Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Australian Government Information Security Manual

JUNE 2021

Guidelines for System Hardening

Operating system hardening

Standard Operating Environments

Allowing users to setup, configure and maintain their own workstations or servers can create an inconsistent environment where particular workstations or servers are more vulnerable than others. This type of environment can easily allow an adversary to gain an initial foothold on a network. A Standard Operating Environment (SOE) is a standardised implementation of an operation system and applications and is designed to ensure a consistent and secure baseline.

When SOEs are obtained from third parties, such as service providers, there are additional supply chain risks that should be considered, such as the accidental or deliberate inclusion of malicious content or configurations. To reduce the likelihood of such occurrences, organisations should not only obtain their SOEs from trusted sources but also scan them before use to ensure their integrity.

As the configuration of operating environments will naturally change over time (e.g. patches are applied, configurations are changed, and applications are added or removed) it is essential that SOEs are reviewed and updated at least annually to ensure that an updated baseline is maintained.

Security Control: 1406; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS
SOEs are used for workstations and servers.

Security Control: 1608; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
SOEs provided by third parties are scanned for malicious content and configurations before being used.

Security Control: 1588; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
SOEs are reviewed and updated at least annually.

Operating system versions

Newer versions of operating systems often introduce improvements in security functionality over older versions. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older versions of operating systems, especially those no longer supported by vendors, exposes organisations to exploitation techniques that have since been mitigated in newer versions of operating systems.

The x64 (64-bit) versions of Microsoft Windows include additional security functionality that the x86 (32-bit) versions lack. Using x86 (32-bit) versions of Microsoft Windows exposes organisations to exploitation techniques mitigated by x64 (64-bit) versions of Microsoft Windows.

Security Control: 1407; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
The latest version (N), or N-1 version, of an operating system is used for SOEs.

Security Control: 1408; Revision: 3; Updated: Sep-18; Applicability: O, P, S, TS
When developing a Microsoft Windows SOE, the 64-bit version of the operating system is used.

Operating system configuration

When operating systems are deployed in their default state it can easily lead to an unsafe operating environment allowing an adversary to gain an initial foothold on a network. Many options exist within operating systems to allow them to be configured in a secure state to minimise this security risk. The Australian Cyber Security Centre (ACSC) produces guidance to assist in securely configuring various operating systems.

Security Control: 1409; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
ACSC and vendor guidance is implemented to assist in hardening the configuration of operating systems.

Security Control: 0383; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
Default operating system accounts are disabled, renamed or have their passphrase changed.

Security Control: 0380; Revision: 7; Updated: Sep-18; Applicability: O, P, S, TS
Unneeded operating system accounts, software, components, services and functionality are removed or disabled.

Security Control: 1584; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Standard users are prevented from bypassing, disabling or modifying security functionality of operating systems.

Security Control: 1491; Revision: 1; Updated: Oct-20; Applicability: O, P, S, TS
Standard users are prevented from running script execution engines in Microsoft Windows, including:

- *Windows Script Host (cscript.exe and wscript.exe)*
- *PowerShell (powershell.exe, powershell_ise.exe and pwsh.exe)*
- *Command Prompt (cmd.exe)*
- *Windows Management Instrumentation (wmic.exe)*
- *Microsoft HTML Application Host (mshta.exe).*

Local administrator accounts

When local administrator accounts are used with common account names and passphrases, it can allow an adversary that compromises these credentials on one workstation or server to easily transfer across a network to other workstations or servers.

Security Control: 1410; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Local administrator accounts are disabled; alternatively, passphrases that are random and unique for each device's local administrator account are used.

Security Control: 1469; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
Unique domain accounts with local administrative privileges, but without domain administrative privileges, are used for workstation and server management.

Application management

While the ability to install any application may be a business requirement for users, this privilege can be exploited by an adversary who can email a malicious application, or host it on a compromised website, and use social engineering techniques to convince users into installing it. Even if privileged access is required to install applications, users will often use their privileged access if they believe, or can be convinced that, the requirement to install the application is legitimate. Additionally, if applications are configured to install using elevated privileges, an adversary can exploit this

by creating a Windows Installer installation package to create a new account that belongs to the local administrators group. One way to manage this security risk is to allow users to install vetted and approved applications from organisation-managed software repositories or from trusted application marketplaces.

Security Control: 1592; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Users do not have the ability to install unapproved software.

Security Control: 0382; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
Users do not have the ability to uninstall or disable approved software.

Application control

An adversary can email malicious code, or host malicious code on a compromised website, and use social engineering techniques to convince users into executing it. Such malicious code often aims to exploit security vulnerabilities in existing applications and does not need to be installed to be successful. Application control can be an extremely effective mechanism in not only preventing malicious code from executing, but also ensuring only approved applications can be installed.

When developing application control rules, defining a list of approved executables (e.g. .exe and .com files), software libraries (e.g. .dll and.ocx files), scripts (e.g. .ps1, .bat, .cmd, .vbs and .js files) and installers (e.g. .msi, .msp and .mst files) from scratch is a more secure method than relying on a list of those currently residing on a workstation or server. Furthermore, it is preferable that organisations define their own approved list of executables, software libraries, scripts and installers rather than relying on lists from application control vendors.

Security Control: 0843; Revision: 8; Updated: Apr-20; Applicability: O, P, S, TS
Application control is implemented on all workstations to restrict the execution of executables, software libraries, scripts and installers to an approved set.

Security Control: 1490; Revision: 2; Updated: Apr-20; Applicability: O, P, S, TS
Application control is implemented on all servers to restrict the execution of executables, software libraries, scripts and installers to an approved set.

Security Control: 0955; Revision: 6; Updated: Apr-20; Applicability: O, P, S, TS
Application control is implemented using cryptographic hash rules, publisher certificate rules or path rules.

Security Control: 1582; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Cryptographic hash rules, publisher certificate rules and path rules used for application control are validated at least annually.

Security Control: 1471; Revision: 2; Updated: Apr-20; Applicability: O, P, S, TS
When implementing application control using publisher certificate rules, both publisher names and product names are used.

Security Control: 1392; Revision: 2; Updated: Apr-20; Applicability: O, P, S, TS
When implementing application control using path rules, file system permissions are configured to prevent unauthorised modification of folder and file permissions, folder contents (including adding new files) and individual files that are approved to execute.

Security Control: 1544; Revision: 1; Updated: Apr-20; Applicability: O, P, S, TS
Microsoft's latest recommended block rules are implemented to prevent application control bypasses.

Security Control: 0846; Revision: 7; Updated: Apr-20; Applicability: O, P, S, TS
All users (with the exception of privileged users when performing specific administrative activities) cannot disable, bypass or be exempted from application control.

Security Control: 0957; Revision: 7; Updated: Jun-21; Applicability: O, P, S, TS
Application control is configured to generate event logs for failed execution attempts, including the name of the blocked file, the date/time stamp and the username of the user attempting to execute the file.

Enhanced Mitigation Experience Toolkit and exploit protection

An adversary who develops exploits for Microsoft Windows will be more successful in exploiting security vulnerabilities when Microsoft's Enhanced Mitigation Experience Toolkit (EMET) has not been installed. EMET was designed to provide a number of system-wide mitigation measures while also providing application-specific mitigation measures. From Microsoft Windows 10 version 1709 and Microsoft Windows Server 2016 onwards, EMET functionality has been incorporated directly into the operating system as part of exploit protection functionality.

Security Control: 1414; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
If supported, the latest version of Microsoft's EMET is implemented on workstations and servers and configured with both operating system mitigation measures and application-specific mitigation measures.

Security Control: 1492; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
If supported, Microsoft's exploit protection functionality is implemented on workstations and servers.

PowerShell

PowerShell is a powerful scripting language developed by Microsoft to provide an integrated interface for automated system administration, and is an important part of system administrator toolkits due to its ubiquity and the ease with which it can be used to fully control Microsoft Windows environments. However, it is also a dangerous exploitation tool in the hands of an adversary. In order to prevent attacks leveraging security vulnerabilities in earlier PowerShell versions, PowerShell 2.0 and below should be removed from operating systems. Additionally, PowerShell's language mode should be set to Constrained Language Mode to achieve a balance between functionality and security. Finally, logging functionality available in PowerShell, such as module logging, script block logging and transcription, can provide invaluable information for incident responders following cyber security incidents that involved PowerShell being used for malicious purposes.

Security Control: 1621; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
PowerShell 2.0 and below is removed from operating systems.

Security Control: 1622; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
PowerShell is configured to use Constrained Language Mode.

Security Control: 1623; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
PowerShell is configured to use module logging, script block logging and transcription functionality.

Security Control: 1624; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
PowerShell script block logs are protected by Protected Event Logging functionality.

Host-based Intrusion Prevention System

Many endpoint security solutions rely on signatures to detect malicious code. This approach is only effective when a particular piece of malicious code has already been profiled and signatures are current. Unfortunately, an adversary can create variants of known malicious code, or develop new unseen malicious code, to bypass traditional signature-based detection mechanisms. A Host-based Intrusion Prevention System (HIPS) can use behaviour-based detection schemes to assist in identifying and blocking anomalous behaviour, such as process injection, keystroke logging, driver loading and call hooking, as well as detecting malicious code that has yet to be identified by antivirus vendors.

Security Control: 1341; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
A HIPS is implemented on workstations.

Security Control: 1034; Revision: 6; Updated: Sep-18; Applicability: O, P, S, TS
A HIPS is implemented on high value servers such as authentication servers, Domain Name System (DNS) servers, web servers, file servers and email servers.

Software firewall

Network firewalls often fail to prevent the propagation of malicious code on a network, or an adversary from extracting important data, as they generally only control which ports or protocols can be used between different network segments. Many forms of malicious code are designed specifically to take advantage of this by using common protocols such as Hypertext Transfer Protocol, Hypertext Transfer Protocol Secure, Simple Mail Transfer Protocol and DNS. Software firewalls are more effective than network firewalls as they can control which applications and services can communicate to and from workstations and servers. The in-built Windows firewall should be used to control both inbound and outbound traffic for specific applications.

Security Control: 1416; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
A software firewall is implemented on workstations and servers to limit both inbound and outbound network connections.

Antivirus software

When vendors develop software they may not use secure coding practices. An adversary can take advantage of this by developing malicious code to exploit security vulnerabilities that have not been detected and remedied. As significant time and effort is often involved in developing functioning and reliable exploits, an adversary will often reuse their exploits as much as possible. While exploits may be profiled by antivirus vendors, they often remain a viable intrusion method in organisations that do not have any measures in place to detect them.

Security Control: 1417; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Antivirus software is implemented on workstations and servers and configured with:

- *signature-based detection enabled and set to a high level*
- *heuristic-based detection enabled and set to a high level*
- *detection signatures checked for currency and updated on at least a daily basis*
- *automatic and regular scanning configured for all fixed disks and removable media.*

Security Control: 1390; Revision: 2; Updated: Sep-18; Applicability: O, P
Antivirus software has reputation rating functionality enabled.

Device access control software

The use of device access control software to prevent the connection of unauthorised devices (e.g. unapproved smartphones, tablets, Bluetooth devices, wireless devices, 4G/5G dongles) to workstations and servers, via external interfaces such as USB ports, adds value as part of a defence-in-depth approach to the protection of workstations and servers.

It has also been demonstrated that an adversary can connect devices to locked workstations and servers via an external interface that allows Direct Memory Access (DMA), and subsequently gain access to encryption keys in memory. Furthermore, an adversary can read or write any content to memory that they desire. The best defence against this security vulnerability is to disable access to external interfaces that allow DMA. External interfaces that allow DMA include FireWire, ExpressCard and Thunderbolt.

Security Control: 1418; Revision: 2; Updated: Sep-20; Applicability: O, P, S, TS
Device access control software is implemented on workstations and servers to prevent unauthorised devices from being connected.

Security Control: 0345; Revision: 5; Updated: Sep-20; Applicability: O, P, S, TS
External interfaces of workstations and servers that allow DMA are disabled.

Further information

Further information on authenticating users can be found in the authentication hardening section of these guidelines.

Further information on the use of removable media with systems can be found in the media usage section of the ***Guidelines for Media***.

Further information on patching operating systems can be found in the system patching section of the ***Guidelines for System Management***.

Further information on logging and auditing of operating system events can be found in the event logging and auditing section of the ***Guidelines for System Monitoring***.

Further information on securely configuring Microsoft Windows operating systems can be found in the following ACSC publications:

- ***Hardening Microsoft Windows 8.1 Workstations*** at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-81-workstations
- ***Hardening Microsoft Windows 10 version 1909 Workstations*** at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-windows-10-version-1909-workstations.

Further information on end of support for Microsoft Windows operating systems can be found in the following ACSC publications:

- ***End of Support for Microsoft Windows 7*** at https://www.cyber.gov.au/acsc/view-all-content/publications/end-support-microsoft-windows-7
- ***End of Support for Microsoft Windows 10*** at https://www.cyber.gov.au/acsc/view-all-content/publications/end-support-microsoft-windows-10
- ***End of Support for Microsoft Windows Server 2008 and Windows Server 2008 R2*** at https://www.cyber.gov.au/acsc/view-all-content/publications/end-support-microsoft-windows-server-2008-and-windows-server-2008-r2.

Further information on securely configuring Linux workstations and servers can be found in the ACSC's ***Hardening Linux Workstations and Servers*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-linux-workstations-and-servers.

Further information regarding implementing application control can be found in the ACSC's ***Implementing Application Control*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-application-control.

Microsoft's latest recommended block rules to prevent application control bypasses can be found at https://docs.microsoft.com/en-au/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-block-rules.

Further information on Microsoft's EMET is available at https://support.microsoft.com/en-us/topic/emet-mitigations-guidelines-b529d543-2a81-7b5a-d529-84b30e1ecee0.

Further information on Microsoft's exploit protection functionality is available at https://docs.microsoft.com/en-au/microsoft-365/security/defender-endpoint/exploit-protection?view=o365-worldwide.

Further information on the use of PowerShell can be found in the ACSC's ***Securing PowerShell in the Enterprise*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/securing-powershell-enterprise.

Further information on implementing PowerShell logging is available at https://www.fireeye.com/blog/threat-research/2016/02/greater_visibilityt.html and https://devblogs.microsoft.com/powershell/powershell-the-blue-team/.

Further information on independent testing results of different antivirus software and their effectiveness is available at https://www.av-comparatives.org/ and https://av-test.org/en/.

Application hardening

Application selection

When selecting applications it is important that organisations preference vendors that have demonstrated a commitment to secure coding practices and have a strong track record of maintaining the security of their applications. This will assist not only with hardening applications but also increase the likelihood that vendors will release timely patches to remediate any security vulnerabilities in their applications.

Security Control: 0938; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Applications are chosen from vendors that have made a commitment to secure development and maintenance practices.

Application versions

Newer versions of applications often introduce improvements in security functionality over older versions. This can make it more difficult for an adversary to craft reliable exploits for security vulnerabilities they discover. Using older versions of applications, especially key business applications such as office productivity suites (e.g. Microsoft Office), Portable Document Format (PDF) viewers (e.g. Adobe Reader), web browsers (e.g. Microsoft Internet Explorer, Mozilla Firefox or Google Chrome), common web browser plugins (e.g. Adobe Flash), email clients (e.g. Microsoft Outlook) and software platforms (e.g. Oracle Java Platform and Microsoft .NET Framework), exposes organisations to exploitation techniques that have since been mitigated in newer versions of applications.

Security Control: 1467; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
The latest releases of key business applications such as office productivity suites, PDF viewers, web browsers, common web browser plugins, email clients and software platforms are used when present within SOEs.

Security Control: 1483; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
The latest releases of web server software, server applications that store important data, and other internet-accessible server applications are used when present within SOEs.

Hardening application configurations

By default, many applications enable functionality that is not required by users while security functionality may be disabled or set at a lower security level. This is especially risky for key business applications such as office productivity suites, PDF viewers, web browsers, common web browser plugins, email clients and software platforms that are likely to be targeted by an adversary. To assist in minimising this security risk, the ACSC produces guidance to assist in securely configuring key business applications. Further, to assist in securely configuring their applications, vendors may provide their own security guides.

Security Control: 1412; Revision: 2; Updated: Feb-19; Applicability: O, P, S, TS
ACSC and vendor guidance is implemented to assist in hardening the configuration of Microsoft Office, web browsers and PDF viewers.

Security Control: 1484; Revision: 1; Updated: Jan-19; Applicability: O, P, S, TS
Web browsers are configured to block or disable support for Flash content.

Security Control: 1485; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Web browsers are configured to block web advertisements.

Security Control: 1486; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Web browsers are configured to block Java from the internet.

Security Control: 1541; Revision: 0; Updated: Jan-19; Applicability: O, P, S, TS
Microsoft Office is configured to disable support for Flash content.

Security Control: 1542; Revision: 0; Updated: Jan-19; Applicability: O, P, S, TS
Microsoft Office is configured to prevent activation of Object Linking and Embedding packages.

Security Control: 1470; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS
Any unrequired functionality in Microsoft Office, web browsers and PDF viewers is disabled.

Security Control: 1235; Revision: 2; Updated: Apr-19; Applicability: O, P, S, TS
The use of Microsoft Office, web browser and PDF viewer add-ons is restricted to organisation approved add-ons.

Security Control: 1601; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
If supported, Microsoft's Attack Surface Reduction rules are implemented.

Security Control: 1585; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Standard users are prevented from bypassing, disabling or modifying security functionality of applications.

Microsoft Office macros

Microsoft Office files can contain embedded code (known as a macro) written in the Visual Basic for Applications programming language. A macro can contain a series of commands that can be coded or recorded, and replayed at a later time to automate repetitive tasks. Macros are powerful tools that can be easily created by users to greatly improve their productivity. However, an adversary can also create macros to perform a variety of malicious activities, such as assisting to compromise workstations in order to exfiltrate or deny access to sensitive or classified data. To reduce this security risk, organisations should disable or secure their use of Microsoft Office macros.

Security Control: 1487; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Microsoft Office macros are only allowed to execute in documents from Trusted Locations where write access is limited to personnel whose role is to vet and approve macros.

Security Control: 1488; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Microsoft Office macros in documents originating from the internet are blocked.

Security Control: 1489; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Microsoft Office macro security settings cannot be changed by users.

Further information

Further information on patching applications can be found in the system patching section of the ***Guidelines for System Management***.

Further information on securely configuring Microsoft Office can be found in the following ACSC publications:

- ***Hardening Microsoft Office 2013*** at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-office-2013
- ***Hardening Microsoft Office 365 ProPlus, Office 2019 and Office 2016*** at https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-office-365-proplus-office-2019-and-office-2016.

Further information on configuring Microsoft Office macro settings can be found in the ACSC's ***Microsoft Office Macro Security*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security.

Further information on configuring Microsoft Office to block macros in documents originating from the internet can be found at https://www.microsoft.com/security/blog/2016/03/22/new-feature-in-office-2016-can-block-macros-and-help-prevent-infection/.

Authentication hardening

Account types

When these guidelines refer to authentication hardening, it is equally applicable to all account types. This includes user accounts, privileged accounts, break glass accounts and service accounts.

Authentication types

When these guidelines refer to authentication hardening, it is equally applicable to both interactive authentication and non-interactive authentication.

Authenticating to systems

Before access to a system and its resources is granted to a user, it is essential that they are authenticated. This is typically achieved via multi-factor authentication, such as a username along with biometrics and a password, or via single-factor authentication, such as a username and passphrase.

Security Control: 1546; Revision: 0; Updated: Aug-19; Applicability: O, P, S, TS
Users are authenticated before they are granted access to a system and its resources.

Multi-factor authentication

Multi-factor authentication uses two or more authentication factors to confirm a user's identity. This may include:

- something a user knows, such as a password
- something a user has, such as a Universal 2nd factor security key, physical one-time password token or smartcard
- something a user is, such as a fingerprint or their facial geometry.

Note, however, that if something a user knows is written down, or typed into a file and stored as plaintext, this becomes something that a user has rather than something a user knows.

Privileged users, positions of trust, users of remote access solutions and users with access to important data repositories are more likely to be targeted by an adversary due to their level of access. For this reason, it is especially important that multi-factor authentication is used for these accounts. In addition, multi-factor authentication is vital to any system administration activities as it can limit the consequences of a compromise by preventing or slowing an adversary's ability to gain unrestricted access to assets. In this regard, multi-factor authentication may be implemented as part of a jump server authentication process rather than performing multi-factor authentication on all critical assets, some of which may not support multi-factor authentication.

When implementing multi-factor authentication, several different authentication factors can be implemented. Unfortunately, some authentication factors, such as those sent via Short Message Service, are more susceptible to compromise by an adversary than others. For this reason, a limited number of authentication factors are recommended for use as part of multi-factor authentication implementations.

The benefit of implementing multi-factor authentication can be diminished when credentials are reused on other systems. For example, when usernames and passwords used as part of multi-factor authentication for remote access are the same as those used for corporate workstations. In such circumstances, if an adversary had compromised the device used for remote access, they could capture the username and password for reuse against a corporate workstation that did not require the use of multi-factor authentication.

Security Control: 0974; Revision: 5; Updated: Sep-18; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate standard users.

Security Control: 1173; Revision: 3; Updated: Mar-19; Applicability: O, P, S, TS

Multi-factor authentication is used to authenticate all privileged users and any other positions of trust.

Security Control: 1384; Revision: 3; Updated: Aug-20; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate privileged users each time they perform privileged actions.

Security Control: 1504; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate all users of remote access solutions.

Security Control: 1505; Revision: 0; Updated: Sep-18; Applicability: O, P, S, TS
Multi-factor authentication is used to authenticate all users when accessing important data repositories.

Security Control: 1401; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Multi-factor authentication uses at least two of the following authentication factors: passwords, Universal 2nd Factor security keys, physical one-time password tokens, biometrics or smartcards.

Security Control: 1559; Revision: 0; Updated: Oct-19; Applicability: O, P
Passwords used for multi-factor authentication are a minimum of 6 characters.

Security Control: 1560; Revision: 0; Updated: Oct-19; Applicability: S
Passwords used for multi-factor authentication are a minimum of 8 characters.

Security Control: 1561; Revision: 0; Updated: Oct-19; Applicability: TS
Passwords used for multi-factor authentication are a minimum of 10 characters.

Security Control: 1357; Revision: 1; Updated: Sep-18; Applicability: O, P, S, TS
When multi-factor authentication is implemented, none of the authentication factors on their own can be used for single-factor authentication to another system.

Single-factor authentication

A significant threat to the compromise of user accounts is offline password/passphrase cracking tools. When an adversary gains access to a list of usernames and hashed passwords/passphrases from a system, they can attempt to recover them by comparing the hash of a known password/passphrase with the hashes from the list of hashed passwords/passphrases that they obtained. By finding a match, an adversary will know the password/passphrase associated with a given username. Combined, this often forms a complete set of credentials for an account.

In order to reduce this security risk, organisations should implement multi-factor authentication. Note, while single-factor authentication is no longer considered suitable for protecting sensitive or classified data, it may not be possible to implement multi-factor authentication on some systems. In such cases, organisations will need to increase the time on average it takes an adversary to compromise a password/passphrase by introducing complexity and continuing to increase its length over time. Such increases in length can be balanced against useability through the use of passphrases rather than passwords. In cases where systems don't support passphrases, and as an absolute last resort, the strongest password length and complexity supported by a system will need to be implemented.

Security Control: 0417; Revision: 5; Updated: Oct-19; Applicability: O, P, S, TS
When systems cannot support multi-factor authentication, single-factor authentication using passphrases is implemented instead.

Security Control: 0421; Revision: 6; Updated: Oct-19; Applicability: O, P
Passphrases used for single-factor authentication are a minimum of 14 characters with complexity, ideally as 4 random words.

Security Control: 1557; Revision: 0; Updated: Oct-19; Applicability: S
Passphrases used for single-factor authentication are a minimum of 17 characters with complexity, ideally as 5 random words.

Security Control: 0422; Revision: 6; Updated: Oct-19; Applicability: TS

Passphrases used for single-factor authentication are a minimum of 20 characters with complexity, ideally as 6 random words.

Security Control: 1558; Revision: 1; Updated: Apr-20; Applicability: O, P, S, TS
Passphrases used for single-factor authentication:

- *are not constructed from song lyrics, movies, literature or any other publicly available material*
- *do not form a real sentence in a natural language*
- *are not a list of categorised words.*

Security Control: 1596; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Passphrases used for single-factor authentication can not be used to authenticate to multiple different systems.

Setting and resetting credentials for user accounts

When passwords/passphrases for users are set or reset on their behalf, it is important that they are randomly generated and, following sufficient verification of their identity (e.g. physically presenting themselves and their pass to a service desk or known colleague, or answering a set of challenge-response questions), provided to them via a secure communications channel in order to prevent their compromise. If this is not possible, alternative risk-based measures will need to be implemented.

Security Control: 1227; Revision: 4; Updated: Aug-20; Applicability: O, P, S, TS
Passwords/passphrases set or reset on users' behalf are randomly generated.

Security Control: 1593; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Users provide sufficient evidence to verify their identity when collecting a password/passphrase for their account.

Security Control: 1594; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Passwords/passphrases are provided to users via a secure communications channel or, if not possible, split into parts with part being provided to the user and part provided to the user's supervisor.

Security Control: 1595; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Users that do not set their own initial password/passphrase are required to change it on first use.

Setting and resetting credentials for service accounts

To provide additional security and credential management functionality for service accounts, Microsoft introduced group Managed Service Accounts in Microsoft Windows Server 2012. In doing so, service accounts that are created as group Managed Service Accounts do not require manual credential management by administrators, as the operating system automatically manages the credentials. This ensures that service account credentials are not misplaced or forgotten, and that they are automatically changed on a regular basis.

Security Control: 1619; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
Service accounts are created as group Managed Service Accounts.

Account lockouts

Locking an account after a specified number of failed logon attempts reduces the likelihood of successful password spraying attacks. However, care should be taken as implementing account lockout functionality can increase the likelihood of a denial of service. Alternatively, some systems can be configured to automatically slowdown repeated failed logon attempts rather than locking accounts. Implementing multi-factor authentication is also an effective way of reducing the likelihood of successful password spraying attacks.

Security Control: 1403; Revision: 2; Updated: Oct-19; Applicability: O, P, S, TS
Accounts are locked out after a maximum of five failed logon attempts.

Security Control: 0431; Revision: 2; Updated: Sep-18; Applicability: O, P, S, TS
Repeated account lockouts are investigated before reauthorising access.

Account unlocks

To reduce the likelihood of social engineering being used to compromise accounts, users should provide sufficient evidence to verify their identity when requesting an account unlock.

Security Control: 0976; Revision: 6; Updated: Aug-20; Applicability: O, P, S, TS
Users provide sufficient evidence to verify their identity when requesting an account unlock.

Insecure authentication methods

Authentication methods need to resist theft, interception, duplication, forgery, unauthorised access and unauthorised modification. For example, Local Area Network (LAN) Manager and NT LAN Manager authentication methods use weak hashing algorithms. As such, passwords/passphrases used as part of LAN Manager authentication and NT LAN Manager authentication (i.e. NTLMv1, NTLMv2 and NTLM2) can easily be compromised. Instead, organisations should use Kerberos for authentication within Microsoft Windows environments.

Security Control: 1603; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Authentication methods susceptible to replay attacks are disabled.

Security Control: 1055; Revision: 4; Updated: Oct-20; Applicability: O, P, S, TS
LAN Manager and NT LAN Manager authentication methods are disabled.

Security Control: 1620; Revision: 0; Updated: Oct-20; Applicability: O, P, S, TS
Privileged accounts are members of the Protected Users security group.

Protecting credentials

Storing credentials with a system that it grants access to increases the likelihood of an adversary gaining access to the system. For example, a password/passphrase should never be written down and stuck to a laptop or computer monitor and one-time password tokens should never be left with computers or in laptop bags. Furthermore, obscuring credentials as they are entered into systems can assist in protecting them against screen scrapers and shoulder surfers.

If storing credentials on a system, sufficient protection should be implemented to prevent them from being compromised as part of a targeted cyber intrusion. For example, credentials can be stored in a password vault rather than in a Microsoft Word or Excel document, credentials stored in a database can be hashed, salted and stretched, or credentials can be stored in a hardware security module.

Finally, asymmetric authentication and secure transmission of credentials reduces the likelihood of an adversary intercepting and using such credentials to access a system under the guise of a valid user.

Security Control: 0418; Revision: 4; Updated: Oct-19; Applicability: O, P, S, TS
Credentials are stored separately from systems to which they grant access.

Security Control: 1597; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Credentials are obscured as they are entered into systems.

Security Control: 1402; Revision: 5; Updated: Aug-20; Applicability: O, P, S, TS
Stored passwords/passphrases are protected by ensuring they are hashed, salted and stretched.

Security Control: 1590; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
Passwords/passphrases are changed if:

- *they are directly compromised*
- *they are suspected of being compromised*

- *they appear in online data breach databases*
- *they are discovered stored in the clear on a network*
- *they are discovered being transferred in the clear across a network*
- *membership of a shared account changes*
- *they have not been changed in the past 12 months.*

Session termination

Implementing measures to automatically terminate user sessions outside of business hours (noting this may differ between different work areas), after an appropriate period of inactivity, and then reboot workstations can assist in both system maintenance activities (such as patching) as well as removing any adversaries that may have compromised a system but failed to gain persistence.

Security Control: 0853; Revision: 1; Updated: Aug-20; Applicability: O, P, S, TS
Outside of business hours, and after an appropriate period of inactivity, user sessions are terminated and workstations are rebooted.

Session and screen locking

Session and screen locking prevents unauthorised access to a system which a user has already been authenticated to access.

Security Control: 0428; Revision: 7; Updated: Jun-21; Applicability: O, P, S, TS
Systems are configured with a session or screen lock that:

- *activates after a maximum of 15 minutes of user inactivity, or if manually activated by the user*
- *conceals all session content on the screen*
- *ensures that the screen does not enter a power saving state before the session or screen lock is activated*
- *requires the user to reauthenticate to unlock the system*
- *denies users the ability to disable the session or screen locking mechanism.*

Logon banner

Displaying a logon banner to users before access is granted to a system reminds them of their security responsibilities. Logon banners may cover topics such as:

- the sensitivity or classification of the system
- access to the system being restricted to authorised users
- acceptable usage and security policies for the system
- the user's agreement to abide by abovementioned policies
- legal ramifications of violating the abovementioned policies
- details of monitoring and auditing activities
- a point of contact for any questions.

Security Control: 0408; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Systems have a logon banner that requires users to acknowledge and accept their security responsibilities before access is granted.

Security Control: 0979; Revision: 4; Updated: Sep-18; Applicability: O, P, S, TS
Legal advice is sought on the exact wording of logon banners.

Further information

Further information on authorisations, security clearances and briefings for system access can be found in the access to systems and their resources section of the ***Guidelines for Personnel Security***.

Further information on restricting administrative privileges can be found in the ACSC's ***Restricting Administrative Privileges*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/restricting-administrative-privileges.

Further information on implementing multi-factor authentication can be found in the ACSC's ***Implementing Multi-Factor Authentication*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/implementing-multi-factor-authentication.

Further information creating strong passphrases can be found in the ACSC's ***Creating Strong Passphrases*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases.

Further information on mitigating the use of stolen credentials can be found in the ACSC's ***Mitigating the Use of Stolen Credentials*** publication at https://www.cyber.gov.au/acsc/view-all-content/publications/mitigating-use-stolen-credentials.

Further information on randomly generating passphrases can be found at the Electronic Frontier Foundation's website at https://www.eff.org/dice (preferably using five dice rolls and the long word list) while a random five dice roller can be found at https://www.random.org/dice/?num=5.

Virtualisation hardening

Containerisation

Containers allow for versatile deployment of systems, and can be used to quickly scale systems. However, they are still systems that run software and should be treated as any other system. Application of security controls in a containerised environment may take a different form when compared to other types of systems. For example, patching operating systems on workstations may be actioned differently to ensuring that a patched image is being used for a container, however the principle is the same. In general, the same security risks that apply to non-containerised systems would likely apply to containerised systems.

Functional separation between computing environments

Software-based isolation mechanisms are commonly used to share a physical server's hardware among multiple computing environments. The benefits of using software-based isolation mechanisms to share a physical server's hardware include increasing the range of activities that it can be used for and maximising the utilisation of its hardware.

A computing environment could consist of an entire operating system installed in a virtual machine where the isolation mechanism is a hypervisor, as is commonly used in cloud services providing Infrastructure as a Service. Alternatively, a computing environment could consist of an application which uses the shared kernel of the underlying operating system of the physical server where the isolation mechanisms are application containers or application sandboxes, as is commonly used in cloud services providing Platform as a Service. The logical separation of data within a single application, which is commonly used in cloud services providing Software as a Service, is not considered to be the same as multiple computing environments.

An adversary who has compromised a single computing environment, or who legitimately controls a single computing environment, might exploit a misconfiguration or security vulnerability in the isolation mechanism to compromise other

computing environments on the same physical server, or compromise the underlying operating system of the physical server.

Security Control: 1460; Revision: 2; Updated: Aug-20; Applicability: O, P, S, TS
When using a software-based isolation mechanism to share a physical server's hardware, the isolation mechanism is from a vendor that uses secure coding practices and, when security vulnerabilities have been identified, develops and distributes patches in a timely manner.

Security Control: 1604; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
When using a software-based isolation mechanism to share a physical server's hardware, the configuration of the isolation mechanism is hardened by removing unneeded functionality and restricting access to the administrative interface used to manage the isolation mechanism.

Security Control: 1605; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
When using a software-based isolation mechanism to share a physical server's hardware, the underlying operating system running on the server is hardened.

Security Control: 1606; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
When using a software-based isolation mechanism to share a physical server's hardware, patches are applied to the isolation mechanism and underlying operating system in a timely manner.

Security Control: 1607; Revision: 0; Updated: Aug-20; Applicability: O, P, S, TS
When using a software-based isolation mechanism to share a physical server's hardware, integrity and log monitoring are performed for the isolation mechanism and underlying operating system in a timely manner.

Security Control: 1462; Revision: 1; Updated: Jul-19; Applicability: P
When using a software-based isolation mechanism to share a physical server's hardware, the physical server and all computing environments running on the physical server are of the same classification.

Security Control: 1461; Revision: 3; Updated: Jan-21; Applicability: S, TS
When using a software-based isolation mechanism to share a physical server's hardware, the physical server and all computing environments running on the physical server are of the same classification and within the same security domain.

Further information

Further information on hypervisor security can be found in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-125A Rev. 1, ***Security Recommendations for Server-based Hypervisor Platforms***, at https://csrc.nist.gov/publications/detail/sp/800-125a/rev-1/final.

Further information on container security can be found in NIST SP 800-190 ***Application Container Security Guide*** at https://csrc.nist.gov/publications/detail/sp/800-190/final.