AUDIT OF SBA'S UNIX

OPERATING SYSTEMS

AUDIT REPORT NUMBER 1-21

SEPTEMBER 28, 2001

U.S. SMALL BUSINESS ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
WASHINGTON, D.C. 20416

AUDIT REPORT
Issue Date: September 28, 2001
Number: 1-21

To: Lawrence E. Barrett, Chief Information Officer

From: for Robert G. Seabrooks
Assistant Inspector General for Auditing

Subject: Audit of SBA's UNIX Operating Systems

We completed an audit of the Sun Solaris UNIX computer operating systems on [FOIA Ex. 2] servers that host SBA's client/server[1] computer applications. We concluded that security over the UNIX servers was not adequate to protect or detect unauthorized access to Agency programs or data. During our audit, the OCIO corrected many of the configuration and access control issues. Our recommendations are focused on correcting those issues that remain to ensure the security over the UNIX operating systems.

BACKGROUND

SBA's Office of the Chief Information Officer (OCIO) has [Ex. 2] servers with UNIX operating systems that operate [FOIA Ex. 2] client/server based computer applications. The applications include the Surety Bond Guarantee/Preferred Surety Bond System, Field Cashiering System and Asset Sales System. [FOIA Ex. 2].

When configured properly, the UNIX operating system can protect data and programs from unauthorized use. This is done primarily by requiring users to authenticate themselves

[1] Client/server is defined by TechWeb encyclopedia as a computer architecture in which the user's PC (the client) is the requesting computer and the server is the supplying computer, both of which are connected via a local area network or wide area network. In client/server, the client processes the user interface (Windows, Mac, etc.) and can perform some or all of the application processing. Servers range in capacity from high-end PCs to mainframes. A database server maintains the databases and processes requests from the client to extract data from or to update the database. An application server provides additional business processing for the clients.

when logging on with both a user identifier (user ID) and a password. After recognizing a user, UNIX restricts the user's access to data and programs according to permission previously granted by owners of the data and programs. UNIX has a "superuser" account that, by convention, has the username "root." This account has unrestricted access to the entire system, including all data and all programs. Access to root is controlled by a password that must be carefully protected in order to secure data and programs from unauthorized access, use, alteration, or destruction.

OBJECTIVES, SCOPE AND METHODOLOGY

The objectives of the audit were to determine whether the security settings and operational controls for the UNIX operating systems were adequate to prevent or detect unauthorized access to programs and data. We also assessed compliance with applicable provisions of OMB Circular A-130, Appendix III, "Management of Federal Information Resources," and SBA's Standard Operating Procedure (SOP) 90-47, "Automated Information Systems Security."

The scope of the audit was the 13 UNIX servers that provide the development, test and production environments for SBA's client/server applications. The [Ex. 2] UNIX servers that are dedicated to the operation of web server software were not within the scope of this audit. We ran diagnostic and security programs on the UNIX servers and interviewed appropriate SBA personnel at SBA's Central Office in Washington, DC between December 2000 and March 2001. We performed our audit in accordance with Government Auditing Standards.

AUDIT RESULTS

We concluded that the security settings and operational controls over the UNIX operating systems were not adequate to prevent or detect unauthorized access to programs and data, and did not comply with Federal and Agency information security requirements in OMB Circular A-130 and SBA SOP 90-47. As a result, there was an increased risk of unauthorized modification, loss and disclosure of data and programs. This risk is somewhat mitigated due to the fact that there are only about 45 authorized users who can log into the UNIX operating system directly. Additionally, the OCIO corrected many of the configuration and access control issues during the audit. Our recommendations are focused on correcting those issues that remain to ensure the security over the UNIX operating systems.

Finding 1: Identification And Authentication Controls Were Not Adequate To Prevent Or Detect Unauthorized Access

Identification and authentication controls (user IDs and passwords) were not properly implemented to prevent or detect unauthorized access to the UNIX operating systems. This occurred because OCIO had not coordinated the overall installation and configuration of the servers to ensure they posed no security risk. Additionally, the UNIX computer operator who

had operational security responsibilities was not trained in and aware of Agency security requirements. As a result, there was increased risk of unauthorized activities occurring and not being detected.

OMB Circular A-130 requires that agencies ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information. In addition, SOP 90-47 requires that operating system software contain adequate security controls to minimize the likelihood of unauthorized access to or use of system resources. The SOP further requires the OCIO to coordinate the installation and configuration of the system(s) to ensure that they pose no security risk.

The specific aspects of non-conformance with OMB Circular A-130 and SOP 90-47 for identification and authentication controls are noted below.

The password for the root ID had not been changed in the appropriate timeframe

The password for the root ID had not been changed in five months. During that time, two individuals who knew the password for the root ID had retired. Additionally, both of these individuals had active accounts on the firewall and could dial into the UNIX systems remotely. This occurred because the UNIX administrator was not aware of the Agency security requirements in the SOP including the requirement to change the password for the root ID. As a result, unauthorized accesses could have occurred and gone undetected.

SOP 90-47 requires that passwords for root IDs on UNIX operating systems be changed at least once every two months. Passwords should be changed more frequently as conditions warrant.

During the audit, the UNIX computer operator changed the password for root and agreed to change it every two months, or more frequently as conditions warrant.

Some passwords were blank or easily guessed

Using a password "cracker" freely available on the Internet, we identified 57 passwords being utilized by 26 user IDs that did not comply with SBA security requirements for password length and complexity. As a result, a user could more easily masquerade as someone else and make unauthorized changes to SBA client/server applications.

SOP 90-47 requires that passwords must be at least eight characters in length, not be easily guessed combinations, e.g., all zeros, dashes, etc, and not be the same as the user ID.

Some of the inappropriate passwords we identified were as follows:

- Thirty-two passwords were substantially the names of the products or utilities supported by the users of those products, e.g., [FOIA Ex. 2]

- Eleven passwords were the initial password given to the user. Those passwords had not been changed.

- Four passwords were blank. Any individual who knew the user ID for those four accounts could have signed on to the systems as those IDs.

- Ten passwords did not comply with agency regulations regarding password length and complexity.

Numerous user IDs were for personnel who were not currently employed

Thirteen of the 60 existing user IDs were for personnel who were no longer SBA employees or contractors. Six of these 13 IDs had active accounts on the SBA firewall and could be used to dial into the UNIX servers remotely. As a result, there is no guarantee that these IDs were not used for an inappropriate purpose. Additionally, there is no ability to ascertain if other individuals accessed the programs and capabilities of the departed employees or contractors and made unauthorized changes to programs or data.

SOP 90-47 requires that accounts will be suspended as quickly as possible, but no more than three working days from the time the user is no longer authorized access to the computer installation or computer application.

During the audit, all non-current user IDs were suspended in UNIX and on the firewall as soon as it was determined that these IDs were for individuals who no longer worked for SBA.

Automated password controls were not enabled within UNIX

Automated controls within UNIX over password settings were not enabled to ensure security and integrity of the operating system. This occurred because the UNIX operator had not activated the UNIX Administrative Tool features that would enforce password change requirements and user ID suspension called for in SBA SOP 90-47. Additionally, the OCIO had not ensured that the controls called for in the SOP would be included in the system configuration. As a result, aspects of the previous two security weaknesses, easily guessed passwords and user IDs existing for non-current SBA personnel, were not automatically corrected within the system.

SOP 90-47 specifies the following controls relating to password administration: (1) the initial password or a reissued password will be replaced and not reissued, (2) users must be able to change their own passwords and passwords must be set to automatically expire every 90 days, and (3) inactive accounts must be suspended after 120 days of inactivity.

During the audit, the computer operator tested the UNIX Administrative Tool features with his own ID and found that the warning message that a password was about to expire did not

work with the agency's client front-end security software.[2] Therefore, the system would not warn users that their passwords were about to expire. Procedures should, therefore, be developed to notify users that their passwords are about to expire at the 90-day interval as required by SOP 90-47.

Recommendations:

We recommend that the Chief Information Officer:

1A. Ensure that the UNIX computer operators who have operational responsibility for maintaining security for the UNIX systems are trained in agency computer security requirements.

1B. Ensure that the password for the root ID is changed every two months or more frequently as circumstances warrant.

1C. Adopt password maintenance procedures to ensure that the initially assigned passwords for the UNIX systems are changed within a reasonable time frame (three to five workdays) and suspend IDs that are not initially used within 5 days.

1D. Enable security features within the UNIX Administrative Tools to comply with SOP 90-47 regarding forcing the expiration of passwords every 90 days and forcing inactive accounts to be suspended after 120 days of inactivity.

1E. Develop procedures to monitor passwords for SBA general support systems on a periodic basis to ensure compliance with SOP 90-47.

1F. Establish procedures to review the access control lists for the UNIX systems and the firewall and purge the systems of user IDs that are no longer needed.

SBA Management's Response:

The Chief Information Officer agreed with the finding and recommendations.

Finding 2: Remote Login Was Enabled On the Main UNIX Server Making It Easier To Penetrate The System

Enabling the remote login setting (rlogin) within UNIX allowed access to the main UNIX server by means other than approved front-end software. As a result, potential unauthorized access to the server could occur and go undetected.

[2] The approved client front-end security software (1) prevents direct login to the system with the Root ID, (2) limits the number of unsuccessful login attempts, and (3) encrypts communications between the client and server computers.

SBA SOP 90-47 requires that users access client servers through client, front-end software provided and approved by the OCIO. Other access methods are prohibited. When enabled, remote login allows for access to the server without using the client, front-end software approved by the OCIO. When remote login was made known to the UNIX computer operator, the setting was immediately disabled.

Recommendation:

2A. We recommend that the Chief Information Officer periodically review the appropriate UNIX configuration files and ensure that sensitive system privileges and capabilities are set to SBA approved settings for all UNIX servers.

SBA Management's Response:

The Chief Information Officer agreed with the finding and recommendation.

Finding 3: The UNIX Servers Did Not Have Appropriate Management Controls as Prescribed for General Support Systems

The UNIX servers processing client/server applications did not have an adequate security plan, an individual formally assigned security duties and authorization to process information as prescribed for general support systems as per OMB Circular A-130. As a result, the UNIX servers did not have the underlying security foundation work needed to identify the security weaknesses that had been noted in this report.

SBA had included the UNIX Servers in a different security plan and accreditation package. The other security plan covered other SBA systems, but did not address the major applications that process on the UNIX servers, nor the protection and security requirements for the 40 plus users of the system. The security plan also did not specifically designate the responsible security official for the UNIX servers. Since the UNIX servers processing client/server applications are a separate general support system, there was not a correct authorization to process information on the UNIX servers.

Recommendations:

We recommend that the Chief Information Officer:

3A. Create the required security plan and documentation for the UNIX servers as separate general support systems processing major applications.

3B. Formally assign security duties for the UNIX systems to an appropriate individual.

3C. Approve or authorize the UNIX systems to operate as separate general support systems processing major applications.

SBA Management's Response:

The Chief Information Officer agreed with the finding and recommendations.

Finding 4: UNIX Operating System Patches Were Not Up-To-Date

The UNIX servers had not been kept up-to-date with the latest security patches and recommended configuration settings as provided by the manufacturer. As a result, the servers may have been more vulnerable than what would have occurred if the systems had been patched as recommended by the manufacturer.

OMB Circular A-130 provides that "adequate security" means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls. Since Sun Solaris UNIX patches come free with the systems, implementing these patches provides cost-effective security products and techniques.

During the audit, a program from the manufacturer was run that analyzed the current patch level on three of the [Ex. 2] UNIX platforms. The tool identified many security and operational patches that had not been installed. According to computer operator staff, this was due to the philosophy that patches would be installed only if there was a compelling need for them (security or issues that directly affected the applications and [Ex. 2]. As the audit progressed, the computer operator updated one of the test environments with the manufacturers recommended "bundle patch" (a collection of all current patches for the system). The bundle patch had not encountered any problems in the test environment and the computer operator was awaiting approval to install the bundle patch on the remaining servers.

During the audit, a program from the manufacturer was also run that determined whether certain system configuration settings were optimized for secure operations. The manufacturer had identified potential weaknesses to the default settings for UNIX and recommended installing a program to update the operating system each time the system is restarted. As the audit progressed, the UNIX computer operator modified the operating system to update the system configuration file on all [Ex. 2] UNIX servers during system restarts.

Recommendation:

4A. We recommend that the Chief Information Officer review the UNIX servers and implement appropriate patches on all servers. Additionally, we recommend that in the future OCIO develop procedures to review the servers and verify that all appropriate patches are timely installed.

SBA Management's Response:

The Chief Information Officer agreed that security patches for the [Ex. 2] servers were not always up to date. He was concerned, however, that implementing a bundle patch on the UNIX servers could cause unintended consequences to the operational environments. Certain patches may not work correctly with SBA installed programs or utilities. The CIO agreed to review the current patch configuration for the UNIX servers to ensure that all necessary patches are currently installed. Additionally, the OCIO will develop procedures to periodically review the patch configuration levels to ensure that all future patches are timely installed on SBA systems.

OIG Evaluation of Management's Response:

We agree with the Chief Information Officer's comments and have modified the recommendation accordingly.

Finding 5: Monitoring "Switch-user" Logs

UNIX has a switch-user command (SU) that allows a user, who is logged on to the system, to log in again under another ID (account). When outside of the console room, secure front-end software is configured to require logging (recording) of user attempts to switch-user. Thus all logins through the switch-user command are recorded (logged) in a switch-user file. This file (log) should be reviewed periodically by appropriate personnel to identify unauthorized user attempts to switch to root or other highly privileged user IDs.

The groups at OCIO that should have monitored the switch-user logs for suspicious behavior did not review those logs and validate appropriate login attempts. This occurred because the logs for the command were periodically monitored by the UNIX computer operators, but not shared with the DBMS programming group and the OCIO Security group. As a result, there was no oversight by the groups who would be most interested in users logging into the servers with IDs that those individuals were not authorized to use.

Recommendation:

5A. We recommend that the Chief Information Officer create copies of the switch-user logs and have those logs reviewed weekly by the DBMS Team Leader and the OCIO Security group. The DBMS Team Leader and OCIO Security should review and validate the appropriateness of the logins using the switch-user logs.

SBA Management's Response:

The Chief Information Officer agreed with the finding and recommendation.

*** * ***

The findings included in this report are the conclusions of the Office of Inspector General's Auditing Division. The findings and recommendations are subject to review, management decision, and corrective action by your office in accordance with existing Agency procedures for audit follow-up and resolution.

Please provide us your management decision for each recommendation within 30 days. Your management decisions should be recorded on the attached SBA Forms 1824, "Recommendation Action Sheet," and show either your proposed corrective action and target date for completion, or explanation of your disagreement with our recommendations.

This report may contain proprietary information subject to the provisions of 18 USC 1905. Do not release to the public or another agency without permission of the Office of Inspector General.

Should you or your staff have any questions, please contact Robert G. Hultberg, Director, Business Development Programs Group at (202) 205-7577.

Attachment

Attachment 1

REPORT DISTRIBUTION

Recipient	Number of Copies
Associate Deputy Administrator for Management and Administration	1
General Counsel	2
General Accounting Office	1
Chief Financial Officer Attention: Jeff Brown	1