

Ohio University

Security Standard for General Information Systems

A Standard for the Configuration and Operation of Information Systems at Ohio
University

System Security Working Group
10/24/2008

TABLE OF CONTENTS

Introduction.....	3
3 Levels of Standard	3
Patching.....	4
Server Deployment.....	4
Remove, Restrict or Disable Unnecessary or Unused Services, Applications, and Network Protocols.....	5
Configure OS User Authentication.....	6
Configure Resource Controls Appropriately (File permissions, network shares, etc)	8
Install and Configure Additional Security Controls.....	8
Securely Installing the Server Software	9
Configuring Access Controls	10
Server Resource Constraints.....	11
Selecting and Implementing Authentication and Encryption Technologies.....	12
Maintaining the Security of the Server.....	12
Server Backup Procedures	13
Security Scanning.....	13
Remotely Administering a Server	13

October 24, 2008

INTRODUCTION

In order to set a baseline for how systems should be configured when attached to the Ohio University Network, a working group was established in August of 2008 for the purpose of developing a standard to which all systems should comply. This working group had a membership roster that included:

- Kapil Bajaj
- Jay Beam
- Doug Bowie
- Donner Davis
- Matthew Dalton
- Mike Elliot
- Chris Hayes
- Steve Hoffer
- Sunil Narasimhan
- Paul Schmittauer
- Ron Yoakem

After reviewing several of the standards in existence, the group took the NIST 800-123 Guide to General Server Security (<http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf>) as their template and modified it to more closely meet the environment of Ohio University. In all cases, the group attempted to stay true to the following security concepts:

- Defense in Depth – Simply stated, good security doesn't rely on only one level of protection
- Principle of Least Privilege – An individual, process or system should only have the minimum amount of rights, access or privilege required to get the job done.
- Less is More – A system should only contain, or have running those files and functions necessary to get the job done – nothing more, nothing less.

3 LEVELS OF STANDARD

One change that the working group made to the standard was the recognition that not all systems are the same. Toward that end, the standard has been broken into three levels. The standard is cumulative – i.e. Moderate systems have to comply to both Moderate and Minimum, while Maximum must comply to all three.

Minimum	Minimum Standards apply to all general purpose computer environments (i.e. Windows, Mac, Linux, BSD, etc.)
Moderate	All Servers are at least Moderate, and servers containing confidential data must meet the maximum requirement.
Maximum	Maximum is required regardless of whether the system is "production" if it contains sensitive data.

October 24, 2008

PATCHING

Minimum	<ul style="list-style-type: none"> • Create, document, and implement a patching process. (may be accomplished through WSUS, GPO, or auto patching) • Install permanent fixes (patches, upgrades, etc.) (see previous bullet)
Moderate	<ul style="list-style-type: none"> • Identify vulnerabilities and applicable patches. (unless automated)
Maximum	<ul style="list-style-type: none"> • Mitigate vulnerabilities temporarily if needed and if feasible (until patches are available, tested, and installed). (depending on exploit available, or difficulty of the fix)

SERVER DEPLOYMENT

Minimum	
Moderate	<ul style="list-style-type: none"> • Keep the servers disconnected from networks or connect them only to an isolated "build" network until all patches have been transferred to the servers through out-of-band means (e.g., CDs) and installed, and the other configuration steps listed in this section have been performed. (Moderate) • Place the servers on a virtual local area network (VLAN) or other network segment that severely restricts what actions the hosts on it can perform and what communications can reach the hosts---only allowing those events that are necessary for patching and configuring the hosts. Do not transfer the hosts to regular network segments until all the configuration steps listed in this section have been performed
Maximum	<ul style="list-style-type: none"> • Administrators should generally not apply patches to production servers without first testing them on another identically configured server

October 24, 2008

REMOVE, RESTRICT OR DISABLE UNNECESSARY OR UNUSED SERVICES, APPLICATIONS, AND NETWORK PROTOCOLS

For the following section, if any of the public services listed below are enabled, the system is at least Moderate.

Minimum	
Moderate	<ul style="list-style-type: none"> • Public Services <ul style="list-style-type: none"> ○ Directory services (e.g., Lightweight Directory Access Protocol [LDAP], Network Information System [NIS]) ○ Web servers and services ○ Email services (e.g., SMTP) ○ System and network management tools and utilities, including Simple Network Management Protocol (SNMP) ○ Remote control and remote access programs, particularly those that do not strongly encrypt their communications (e.g., Telnet) • File and printer sharing services (e.g., Windows Network Basic Input/Output System [NetBIOS] file and printer sharing, Network File System [NFS], FTP) • Wireless networking services (unless currently in use) • Bluetooth, infrared
Maximum	<ul style="list-style-type: none"> • Language compilers and libraries (Off if production) • System development tools (Off if production)

October 24, 2008

CONFIGURE OS USER AUTHENTICATION

Minimum	<ul style="list-style-type: none"> • Remove or Disable Unneeded Default Accounts---The default configuration of the OS often includes guest accounts (with and without passwords), administrator or root level accounts, and accounts associated with local and network services. The names and passwords for those accounts are well known. Remove (whenever possible) or disable unnecessary accounts to eliminate their use by attackers, including guest accounts on computers containing sensitive information. For default accounts that need to be retained, including guest accounts, severely restrict access to the accounts, including changing the names (where possible and particularly for administrator or root level accounts) and passwords to be consistent with the organizational password policy. Default account names and passwords are commonly known in the attacker community. (Minimum) • Disable Non-Interactive Accounts---Disable accounts (and the associated passwords) that need to exist but do not require an interactive login. For Unix systems, disable the login shell or provide a login shell with NULL functionality (e.g., /bin/false). (Minimum) • Create the User Groups---Assign users to the appropriate groups. Then assign rights to the groups, as documented in the deployment plan. This approach is preferable to assigning rights to individual users, which becomes unwieldy with large numbers of users. (Minimum) • Create the User Accounts---The deployment plan identifies who will be authorized to use each computer and its services. Create only the necessary accounts. Permit the use of shared accounts only when no viable alternatives exist. Have ordinary user accounts for server administrators that are also users of the server. (Minimum) • Configure Automated Time Synchronization---Some authentication protocols, such as Kerberos, will not function if the time differential between the client host and the authenticating server is significant, so servers using such protocols should be configured to automatically synchronize system time with a reliable time server. Typically the time server is internal to the organization and uses the Network Time Protocol (NTP) for synchronization; publicly available NTP servers are also available on the Internet. (Minimum) • Check the Organization's Password Policy---Set account passwords appropriately. Elements that may be addressed in a password policy include the following: (Minimum - Use highest level of enforcement that the system supports) <ul style="list-style-type: none"> ○ Length---a minimum length for passwords. ○ Complexity---the mix of characters required. An example is requiring passwords to contain uppercase letters, lowercase letters, and nonalphanumeric characters, and to
---------	--

October 24, 2008

	<p>not contain "dictionary" words.</p> <ul style="list-style-type: none"> ○ Aging---how long a password may remain unchanged. Many policies require users and administrators to change their passwords periodically. In such cases, the frequency should be determined by the enforced length and complexity of the password, the sensitivity of the information protected, and the exposure level of passwords. If aging is required, consideration should be given to enforcing a minimum aging duration to prevent users from rapidly cycling through password changes to clear out their password history and bypass reuse restrictions. ○ Reuse---whether a password may be reused. Some users try to defeat a password aging requirement by changing the password to one they have used previously. If reuse is prohibited by policy, it is beneficial, if possible, to ensure that users cannot change their passwords by merely appending characters to the beginning or end of their original passwords (e.g., original password was "mysecret" and is changed to "1mysecret" or "mysecret1"). ○ Authority---who is allowed to change or reset passwords and what sort of proof is required before initiating any changes. ○ Password Security---how passwords should be secured, such as not storing passwords unencrypted on the server, and requiring administrators to use different passwords for their server administration accounts than their other administration accounts. ○ Configure Computers to Prevent Password Guessing---It is relatively easy for an unauthorized user to try to gain access to a computer by using automated software tools that attempt all passwords. If the OS provides the capability, configure it to increase the period between login attempts with each unsuccessful attempt. If that is not possible, the alternative is to deny login after a limited number of failed attempts (e.g., three). Typically, the account is "locked out" for a period of time (such as 30 minutes) or until a user with appropriate authority reactivates it
Moderate	
Maximum	<ul style="list-style-type: none"> ● Install and Configure Other Security Mechanisms to Strengthen Authentication

October 24, 2008

CONFIGURE RESOURCE CONTROLS APPROPRIATELY (FILE PERMISSIONS, NETWORK SHARES, ETC)

Minimum	
Moderate	<ul style="list-style-type: none"> • Permit access to only required files (e.g. users shouldn't be allowed to access system mmc controls or other users' files) (Moderate) • Isolate service users to virtual environments (e.g. chroot 'jails') (Moderate)
Maximum	

INSTALL AND CONFIGURE ADDITIONAL SECURITY CONTROLS

Minimum	<ul style="list-style-type: none"> • Anti-malware software, such as antivirus software, anti-spyware software, and rootkit detectors, to protect the local OS from malware and to detect and eradicate any infections that occur. Examples of when anti-malware software would be helpful include a system administrator bringing infected media to the server and a network service worm contacting the server and infecting it. (as it applies) • Host-based firewalls, to protect the server from unauthorized access. (Minimum if it can support) • Periodic security testing of the OS is a vital way to identify vulnerabilities and to ensure that the existing security precautions are effective and that security controls are configured properly
Moderate	

October 24, 2008

Maximum	<ul style="list-style-type: none"> • Host-based intrusion detection and prevention software (IDPS), to detect attacks performed against the server, including DoS attacks. For example, one form of host-based IDPS, file integrity checking software, can identify changes to critical system files. • Network based firewalls should be configured as additional protection • Patch, Package and Configuration management or vulnerability management software to ensure that vulnerabilities are addressed promptly. Patch management and vulnerability management software can be used only to apply patches or also to identify new vulnerabilities in the server's OSs, services, and applications. (above and beyond WSUS, yum, up2date) (Altiris, BigFix, ZenWorks, etc.) • Disk Encryption technologies (and Portable - as possible)
---------	---

SECURELY INSTALLING THE SERVER SOFTWARE

Minimum	<ul style="list-style-type: none"> • Apply any patches or upgrades to correct for known critical vulnerabilities in the server software (i.e. Apache, IIS, Oracle, MS-SQL, Cold Fusion, etc.)
Moderate	<ul style="list-style-type: none"> • Install the server software either on a dedicated host or on a dedicated guest OS if virtualization is being employed. (Single network service/role per server - Web, database, DNS, smtp, etc.) • Apply any patches or upgrades to correct for known vulnerabilities in the server software (i.e. Apache, IIS, Oracle, MS-SQL, Cold Fusion, etc.) • Create a dedicated physical disk or logical partition (separate from OS and server application) for server data, if applicable. • Remove or disable all services installed by the server application but not required (e.g., gopher, FTP, HTTP, remote administration). • Remove or disable all unneeded default user accounts created by the server installation. • Remove all example or test files from the server, including sample content, scripts, and executable code (for production) • Remove all unneeded compilers. • Reduce the permissions that a service account has to only those required.

October 24, 2008

	<ul style="list-style-type: none"> • Apply the appropriate security template or hardening script to the server. • For external-facing servers, reconfigure service banners not to report the server and OS type and version, if possible. • Configure warning banners for all services that support such banners. • Configure each network service to listen for client connections on only the necessary TCP and UDP ports, if possible.
Maximum	<ul style="list-style-type: none"> • Remove all manufacturers' documentation from the server.

CONFIGURING ACCESS CONTROLS

Minimum	
Moderate	<ul style="list-style-type: none"> • Limit the access of the server application to a subset of computational resources. (If Possible/feasible - can be accomplished through virtualization, but not easy in many modern OSs) • Limit the access of users through additional access controls enforced by the server, where more detailed levels of access control are required. • Typical files to which access should be controlled are as follows: <ul style="list-style-type: none"> ○ Application software and configuration files ○ Files related directly to security mechanisms: <ul style="list-style-type: none"> ▪ Password hash files and other files used in authentication ▪ Files containing authorization information used in controlling access ▪ Cryptographic key material used in confidentiality, integrity, and non-repudiation services ○ Server log and system audit files ○ System software and configuration files ○ Server content files

October 24, 2008

	<ul style="list-style-type: none"> • Service processes are configured to run as a user with a strictly limited set of privileges (i.e., not running as root, administrator, or equivalent). • Service processes can only write to server content files and directories if necessary. • Temporary files created by the server software are restricted to a specified and appropriately protected subdirectory (if possible). Access to these temporary files is limited to the server processes that created the files (if possible).
Maximum	

SERVER RESOURCE CONSTRAINTS

Minimum	
Moderate	<ul style="list-style-type: none"> • Installing server content on a different hard drive or logical partition than the OS and server software. Placing a limit on the amount of hard drive space that is dedicated for uploads, if uploads to the server are allowed. Ideally, uploads should be placed on a separate partition to provide stronger assurance that the hard drive limit cannot be exceeded. • If user uploads are allowed to the server, ensuring that these files are not published by the server until after some automated or manual review process is used to screen them. This measure prevents the server from being used to propagate malware or traffic pirated software, attack tools, pornography, etc. It is also possible to limit the size of each uploaded file, which could limit the potential effects of a DoS attack involving uploading many large files. • Ensuring that log files are stored in a location that is sized appropriately. Ideally, log files should be stored on a separate partition. If an attack causes the size of the log files to increase beyond acceptable limits, a physical partition helps ensure the server has enough resources to handle the situation appropriately. • Configuring the maximum number of server processes and/or network connections that the server should allow.
Maximum	

October 24, 2008

SELECTING AND IMPLEMENTING AUTHENTICATION AND ENCRYPTION TECHNOLOGIES

Minimum	<ul style="list-style-type: none"> Systems should employ encryption technologies when transmitting or storing sensitive information and authentication credentials.
Moderate	<ul style="list-style-type: none"> Systems should authenticate to a central system, such as OIT AD to allow access to non-public resources
Maximum	

MAINTAINING THE SECURITY OF THE SERVER

Minimum	
Moderate	<ul style="list-style-type: none"> Logging <ul style="list-style-type: none"> Identifying Logging Capabilities and Requirements <ul style="list-style-type: none"> Logs should capture successful and failed authentication attempts If possible, logs should capture privileged use attempts Logs should capture account management activities Logs should capture, as much as possible, system configuration changes, schema changes, or state changes Reviewing and Retaining Log Files <ul style="list-style-type: none"> Log files should be retained for at least one year Log files should be reviewed weekly for anomalies
Maximum	<ul style="list-style-type: none"> Log files should be reviewed through the University's Security Information and Event Manager (SIEM)

October 24, 2008

SERVER BACKUP PROCEDURES

Minimum	<ul style="list-style-type: none"> • Backup media should be protected from theft and/or disclosure at the same level as the system itself (physical, encryption, etc.)
Moderate	<ul style="list-style-type: none"> • Minimum of Differential backups should occur at least nightly • Full Backups should occur at least twice a Month • Backup recovery testing should be performed at least twice a year • Backups should be maintained in a separate physical location/building from the system itself. • Recommend at least 3 full backups be kept, but environment may dictate differently
Maximum	<ul style="list-style-type: none"> • Full Backup recovery test should be performed at least twice a year

SECURITY SCANNING

These services will be performed by the University Information Security Office

Minimum	<ul style="list-style-type: none"> • Systems should be scanned for common external vulnerabilities quarterly, or as new, significant vulnerabilities are discovered <ul style="list-style-type: none"> ○ Some findings may result in the immediate removal of the system from the network until remediation is performed
Moderate	<ul style="list-style-type: none"> • The results of these scans need to be addressed within one week of them being provided to the administrator of the system
Maximum	<ul style="list-style-type: none"> • Penetration testing should be performed on an annual basis

Note: Some operating systems have self remediation tools such as the Microsoft Baseline Security Analyzer, that allow a user or administrator to assess some of the security of their system. Although not required, these are helpful to determine what may need to be performed on a system prior to, or between scans.

REMOTELY ADMINISTERING A SERVER

October 24, 2008

Minimum	<ul style="list-style-type: none"> • Restrict which hosts can be used to remotely administer the server. (minimum) • Restrict by authorized users (minimum) <ul style="list-style-type: none"> ○ Restrict by IP address (not hostname) (minimum) ○ Restrict to hosts on the internal network or those using the organization's enterprise remote access solution. (minimum) ○ Use secure protocols that can provide encryption of both passwords and data (e.g., SSH, HTTPS); do not use less secure protocols (e.g., telnet, FTP, NFS, HTTP) unless absolutely required and tunneled over an encrypted protocol, such as SSH, SSL, or IPsec. (minimum) • Enforce the concept of least privilege on remote administration (e.g., attempt to minimize the access rights for the remote administration accounts). (minimum) • Do not allow remote administration from the Internet through the firewall unless accomplished via strong mechanisms, such as VPNs. (minimum) • Use remote administration protocols that support server authentication to prevent man-in-the-middle attacks. (minimum) • Change any default accounts or passwords for the remote administration utility or application. (minimum)
Moderate	<ul style="list-style-type: none"> • Use a strong authentication mechanism (e.g., public/private key pair, two-factor authentication).
Maximum	