DATA COMMUNICATIONS MANAGEMENT

SERVER SECURITY POLICIES

Jon David

INSIDE

INTRODUCTION
Local area networks (LANs) have become the repository of mission-critical information at many major organizations, the information-processing backbone at most large organizations, and the sole implementation avenue for Internet protocol (IP) efforts in smaller concerns. The growing importance of LANs — the integrity and confidentiality of data and programs on them, their availability for use — demands proper security, but LANs have historically been designed to facilitate sharing and access, not for security. There is a growing pattern of interconnecting these networks, further increasing their vulnerabilities.

The Internet has similarly become an integral part of day-to-day operations for many users, to a point that business cards and letterheads often contain E-mail addresses, and a large number of organizations have their own Internet domain, organization-name.com. The World Wide Web (WWW) is an extension of the Internet, actually an additional set of functions the Internet makes readily available. It is gaining in popularity at a very fast rate, such that it is now common to see even TV advertisements cite Web addresses for additional information or points of contact (e.g., www.news-show.com, www.product-name.com, etc.). Today, even with the Web still in its infancy, there is much Web commerce, e.g., the display and purchase of merchandise. Although LANs come from a background where relatively little attention was devoted to security, the RFCs (Requests for Comment, i.e., the specifications to which the Internet conforms) specifically state...
that security is not provided and is therefore the sole responsibility of users. The Internet is rife with vulnerabilities, and the Web adds a further level of risks to those of the Internet.

Although servers are integral parts of various types of networks, this article will deal with LANs, not the Internet or the Web, or any other type of network. The Internet and the Web are individually and together important, and servers are particularly critical components (with PCs through mainframes being used as Web servers), but it is felt that most readers will be LAN oriented. The exposures of both the Internet and the Web differ significantly from LAN vulnerabilities in many areas, and deserve separate (and extensive) treatment on their own.

THE NEED FOR SERVER SECURITY
For a long time, information — and its processing — has been a major asset, if not the major asset, of large organizations. The importance of information is even reflected in the language used to refer to what originally was a simple and straightforward function: What was once known as computing became electronic data processing (EDP) and is now information processing; when expert guidance is needed in this field, people skilled in information technology (IT) are sought; in the contemporary electronic world, both the military and commercial segments fear information warfare (IW).

The information that we enter into, store on, and transmit via our computers is critical to our organizations, and in many cases it is critical not just for efficiency, profit, and the like, but to the very existence of the organization. We must keep prying eyes from seeing information they should not see, we must make sure that information is correct, we must have that information available to us when needed. Privacy, integrity, and availability are the functions of security.

LANs are a key part of critical information processing; servers are the heart of LANs. The need for proper server security is (or at least certainly should be) obvious.

Server/NOS vendors do not help the situation. As delivered, servers are at the mercy of the “deadly defaults.” Because security tends to be intrusive and/or constraining in various ways, servers “from the box” tend to have security settings at the most permissive levels to make their networks perform most impressively.

THE NEED FOR SERVER SECURITY POLICIES
The media have been very helpful in recent years in highlighting the importance of proper information security. Although they have certainly not been on a crusade to make large operations more secure, the many security breaches experienced have made good copy and have been well publicized. Because pain is an excellent teacher, and successful or-
ganizations endeavor to learn from the pain of others, the publicizing of various breaches of information security has made everyone aware of its importance.

Successful organizations endeavor to remain successful. If they recognize a need (versus merely a nicety), they endeavor to treat it. "Go out and buy us some," and "What will it cost?" are frequently heard once the need for security is recognized. Unfortunately, security is not something you go out and buy, it is something you plan and something you work on — when planning it, when creating it, when living with it.

Security policies are a prerequisite to proper security. They provide direction, they treat all areas necessary for proper security, and, possibly most important, because it is so rarely recognized, they provide a means for consistency. Without direction, completeness, and consistency, security can always be trivially breached. If your security efforts concentrate on securing your servers, yet you do not tell users not to have stick-on notes with their passwords on their monitors, your security policies are deficient; if you require server changes be made only at the server console, yet allow anyone other than duly authorized administrators to make such changes, you have again missed the boat in terms of security policy. And, when networks that are 100% secure in and of themselves can each compromise the others via inconsistencies in their respective security types if they are interconnected (and interconnection has been a hot item for some time), having components with proper security is no longer enough; you must have consistent security set forth in your policies.

Warning: Your policies should fit your operational environment and requirements. It is unlikely that the policies of even a similar organization will be best for you in every area. This does not mean that looking at the policies of other organizations cannot be of help to you — if they are good policies, of course — in terms of suggesting things like the types of areas to be treated, but you need to do what is right for you, not what may or may not have been right for somebody else.

POLICIES
Servers are parts of networks, networks are parts of information-processing structures, and information-processing structures are parts of organizational operations. Although this article deals only with server security policies, all other security areas must be dealt with in an organization's full security policies statement. A single security breach of any type can, and often does, compromise all operations. (If, for example, visitors were allowed to enter a facility unchallenged, and if nodes were left operationa but unattended — during lunch periods or whatever — the best server security policies in the world would readily be defeated.)

The statements of policy set forth below are generic in nature. Not all will apply — even in modified form — to all servers, and many, if not
most, will have to be adapted to specific operations. They are, however, most likely better than those you are likely to get from friends, and should serve as a good start for; and basis of, proper server security policies for your particular situation. For convenience, they are grouped in functional areas.

One area, and possibly the most critical one, will not be covered: the LAN security administrator. Your security cannot be any better than your administrators make and maintain it. You require the best possible personnel, and they must be given the authority, and not just the responsibility, to do whatever is necessary to provide the proper server — and network — security. Too often we see "the Charlie Syndrome": LANs come in, administrators are needed, Charlie is free, so Charlie is made the system administrator. Why is Charlie free? Well, in all honesty, it is because Charlie is not good enough to be given anything worthwhile to do. What this means is that rather than having the best people as system administrators, the worst are too frequently in that position — system administration should not be a part-time assignment for a secretary!

SERVER FUNCTIONS

Access Control

• The server shall be able to require user identification and authentication at times other than log-on.
• Reauthentication shall be required prior to access to critical resources.
• File and directory access rights and privileges should be set in keeping with the sensitivity and uses of the files and directories.
• Users should be granted rights and privileges only on a need-to-know/use basis (and not be given everything except the ones they are known not to need, as is very commonly done).

Encryption

• Sensitive files should be maintained in encrypted form. This includes password files, key files, audit files, confidential data files, etc. Suitable encryption algorithms should be available, and encryption should be able to be designated as automatic, if appropriate.
• For any and every encryption process, cleartext versions of files encrypted must be overwritten immediately after the encryption is complete. This should be made automatic, effectively making it the final step of encryption.

Logging

• Audit logs should be kept of unsuccessful log-on attempts, unauthorized access/operation attempts, suspends and accidental or deliber-
ate disconnects, software and security assignment changes, log-ons/log-offs, other designated activities (e.g., accesses to sensitive files), and, optionally, all activity.

• Audit log entries should consist of at least resource, action, user, date and time, and, optionally, workstation ID and connecting point.

• There should be an automatic audit log review function to examine all postings by posting type (illegal access attempt, access of sensitive data, etc.), and for each posting type. If a transaction threshold (set by the LAN administrator) for any designated operation exception is exceeded, an alarm should be issued and an entry made in an action-item report file.

• The audit file should be maintained in encrypted format.

• There should be reporting functions to provide user profiles and access rules readily and clearly, as well as reports on audit log data.

Disk Utilization

• As appropriate to their sensitivity, ownership, licensing agreements, and other considerations, all programs should be read-only or execute-only, and/or should be kept in read-only or execute-only directories. This should also apply to macro libraries.

• Users should be provided with private directories for storage of their nonsystem files. (These include files that are shared with other users.)

• There should be no uploads of programs to public areas; the same is true for macros and macro libraries.

Backup

• The availability of the LAN should be maintained by the server scheduling and performing regular backups. These backups should provide automatic verification (read-after-write), and should be of both the full and partial (changed items only) varieties. All security features, including encryption, should be in full effect during back-ups.

• Both backups and the restore/recovery functions should be regularly tested.

• Backups should be kept off premises.

• Automatic recovery of the full LAN and of all and individual servers (and workstations) must be available.

Communications

• Communications (i.e., off-LAN) access should be restricted to specific users, programs, data, transaction types, days/dates, and times.

• An extra layer of identification/authentication protocol should be in effect (by challenge-response, additional passwords, etc.) for communications access.
• All communications access should be logged.
• All communications access messages should be authenticated, using message authentication codes (MACs), digital signatures, etc.
• The password change interval should be shorter for communications access users.
• Stronger encryption algorithms should be used for communications access users.
• Any and all confidential information — passwords, data, whatever — should be encrypted during transmission in either or both directions for all communications access activities.
• Encryption capabilities for communications should include both end-to-end and link encryption.

Server Access and Control
• There shall be no remote, i.e., from other than the console, control of any kind of the server, and there shall similarly be no remote execution of server functions.
• All server functions must be done from the console. This specifically excludes access via dial-in, gateways, bridges, routers, protocol converters, PADs, micro-to-mainframe connections, local workstations other than the server console, and the like.
• All administrator operations (e.g., security changes) shall be done from the console.
• Supervisor-level log-on shall not be done at any device other than the console.
• If supervisor-level use of a device other than the console becomes necessary, it shall be done only after a boot/restart using a write-protected boot diskette is certified as “clean” (this implies that such diskettes are readily available, as they should be for even stand-alone PCs), or from tape.
• There shall be no user programs executed at the server by user (i.e., remote or local workstation) initiation.
• There shall be no immediate workstation access to the server or to any server resources following a diskette boot at the server.
• All communication among and between nodes must be done through the server. There shall be no peer-to-peer direct communication.
• There shall be no multiple user IDs (UIDs)/passwords logged on (i.e., the same user on the system more than once at a given time). There should also be the ability to suspend the active user session and/or issue alarms should this situation occur.

General (Node) Access Control
• Both a user ID and a password shall be required by servers for a user as part of logging on.
• The server should be able to identify both the workstation and work-
station connection point at log-on.
• All files (programs and data) and other resources (peripheral equip-
ment, system capabilities) should be able to be protected.
• All resource access should be only on a need-to-know/need-to-use
basis.
• File access control should be at file, directory, and subdirectory levels.
• File access privileges should include read, read-only, write (with sep-
arate add and update levels), execute, execute-only, create, rename,
delete, change access, none.
• Resource access should be assignable on an individual, group, or
public basis.

Passwords
• There should be appropriate minimum (6 is the least, 8 is recom-
mended, more is better) and maximum (at least 64, more is better)
lengths. (Longer “passwords” are usually “pass-phrases,” e.g., “Four
score and 7 years ago.”)
• Passwords should be case sensitive.
• There should be a requirement for at least one uppercase character;
one lowercase character; one numeric, and one alphabetic character to
be used in user-selected passwords. For high-security access, this
should be extended to include one nonprint (and nonspace) character.
• There should be computer-controlled lists of prescribed passwords
to include common words and standard names, and employee/com-
pany information as available (name, address, social security num-
ber; license plate number; date of birth; family member names;
company departments, divisions, projects, locations, etc.). There
should also be algorithms (letter and number sequences, character
repetition, initials, etc.) to determine password weakness.
• Passwords should be changed frequently; quarterly is a minimum —
monthly is better. High security access should have weekly change.
• There should be reuse restrictions so that no user can reuse any of
the more recent passwords previously used. The minimum should be
5, but more is better, and 8 is a suggested minimum.
• There should be no visual indication of password entry, or password
entry requirements. This obviously prohibits the password characters
from echoing on the screen, but also includes echoing of some dum-
my character (normally an asterisk) on a per character basis, or used
to designate maximum field length.
• New passwords should always be entered twice for verification.
• LAN administrators, in addition to their passwords with associated
supervisory privileges, should have an additional password for “nor-
mal” system use without supervisory privileges.
Note: There are password test programs to allow automatic review and acceptance/rejection of passwords. These are usually written in an easily ported language, typically C, and can be readily structured to implement whatever rules the security administrator feels are appropriate. They are used between the password entry function and the password acceptance function already in place, so only proper passwords get used by the system.

Physical Security

- All servers should be as secured as possible in keeping with their sensitivity.
- Servers should be physically secured in locked rooms.
- Access to servers should be restricted to authorized personnel.
- Access to the server area should be automatically logged via use of an electronic lock or other such mechanism as appropriate.
- The room in which the server is kept should be waterproof and fire-proof.
- Walls should extend above the ceiling to the floor above.
- Water sprinklers and other potentially destructive (to computers) devices should not be allowed in the server room.
- The server console should be kept with the server.
- Servers should have key locks.
- Connection points to servers should be secured (and software-disabled when not in use) and regularly inspected.
- All cabling to servers should be concealed whenever possible. Access to cabling should be only by nonpublic avenues.
- All “good” media practices — encryption of sensitive information, storage in secure locations, wiping/overwriting when finished, etc. — should be in full effect.

Legal Considerations

- Programs that by license cannot be copied should be stored in execute-only or, if this is not possible, read-only directories, and should be specifically designated as execute-only or read-only.
- Concurrent use count should be maintained and reviewed for programs licensed for a specific number of concurrent users. There should be a usage threshold above which additional concurrent access is prohibited.
- Access rules should be reviewed for all programs licensed for specific numbers of concurrent users.
- Appropriate banner warnings should be displayed as part of the log-on process prior to making a LAN available for use.
- Appropriate warning screens should be displayed on access attempts to sensitive areas and/or items.
Other

- There shall be no unauthorized or unsupervised use of traffic monitors/recorders, routers, etc.
- There should be a complete formal and tested disaster recovery plan in place for all servers. This should include communications equipment and capabilities in addition to computer hardware and software. (This is, of course, true for full LANs, and for the entire IP operations.)
- There shall be no sensitive information ever sent over lines of any sort in cleartext format.
- Servers should require workstations that can also function as stand-alone PCs to have higher levels of PC security than those PCs that are not connected to a LAN. Workstations that operate in unattended modes, have auto-answer abilities, are external to the LAN location (even if only on another floor), and/or are multiuser should have the highest level of PC security.
- Workstation sessions should be suspended after a period of inactivity (determined by the LAN administrator), and terminated after a further determined period of time has elapsed.
- Explicit session (memory) cleanup activities should be performed after session disconnect, whether the session disconnect was by workstation request (log-off), by server initiative (such as due to inactivity), or accidental (even if only temporary, as might be the case with a line drop).
- In cases where session slippage tends to occur (such as line drops), or in instances where service requests require significant changes of access level privileges, reauthentication should be required.
- Unused user IDs and passwords should be suspended after a period of time specified by the LAN administrator.
- Successful log-ons should display date and time of last log-on and log-off.
- There should be the ability to disable keyboard activity during specified operations.
- The integrity of data should be maintained by utilization of transaction locks on all shared data — both data files and databases.
- The integrity of data and the availability of data and the entire LAN should be maintained by specific protections against viruses and other malicious code.
- All security functions and software changes/additions should be made only from the server and only by the LAN administrator.

**HIGHER-LEVEL SECURITY**

Although the preceding capabilities will be significantly more than most LAN servers would find appropriate, there are still more sophisticated se-
curity features that are appropriate to LANs with high-risk/high-loss profiles. For the sake of completeness, major ones are set forth in the following:

- Access to critical resources should require reauthentication.
- Access to critical resources should not only authenticate the user, but further verify the correctness of the workstation in use, the connection point of that workstation, and the correctness of the day/date/time of the access.
- Message sequence keys should be used to detect missing or misordered messages.
- After a failed log-on attempt, the server should generate an alarm, and be able to simulate a proper log-on for the failed user (to keep this user connected while personnel go to the offending workstation).
- After excessive access violations, the server should generate an alarm, and be able to simulate a continuing session (with dummy data, etc.) for the failed user (to keep this user connected while personnel go to the offending workstation).
- Traffic padding — the filling in of unused transmission bandwidth with dummy pseudo-traffic — should be used to prevent transmission patterns from being readily detected (thereby making it easier to “trap” valid information).
- Multiple — at least two — LAN administrators should be required for all potentially critical server changes. (These might be adding a new user, altering an existing user’s rights and privileges, changing or adding software, and the like.) For example, one administrator could add a user, but only from a list internal to the computer that a second administrator created. This means that any deliberate breach of security by an administrator would require collusion to be effective.
- LAN administrators should have separate passwords for each individual server function they perform, the rights and privileges associated with that password being the minimum necessary to do the specific job for which it is being used.
- The server should be fully compatible with tokens, biometric devices, and other such higher-security access control products and technologies.
- The server should be able to do automatic callback for any and all communications access.
- To improve the availability of the LAN, it should be fault tolerant. Multiple (shadow) servers, disk mirroring, and the like should be in place.
- There should be a file/system integrity product in regular and automatic use to alert the administrator to any and all server changes.
- Sophisticated authentication methodologies should be in place to assure not only the contents of a message/request, but also the source. MACs and digital signatures are viable means to certify contents, and public key/private key (commonly known as RSA-type) encryption provides acceptable source verification.
- Backups should be made to an off-LAN facility. This could be an organizational mainframe, a service bureau, or whatever. With this "store and forward backup," recovery media is immediately away from the server.
- Servers should be compatible with biometric devices (fingerprint, retinal scan, palm print, voice, etc.) for user verification.

CAVEATS
Seat belts, air bags, and other automotive safety devices merely make it less likely that you will be seriously injured in an accident, and certainly do not guarantee your not being involved in one. By the same token, computer security merely lessens the chances your systems will be misused, lessens the likelihood of damages associated with certain common incidents, makes it more likely to discover and limit any misuse and/or damages promptly, and makes it easier to recover from various types of both accident and misuse.

No realistic computer security "can't be beaten," and this certainly includes server security. Proper server security will make networks much more difficult to compromise, and can make it not worth an intruder's time (in terms of anticipated cost to break in versus expected return as a result of a break-in) to even attempt to break into a properly secured network.

With servers viewed as being in the hands of "experts" (which they often are, of course), many, if not most, users rely exclusively on server security for total protection, and do not practice proper security as part of their operations. Server security, and even full network security, is not a substitute for other types of security; your security policies must reflect this.

TEETH
The best policies in the world will fail if they are not enforced. ("Thou shalt not print your password on a stick-on note and post it to your monitor" sounds good, but people still tend to do it — If you don't make sure that they don't, or take proper corrective actions if they do, your policies are little more than a waste of paper.) Your policies should have teeth in them: as appropriate, server, as well as all other security policies, should contain monitoring and enforcement sections.

Because operational environments are often in a virtually continuous state of change — new equipment and users, changing capabilities,
rights and privileges, etc. — you should regularly review your server (and full) security to make sure it continues to be in agreement with your server security policies.

Similarly, untested server security may only be security on paper. Because even the most qualified personnel can make mistakes in creating server security policies and/or in implementing them, your security should be tested to see that it really works as intended and conforms to your server security policies. This should obviously be done when you design/develop/install your security, but should also be done on a reasonable periodic basis (quarterly, yearly, whatever). Such tests are usually done best by outsiders, because truly capable personnel often are not available on staff, and employees often have friends to protect and personal interests in particular operations.

CONCLUSION
LANs have become critical processing elements of many, if not most, organizations of all sizes, and servers are the hearts of LANs. As the frequent repository of highly sensitive, often mission-critical information, proper security is of prime importance. Without proper security policies, security is unlikely to succeed, and policies have to be in place to allow the appropriate security to be designed and installed. Adequate security can be obtained by companies willing to work at it, and the work must start with proper security policies and must continue by seeing that security continues to conform to existing security policies. The key element by far in LAN security is the LAN administrator; for all purposes, and in spite of whatever products you may purchase, the quality of security will be in one-to-one correspondence with the abilities and efforts of this person.

Jon David is an independent consultant with more than 20 years experience in system and network security. He is an expert in Internet and WWW security. His clients include major financial organizations, top Fortune companies, and key government agencies.