

Secure Computer Standard

Published By

Secure IT Foundation / SecurityBrad.com

"It is possible to secure a computer to the highest standards, but the final level of security is determined by the user's behaviour. No standard can guarantee secure user behaviour."

Version: 1.0

Status: Final

Published: 24 October 2009

1. Introduction

The Secure IT Foundation publishes the Secure Computer Standard as a baseline to which computer manufacturers and retailers can use to demonstrate the level of security applied to the software as received by the home computer purchaser. This standard can be considered comparable to publications from [ISE](#), [NIST](#), [CESG](#) and [PCI](#) that give financial enterprises and government agencies baseline security requirements, but targeted at the home computer user.

The Standard itself has been developed from many years of computer security experience gained by implementing technical standards in corporate environments. For large organisations, there are legal and regulatory standards to be met, supported by the IT Security industry. Payment data, pin codes, passwords, medical data, personal data all must be secured to a standard by law or regulatory code. For the ordinary home computer user, historically there are no computer standards to apply. There is plenty of guidance but this requires extensive knowledge of computers to apply it with uncertain results. This has been likened to a new car purchaser being given a box of parts and told put them together to make their new car secure.

The goal of the Standard is to place security alongside functionality as key motivating factors when choosing a new computer. Security that severely limits functionality is typically disabled or removed, so this Standard attempts to balance best practice security concepts with practical configurations that are more likely to be adopted by the home computer user.

The output of the Secure Computer Standard is a baseline to which a rating scheme can be applied allowing the computer purchaser the ability to understand and compare the security of the models offered for sale. The rating scheme suggested by the Secure IT Foundation is based on a five level security model:

- **Level 0 - Not suitable for use on the Internet**
No security features enabled meet Secure Computer Standard requirements
- **Level 1 - Limited Internet use only, not recommended for personal or financial data**
Network security controls and virus controls meet Secure Computer Standard
- **Level 2 - Basic Internet use only, not recommended for personal or financial data**
Previous level plus operating system configuration meets Secure Computer Standard
- **Level 3 - Internet use ok, acceptable for personal and financial data**
Previous levels plus all installed application configurations hardened to Secure Computer Standard
- **Level 4 –Internet use ok, hard drive encryption in case of computer theft**
Previous levels plus complete fixed disk encryption with pre boot authentication applied

Each new computer should have a label displaying the level of the Secure Computer Standard certified and the version of the Standard applied. Later versions of this standard are expected to be more stringent in requirements and will be publically updated regularly to reflect changes required.

2. Legal Note

This standard is written using best practice and knowledge available and improved using peer review and public scrutiny, however application of the standard does not guarantee data security and the Secure IT Foundation and its volunteers cannot be held legally or financially liable for any foreseen or unforeseen consequences for using the contents of this document in the production of a secure computer.

It is provided for guidance only for use by computer manufacturers and vendors for direct application by security professionals after thorough independent testing and configuration.

3. Contents

- 1. Introduction..... 2
- 2. Legal Note..... 3
- 3. Contents 4
- 4. Standard 5
 - 4.1. Common Principles..... 5
- 5. Network security and virus controls 6
 - 5.1. Background..... 6
 - 5.2. Aim of requirements 6
 - 5.3. Technical Requirements 6
- 6. Operating system configuration hardening 7
 - 6.1. Background..... 7
 - 6.2. Aim of requirements 7
 - 6.3. Technical Requirements 7
- 7. Application configuration hardening..... 9
 - 7.1. Background..... 9
 - 7.2. Aim of requirements 9
 - 7.3. Technical Requirements 9
- 8. Hard drive encryption..... 11
 - 8.1. Background..... 11
 - 8.2. Aim of requirements 11
 - 8.3. Technical Requirements 11
- 9. Appendix - Rating Scheme..... 12

4. Standard

To meet the requirements fully for the Secure Computer Standard, four key controls must be implemented.

- Network security and virus controls
- Operating system configuration hardening
- Application configuration hardening
- Hard drive encryption

These four controls when combined give a baseline level of security for home computers, which gives a minimum assurance level for confidentiality of personal and financial data. Note that integrity and availability of data is not protected by this standard due to the complexity of provisioning. Although encouraged for widespread usage, especially the use of multiple hard drives in computers, it has been considered too onerous to include in this standard.

4.1. Common Principles

The following principles are common to all levels of the Secure Computer Standard:

1. The computer is expected to maintain its security baseline throughout the life of the computer without user intervention e.g. a minimum life of two years should be expected by which time the user would be expected to have the computer maintained by a computer professional.
2. Trust has to be positively assigned by the user. Access to the computer is only possible by the user changing default security settings e.g. by enabling file sharing.
3. Security cannot be assured by the use of a single isolated control; multiple controls should be used to provide defence in depth.
4. Least privilege used to ensure permissions and rights given to user for day to day usage are the lowest possible while still maintaining usability and stability e.g. non-administrative accounts are used for everyday computing.
5. All software on the computer, including the operating system, at time of purchase should automatically update itself to latest stable versions with minimal user intervention. Users have limited capability in determining if software should be updated for security purposes, automation of the updating process for installed software removes the need for the user to have this capability.
6. Open source and 'free for non commercial use' software should be used where the alternative is a limited usage trial e.g. security software that expires in 60 days relies upon the user to renew the software, so it is recommended to use similar software which has an indefinite licence or will function effectively for at least 24 months.

5. Network security and virus controls

5.1. Background

Historically personal computers have been used outside of the corporate environment as dedicated word processing, calculation or gaming devices, which were not connected to other computers. To steal a home computer user's personal and financial data required the thief to be in the same physical location. The advent of networking and the Internet have made theft or alteration of data possible from any location in the world.

5.2. Aim of requirements

Confidentiality of personal and financial data should be protected by ensuring unauthorised access is not possible without user intervention permitting the access e.g. using a browser on the Internet to receive data, receiving emails, enabling file sharing.

If access is granted then controls for checking all code executed and files stored are required to minimise the risk of malicious actions occurring.

5.3. Technical Requirements

1. All incoming network activity must be blocked by default.
2. No incoming network activity should cause the computer to perform any activity outside of logging of the activity.
3. All data sent or received must be checked for malicious code and potential malicious activity before execution.

6. Operating system configuration hardening

6.1. Background

Historically personal computers have been supplied with operating system configurations that allow for maximum compatibility with corporate environments where security would be applied after delivery by corporate security experts. The same operating system configuration, when used on the Internet without effective network security and virus controls, typically will be compromised within hours of connection¹.

6.2. Aim of requirements

Confidentiality of personal and financial data should be protected by ensuring access to the computer does not allow compromise by means of code execution or privilege escalation. Operating system configuration should be changed from default to ensure that the minimum level of trust is granted to users and that the minimal attack surface is presented for compromise opportunities. Operating system security features should be enabled for layers of protection where practical.

6.3. Technical Requirements

1. Each installed operating system must be required to have two user accounts, one for administration, and one for daily usage with minimal rights i.e. if a user chooses to use the administration account for daily usage then it is the user who compromises their security by choice.
2. All logon / logoff, privilege escalation, privileged access and administrative events must be logged and available for review in an audit trail e.g. logging enabled for investigation after a suspected compromise by law enforcement.
3. The operating system must prevent further access attempts after ten failed interactive logon attempts for a minimum period of five minutes before allowing further access attempts.
4. All automatic execution of code from removable media must be disabled by default.
5. All file and print sharing facilities must be disabled by default i.e. the user should explicitly decide if they wish to share a file or folder.
6. A screensaver must be configured to require password to regain access to the computer after a minimum period of 90 minutes. If a shorter period is required by the user then they should have a facility for altering the time period manually.
7. All user account passwords created must meet the following requirements
 - a. Minimum of 8 characters in length
 - b. Consist of at least one capital letter and one numeric digit

¹ <http://isc.sans.org/survivaltime.html>

- c. Required to be changed every 180 days or sooner
8. All security related operating system updates must be automatically applied without user intervention by default. The inaction of the user should not prevent security issues being mitigated within the operating system where updates are cryptographically certified as originating from the producer of the operating system.
 9. All server functions and unnecessary services must be disabled by default. The user should choose if server functions or additional services are enabled.
 10. All administrative user accounts are disabled by default. The user should create the administrative account on first usage of the computer.
 11. All remote access must be disabled by default. The user should decide who has access to their computer for support and management.
 12. All user accounts must be protected by means of passwords, digital certificates or two-factor authentication. Blank passwords must not be allowed without explicit user interaction.
 13. All user account password storage must be encrypted and password protected as a minimum. All password storage that does not meet this requirement must be disabled. The user should be made aware of the insecure nature of this password storage before being allowed to enable it.
 14. User must be able to identify the format of files stored by visual inspection without further action required e.g. file extensions are always displayed.
 15. No personal data should be sent back to the operating system manufacturer unless explicitly given.

7. Application configuration hardening

7.1. Background

Typically personal computers have been supplied with the operating system and applications preinstalled, with the choice of applications partially decided by the purchaser and vendor. Where software, as supplied with a new computer, is not frequently updated, the home computer user is often using unsupported or insecure software from first use. Similar to operating system configurations, applications often are installed using default settings, which are set for maximum compatibility and with little used or known insecure features, enabled.

7.2. Aim of requirements

Application configurations should be changed from default to ensure that the minimum level of trust is granted to applications and that the minimal attack surface is presented for compromise opportunities. Applications must be segregated from each other to minimise the risk of compromise by means of cross-linked applications. The browser is the best example of an application that is often embedded in the operating system, and runs additional applications from within it.

7.3. Technical Requirements

1. Where removal of application functions does not inhibit basic usage, all additional functions must be disabled by default e.g. to read some types of print files, it should not be necessary to enable code execution.
2. Applications installed must not require the removal or alteration of security functions without explicit interaction by the user e.g. peer to peer software requiring incoming connections can only be allowed by the firewall with explicit user interaction.
3. All security related updates for applications must be automatically applied without user intervention by default. The inaction of the user should not prevent security issues being mitigated within applications where updates are cryptographically certified as originating from the producer of the application.
4. Applications must not send personal data to the vendor or any other third party without explicit user consent granted prior to sending or by using a publicly available method to anonymise the data prior to sending.
5. Applications installed on a time-restricted basis must not impede security functions if the time limit expires and must be completely removable without impairing security functions.
6. Applications installed with limited functionality must not impede the ability to perform all security functions required to comply with this standard and must be completely removable without impairing security functions.
7. Applications installed must not enable functionality that is outside the products primary purpose without explicit user interaction permitting the function e.g. animation viewers

should not enable remote computers to view locally installed cameras without explicit approval by the user.

8. Hard drive encryption

8.1. Background

Historically personal computers have been supplied with a hard drive based on an unencrypted file storage structure. Lost laptop stories in the media have become commonplace. Attempts were made to supply drives with hardware based data encryption but with limited success in the enterprise and consumer markets. This has left encryption by software as the dominant means of protecting data at rest from theft. Typically, the issue with pre-supplied encryption is the requirement to supply the password from the vendor to the end user thereby making the security weak with publicly available default passwords or at least not secret passwords. Given that it is possible for financial authentication information, e.g. PIN numbers, to be sent out without knowledge of the bank employees similar provisions are possible for initial encryption passwords.

8.2. Aim of requirements

Hard drive encryption is the primary protection of personal and financial data from physical theft. It should be used by default, as a drive encrypted by a random password by the manufacturer or vendor is still stronger security than a drive with no encryption. Partial encryption of drives is to be avoided as it makes the user choose to apply on security of the data without a full understanding of the consequences of using partial encryption.

8.3. Technical Requirements

1. Each physical disk must be completely encrypted with a [NIST](#) approved authentication algorithm and the Trusted Platform Module key storage should be used where available.
2. Initial passwords as supplied to the computer purchaser must meet the following requirements
 - a. Minimum of 16 randomly generated characters in length
 - b. Consist of at least one capital letter and one numeric digit
 - c. Not be a word found in a dictionary of any language
 - d. Not be displayed or accessible like a serial number for an application or operating system e.g. kept private by means of a foil covering, similar to a scratch card
3. Decryption must be only possible after successful authentication by password, digital certificate or two factor authentication methods.
4. Recovery methods outside of standard decryption process must not be used i.e. no 'back doors' or secondary decryption methods unless required by legislation.
5. Encryption must not impede performance of the hard drive to the point a typical user will remove it in preference to securing the data.

9. Appendix - Rating Scheme

Rating Level	Applied Security Features	Missing Security Features
0	None	Network security and virus controls Operating system configuration hardening Application configuration hardening Hard drive encryption
1	Network security and virus controls	Operating system configuration hardening Application configuration hardening Hard drive encryption
2	Network security and virus controls Operating system configuration hardening	Application configuration hardening Hard drive encryption
3	Network security and virus controls Operating system configuration hardening Application configuration hardening	Hard drive encryption
4	Network security and virus controls Operating system configuration hardening Application configuration hardening Hard drive encryption	None