the supplier. Instead of the supplier having to call the manufacturer every time to check on order status, the supplier accesses the application and looks up the information directly. In order to protect their networks, both companies have implemented a SOCKS firewall. Each company has its own access and control policies, and each firewall is configured differently. The supplier employees who need access to the manufacturing application are given SOCKS client software. This client software allows the supplier to negotiate an outbound connection through the supplier's firewall and then negotiate an inbound connection through the manufacturer's firewall. No configuration details are needed for either firewall. The SOCKS protocol handles the negotiation and authentication process transparently to the end user or the mainframe application.

While SOCKS firewalls are the latest generation of technology to protect the integrity of the network, they still have some drawbacks. SOCKS firewalls are not yet widely deployed. They make up about ten percent of the installed base. In order for the client negotiation to work, SOCKS client software must be installed on every desktop that needs access. This can cause a maintenance and distribution headache for network administrators because they now have an additional software component on every desktop that must be maintained. A number of application vendors have recognized this and are adding SOCKS client support directly into their applications, providing users with the benefits of a SOCKS fire-
Firewalls are the most common and one of the best ways to protect the integrity of one's network. In order to facilitate access, one needs to allow authorized users to access only those resources for which they have permission. This brings us to the topic of authentication and access controls.

Authentication/Access Controls
Access controls are used to authenticate users and allow them to access only certain resources. These resources could be an internal ftp server, a specific mainframe, or a specific mainframe application. Or, one might want to restrict access to standard working hours. Although one might allow business partners or customers access to certain applications or resources, one does not want them to have full reign over one's internal systems. Access controls involve two major components: authentication and resource permissions. Both of these areas were solved long ago in the IBM mainframe environment. Unfortunately, tools like RACF or ACF2 cannot really be used to control and authorize users for network-based resources.

RACF is one of the most well-known systems for providing authentication services and access controls for mission-critical systems. When a user is authenticated by RACF, that user has a permission profile that is activated. This profile not only contains what areas or applications on the mainframe system(s) the user is allowed to access, but also what resources and portions of data records that the applications the user is running can access. While this system provides a high degree of control over the environment, a user must log on to the mainframe for it to be active. RACF cannot protect or control access to non-mainframe applications.

And, because the mainframe applications are mission critical, one will want to make sure an unauthorized user does not even get to the mainframe log-on screen. RACF, while very powerful, is still a userid-and-password-based system. Once a password is compromised, the security is gone. What one needs to implement is a RACF style authentication system for your network itself. The two functions that must be provided by the network are authentication services and access controls.

Authentication Services. Most early solutions solely relied on userid and passwords. This is authentication in its simplest form. This is also the easiest type of system to break. Due to the large number of systems that a typical user needs to access via a password, most pick short, easy-to-remember passwords. For example, many choose a child’s name, date of birth, or other common item. Trying to remember which password was for e-mail, which was for mainframe access, etc. was a chore the com-
mon user reluctantly was forced to deal with. Some companies are successful forcing their users to change their password every 30 to 90 days, while others gave up that requirement due to user revolt.

There have been several improvements to simple ID-and-password-based systems. One of the popular methods is to use a hardware token or card to generate a new password every time. One of the popular implementations of this was SecureID. SecureID consists of an authentication server at the central office and a hardware card. This hardware card is synchronized with the server and generates a four-digit number every 30 to 60 seconds. This number is the user's password. A log-on dialog box is displayed to the user. The user enters the correct ID and the password displayed on the SecureID card. The SecureID server validates the user and current password, and then grants access to the network.

While this method eliminates the problem of easily guessed passwords, it does have some drawbacks. For starters, users have to rely on a hardware card. While the cards are not expensive, if a user loses the card, he loses network access. This does happen, especially with traveling users. Also, the default for most token-based systems is to generate a new password every 30 seconds. If the server takes longer than 30 seconds to authenticate the user, or the user attempts to log on after 29 seconds have passed, the user may have to attempt a connection several times before he is successful. While MIS departments may feel this is a small price to pay for security, tell that to the CEO or Vice President of Sales after having to make several attempts after a long day of meetings. One final drawback with this system is that the network-based application server must support the system. While most popular systems such as Windows NT and UNIX support SecureID, not all operating environments or Web servers do.

The newest authentication systems involve a digital signature. A recognized Certificate Authority, such as Verisign, can generate this digital signature or the company can generate it. The most common type of digital signatures is an X.509 certificate (cert) used for secure socket layer authentication. This certificate is an electronic stamp or file that is stored on the local PC. The most common use of a cert is for browser authentication. Both Microsoft Internet Explorer and Netscape Communicator support authentication to a Web server using certs. When accessing a network via the Web server, the server queries the browser for its cert. The server looks up the cert to see if the user is authorized for access. This mechanism solves the password issues by storing the digital signature. The only drawbacks are that the cert is tied to a physical machine and that not many systems other than Web servers support digital certificates yet.

Companies and vendors are addressing this latter issue by utilizing enterprise directory services. The directory service that is quickly becoming
the most popular is Lightweight Directory Access Protocol (LDAP), which falls into the category of access controls.

**Access Controls.** There are several network-based access control systems available today. These include RADIUS, TACACS+, and even some custom-developed systems. RADIUS servers have become very common for remote access authentication systems. They cannot only authenticate a user, but some control information can be configured. This includes the time of day or days of the week a user can dial in, how long the user can be connected, etc. RADIUS servers became very common in UNIX and remote access environments. A standard was developed so that systems can support RADIUS servers from multiple vendors. RADIUS was the first attempt at having a centralized authentication and access server. While RADIUS offers a number of good features for access controls, it is not flexible enough or widely supported enough to become a true enterprise authentication server. TACACS+ was Cisco’s implementation of an authentication and access control server for its remote access solutions. TACACS+ offers the same level of services as RADIUS, but is specific to a Cisco environment.

The industry realized quite some time ago that an enterprise directory would be needed. The first attempt at an enterprise standard was the X.500 directory standard. This was a very complex standard that attempted to define all possible options. It was very complex, added a lot of overhead, and was very difficult to implement and administer. As a result of this complexity and the lack of real requirements at that time, most applications did not offer X.500 support. Those that did were unwieldy, slow, and not well received by the user community.

In addition to the complexity, X.500 directory services did not gain popularity because it was not until recently that the network has moved beyond its role as a communications infrastructure to become the focal point for access. Users now wish to be able to log on once and then have access to all the applications for which they are authorized. This desire, coupled with new developments in directory services, now make “single signon” a reality.

**LDAP.** LDAP defines an interface to locate network services. Authentication and access controls are part of network services. As mentioned earlier, LDAP is not the first network directory to be introduced. Along with X.500, Novell has developed Network Directory Services (NDS) and Microsoft has been promoting its own undelivered Active Directory. Both offerings from Novell and Microsoft are designed to work best in their specific network environments. To be fair to Novell, it has gone to great lengths to make NDS available for non-NetWare platforms. The proprietary nature of these directory services is one of the main reasons that
they have not gained popularity. User organizations have decided to follow standards-based approaches whenever possible. This is especially true for Web-based solutions. LDAP is a public standard. There are a variety of places that one can even get the source code to LDAP royalty free. This gives organizations the choice of purchasing a commercial LDAP server or maintaining their own source code.

Because LDAP defines an interface and not necessarily the underlying structure, organizations can define what information they want to store in their central repositories. User information can be stored in a central LDAP server. Applications can be “LDAP-aware.” With LDAP, organizations can finally begin to regain the centralized control they used to have via mainframe systems like RACF. A user can log on to the network and gain authentication via an LDAP server. That log-on process could also connect authorized users to their main applications by reading the userid and passwords for those applications from the LDAP directory. One of the biggest benefits to the user community is the ability to achieve single log-on. From an MIS point of view, there is only one place to administer and maintain user information. Instead of going to the e-mail server, authentication server, file server, etc. to add, change, or delete a user, all this can be done from one central location.

User profiles can be stored in this central repository and utilized by LDAP-aware applications. In a mainframe access environment, information such as the SNA gateway address, destination mainframe, and Logical Unit name are used to provide connectivity. The user's mainframe password and ID can be sent to the mainframe automatically. Other user-configured items such as emulator keyboard and color map can also be stored and managed centrally. Exhibit 2 shows an example of a user, David Johnson, gaining authentication and access control using LDAP servers. In this case, a customized HTML page is built and sent based on David Johnson’s unique set of parameters stored in the LDAP server.

EXHIBIT 2 — Example of a User
LDAP not only provides a standards-based method for authentication and access control, it allows administrators the ability to recentralize user profiles and other information. Not all applications are LDAP-aware. Most successful network application vendors have realized the power of centralized management. More and more solutions that support LDAP are available. With the finalization of LDAP 3.0, most vendors will soon be offering LDAP support in their applications. IBM has even announced a version of LDAP 3.0 that will run on OS/390.

Application Integrity
The last major difference between enterprise mainframe systems and the Inter/intranet is the method of communication. 3270 applications were designed with a terminal and controller at one end of a leased line and the mainframe via a front-end processor at the other using SNA as the communication protocol. SNA is a state or persistent type of connection. The communication link is established for the duration of the application session. This is analogous to a standard telephone conversation — one calls somebody and then has an established connection until hang-up. Most 3270 applications are long-running conversations.

The HTTP protocol, utilized by the World Wide Web and corporate intranets, is a stateless protocol with the browser controlling the conversation. The browser asks the Web server for some information and then disconnects. Using the phone call analogy, this would be similar to:

1. Dialing the number, asking how the person is doing, getting a response, and then hanging up
2. Dialing the number, asking if the person is available for dinner, getting a response, and hanging up, etc.

This is an awful lot of overhead for a conversation and, worse, the potential is there for someone else to easily dial up and break into the conversation.

Providing secure browser-based access to SNA applications must take this issue into account. It is possible, using technology such as Java or ActiveX, to recreate the SNA-style persistence and supply either a character or graphical interface to the existing SNA application. By using TCP socket technologies, applications developed in Java or ActiveX can create a state-oriented connection. Both Java and ActiveX allow a character-style interface or a full graphical interface to be used. Both solutions can also encrypt all the information that is flowing to and from the SNA Web server. This ability allows one to explore the possibility of the public Internet as an access method or a low-cost remote access network for employees, business partners, and even customers.
Data Protection. The ability to keep corporate information safe from prying eyes while traveling across a TCP/IP infrastructure is paramount in today’s exposed environment. This is one area where Web-based solutions have completely surpassed traditional emulation. TN3270(E) has exposed a potentially serious security hole in the enterprise. TN3270(E) sends all information in simple clear text. It would not take long for a user with a shareware network “sniffer” program to collect mainframe userids and passwords. Exhibit 3 shows a network trace done using a standard shareware program from the Internet. The first is a trace of a standard TN3270E connection to the mainframe, clearly showing the userid as AU09615 and password as TSCHAULE. Exhibit 4 shows the same
connection using a Web-based solution that provides built-in encryption. The userid and password are impossible to decipher.

One used to frequently hear the phrase, “It’s our internal network; security is not an issue.” Most people do not realize that research shows 80 percent of all break-ins are by internal users. Who would have more to gain from access to your mainframe? The 13-year-old hacker looking for a cool game or the disgruntled employee that “sniffs” the accounting userid, passwords, and account numbers, looking for an unauthorized pay raise?

CONCLUSION
This article has discussed several options to help secure one’s network, but still provide access to these mission-critical applications for authorized users such as mobile employees, business partners or suppliers, and even customers. Implementing security in areas such as network integrity, authentication/access control, application integrity, and data protection can protect one’s network and systems, but still provide the flexibility needed for authorized access. When evaluating options for providing Internet access to mainframe systems, use Exhibit 5 as a set of minimum requirements.

With adequate protection in these areas, an organization can begin to utilize the Internet to be more competitive. Benefits can range from offering 7x24 customer service applications to realtime dissemination of information to business partners and suppliers. Financial benefits consist of both internal cost reductions and increased revenue, and customer satisfaction that comes with realtime information access. Secure, controlled access to “glass house” applications can bring enormous benefits to an organization. There are solutions and systems available today to make that secure access a reality.

EXHIBIT 5 — Access Control Checklist

<table>
<thead>
<tr>
<th>Type of Security</th>
<th>Why a Requirement?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firewalls in place providing at least filtering</td>
<td>Prevent unauthorized external access</td>
</tr>
<tr>
<td>User authentication and access controls in place, at a minimum userid and password</td>
<td>Ensure that only authorized users gain access to the systems and network required to do their job</td>
</tr>
<tr>
<td>Plan in place to integrate network-based authentication/access control (e.g., LDAP) with legacy systems</td>
<td>Provide comprehensive and seamless single log-on with reduced administration and high level of security</td>
</tr>
<tr>
<td>Web-to-host solutions ensure SNA-style persistent sessions</td>
<td>Prevent unauthorized break-in to the middle of an SNA session</td>
</tr>
<tr>
<td>All new mainframe access is encrypted</td>
<td>Prevent internal and external attacks on mainframe systems</td>
</tr>
</tbody>
</table>
David Johnson joined OpenConnect Systems Incorporated in August 1996. As Director, Product Marketing, Mr. Johnson is responsible for overseeing the marketing and sales and product strategies for all of OpenConnect's product offerings. With over ten years of high-tech industry experience, Mr. Johnson is well versed in technologies ranging from traditional IBM SNA access products to leading-edge remote access and Internet technology. Mr. Johnson has held marketing and technical positions at SNA emulation companies, wide area networking, and remote access solution providers. Prior to joining OpenConnect, Mr. Johnson was a Senior Product Marketing Manager at U.S. Robotics, Corporate Systems Division.