Best Practices for NSA's UEFI Secure Boot Guidelines

Published by: The Office of Security & Trust, Insyde Software
Tim Lewis
CTO, Insyde Software

Rev: 04.12.2021

Introduction

Recently, the National Security Agency (NSA) of the United States released its "UEFI Secure Boot Customization" report that provides guidelines for configuring a platform's firmware to take advantage of the security promise provided by Secure Boot.[1] Malware targets firmware because of its unique role in setting up and maintaining the platform's hardware security capabilities. Malware also targets firmware because anti-virus solutions today cannot effectively detect and remove it. Secure Boot prevents malware that targets platform firmware from getting started by verifying that each component is trusted before using it.

The NSA's guidelines help IT administrators and end users correctly configure the UEFI Secure Boot and related settings in their BIOS by listing six recommendations. It is not enough to have Secure Boot, it must be enabled correctly. The following sections describes these in more detail and how InsydeH2O® UEFI BIOS from Insyde Software supports them.

NSA #	Summary	Description
1	Turn On UEFI Boot	"Machines running legacy BIOS or Compatibility Support Module (CSM) should be migrated to UEFI native mode." Current platforms support UEFI boot, but the security advantages are negated if not enabled. The previous "legacy" boot standard is inherently insecure, leaving opportunities for malware to insert itself into the boot process.
2	Turn On UEFI Secure Boot	"Secure Boot should be enabled on all endpoints and configured to audit firmware modules, expansion devices, and bootable OS images (sometimes referred to as Thorough Mode)."
3	Customize UEFI Secure Boot	"Secure Boot should be customized, if necessary, to meet the needs of organizations and their supporting hardware and software." BIOS options can further reduce the attack vectors by focusing on installed hardware and software and their use cases.
4	Set Strong Administrator Passwords	"Firmware should be secured using a set of administrator passwords appropriate for a device's capabilities and use case." Administrator passwords restrict access to BIOS configuration options that control UEFI Secure Boot and other platform security features.
5	Update BIOS Regularly	"Firmware should be updated regularly and treated as importantly as operating system and application updates." Like other software in the system, firmware may need regular updates as security issues are discovered and security fixes released.
6	Verify BIOS Integrity with a TPM	"A Trusted Platform Module (TPM) should be leveraged to check the integrity of firmware and the Secure Boot configuration." The TPM checks the integrity of the firmware and the Secure Boot configuration and passes this to the operating system.

The following sections describe how each of these NSA recommendations can be activated on a system with InsydeH2O. There are examples from Insyde's reference setup utility, but actual screens may differ

[1] UEFI Secure Boot Customization, Version 1.1, September 16, 2020, https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF

from vendor to vendor. Applying these recommendations consistently using InsydeH2O raises an organizations security readiness.

1. Enable UEFI Boot

The first recommendation from the NSA is simple: turn on UEFI Boot! While UEFI has been around for over 15 years, some IT departments are still reluctant to enable it for booting because a beloved piece of hardware doesn't work with UEFI or a trusted (but aging) OS version doesn't boot with UEFI.

InsydeH2O supports the use of older hardware or operating systems through a Compatibility Support Module (or CSM). However, the standards used by this "legacy" style of booting are inherently insecure because they assume that the devices and operating systems installed in your system are trusted. Malware authors and security researchers have successfully exploited this trust by pretending to be a typical plug-in hardware device or operating system. Enabling UEFI Boot removes this potential back-door into your system.

Table 1 - Enable UEFI Boot recommendations (as described in Appendix 7.1)

Option	NSA Recommended Setting	InsydeH2O Support
UEFI Boot	Enable	Enable in Setup.

To use UEFI Boot, go to the Boot Menu in Setup and change the "Boot Type" to "UEFI Boot" Refer to the following picture:

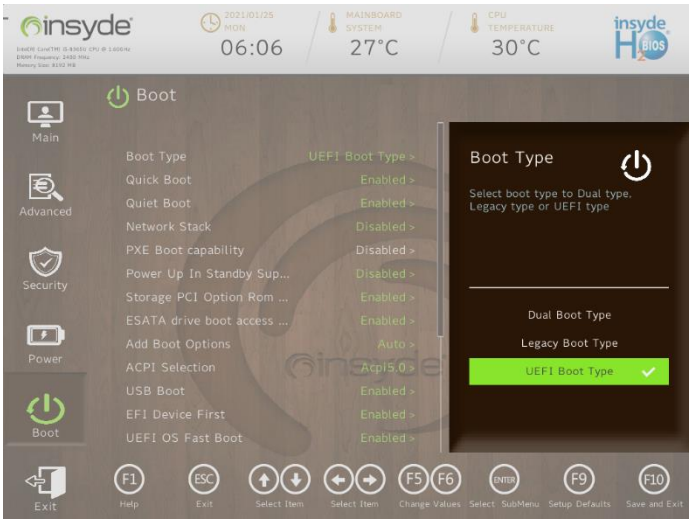

Figure** 1 **- Enable UEFI Boot

2. Enable UEFI Secure Boot

The second recommendation extends UEFI Boot by enabling UEFI Secure Boot on all platforms and configuring it to verify all firmware modules, expansion devices, and bootable OS images. While UEFI Boot enables a new style of booting, UEFI Secure Boot adds cryptographic verification of all code that is not a part of the platform BIOS, including OS loaders and plug-in option ROMs, during platform startup. The BIOS

verifies that the code has not been tampered with and that the code was signed by someone the platform owner trusts. The certificates used for this verification are stored in the UEFI Secure Boot database.

Table 2 - Enable UEFI Secure Boot recommendations (as described in Appendix 7.1)

Option	NSA Recommended Setting	InsydeH2O Support
UEFI Secure Boot	Enable	Enable in Setup.

Most platforms using InsydeH2O ship with Secure Boot enabled and all modules/devices/OS images are verified by default using a certificate provided by the UEFI Forum. If it is not enabled, it should be enabled before being deployed.

InsydeH2O Example

To use UEFI Secure Boot, go to the Administer Secure Boot page in Setup and change "Enforce Secure Boot" to "Enabled" Refer to the following picture:

Figure 2 - Enable Secure Boot

NOTE: The NSA guidelines mention that some BIOS implementations check the *Fast Boot* setting to decide whether or not to perform some Secure Boot checks. InsydeH2O does contain a Fast Boot option that focuses on improving boot speed, especially in consumer devices. However, InsydeH2O does not skip UEFI Secure Boot security checks when Fast Boot is enabled.

3. Customize UEFI Secure Boot

The third recommendation is to customize Secure Boot to meet the needs of IT administrators and platform owners. Depending on the way that the platform is used, it may be possible to strengthen the protections offered by InsydeH2O by customizing Secure Boot.

Customizing UEFI Secure Boot includes changing the contents of the UEFI Secure Boot database. If the platform includes the standard UEFI CA secure boot database (db) of OS boot loaders signatures then the platform can load the standard OS distributions. It is possible to increase security of the platform by

enrolling your own certificate instead of the standard one that specifically targets the OS loader that is actually being used.

Customizing UEFI Secure Boot also allows controlling the entries in the UEFI Secure Boot exclusion (dbx) database. There are standard exclusion lists recommended by the UEFI forum, but care should be exercised when applying thee because it may prevent an OS from loading, if that OS was added to the exclusion list due to security vulnerabilities.

The following table, derived from NSA's recommendations in Appendix 7.1, shows recommendations for UEFI Secure Boot customization:

Table 3 - Customize UEFI Secure Boot recommendations (as described in Appendix 7.1)

Option	NSA Recommended Setting	InsydeH2O Support
Secure Boot Custom Mode	Disable	Custom mode defaults to disabled. Only enabled if new certificates required. Only changeable by administrators.

InsydeH2O Example

InsydeH2O provides administrators full control to change and audit the platform keys and key exchange keys as well as the UEFI Secure Boot database and revocation list. Typically, platforms ship with a default set certificates and a default revocation list that includes the standard UEFI Certificate Authority certificate and (in most cases) the Microsoft Windows production certificate. These entries can be deleted or replaced using the Administer Secure Boot setup page and, at any time, the user can revert the contents of all of these back to the factory default settings.

The Administer Secure Boot page also gives options to add or delete the Platform Key (pk), Key Enrollment Keys (kek), entries in the Secure Boot Database (db) and entries in the Secure Boot Revocation Database (dbx). It also allows the BIOS to revert back to the factory default settings. Refer to the following pictures for more information.

Figure 3 Enroll or Delete UEFI Secure Boot Database (db) entry

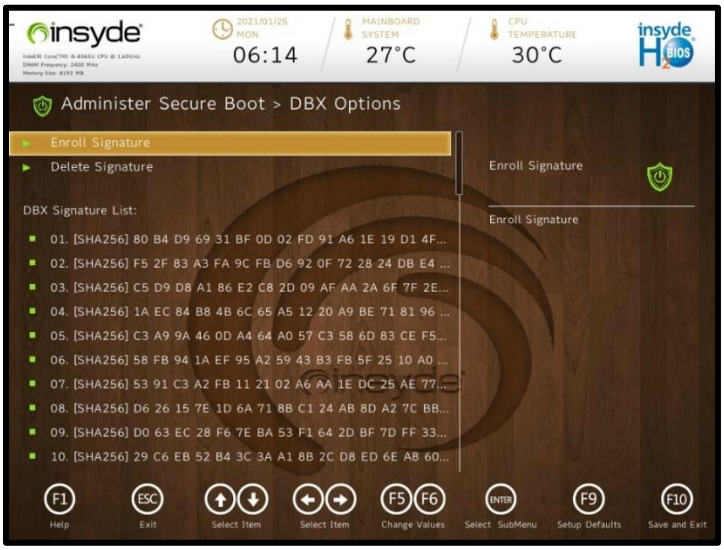

Figure 4 Enroll or Delete UEFI Secure Boot Revocation List (dbx) entry

There are also several options related to secure boot and external storage and networking in the NSA recommendations. These are described in the following sections.

External Storage

There are several NSA recommendations for external storage devices. These are another layer of defense against attacks that require physical presence and can be used by "insiders", including rebooting the system into an alternate OS environment where some or all security protections are not enforced. This can include booting into an OS recovery disk or even DOS or the UEFI Shell.

Table 4 - SATA-Related Recommendations (from "UEFI Lockdown Configuration", section 7.1)

Option	Recommended Setting	InsydeH2O Support
eSATA Port	Disable	Provides option to allow or prevent boot from external SATA devices.
SATA Operation	AHCI	Enable RAID or IRST (Intel Rapid Storage Technology) if appropriate.
SATA Password	Not set	Recommend not to set to allow automatic flash update without user intervention.
SATA ports	Connected only.	Disables SATA ports when no device is connected.
Storage Option ROM Access	Disable	Access for non-administrators is configurable.

NSA guidelines recommend that external SATA devices be disabled. This prevents someone from walking up, attaching a SATA device to an external SATA port, restarting the system and booting off of the SATA device instead of the normal boot drive.

InsydeH2O Example

InsydeH2O provides the option to disable all boot attempts from external SATA devices. Refer to the following picture for more information:

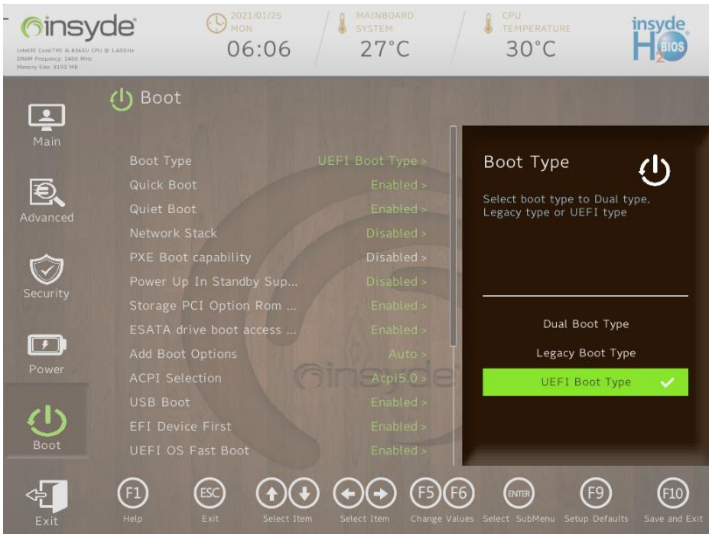

Figure 5 External SATA (ESATA) and USB Boot Disable

NSA guidelines recommend that SATA be set to AHCI mode unless RAID is required. The following screen shot shows how to control the SATA mode.

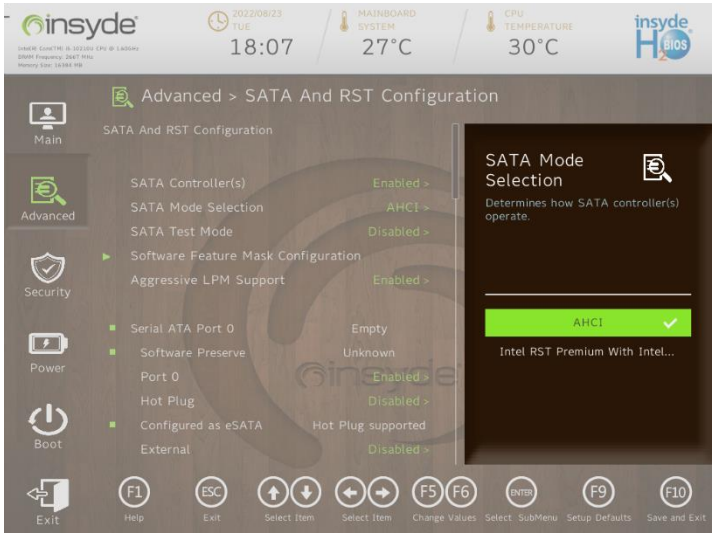

Figure 6 - SATA Controller Mode Selection

NSA guidelines also recommend that SATA password be disabled, which may seem counter-intuitive. However, one of the key recommendations is allowing automatic firmware updates. Requiring that a hard drive password be entered during the boot process prevents this process from being automatic. In order to prevent drives being hijacked, the SATA password should not be modifiable if the user does not log in as the administrator.

Option ROMs

NSA guidelines recommend that the user interface provided by option ROMs that support SATA storage devices should be disabled unless the administrator has logged in. In addition to the weaknesses described for option ROMs in general, the user interface often provides the ability to perform low-level tasks on the drives.

InsydeH2O Example

For InsydeH2O the access to these option ROMs must be for non-administrators, as shown in the following picture:

Figure 7 - Option ROM Access Disable for Non-Administrator

USB

Similar to those for SATA, the NSA guidelines recommend that USB boot be disabled. This prevents someone from walking up, inserting a USB thumb drive into an external USB port, restarting the system and booting off of the USB device. For external USB devices, the NSA guidelines recommend that external USB ports be disabled if not being used. InsydeH2O provides the option to disable all boot attempts

Table 5 - USB-Related Recommendations (from "UEFI Lockdown Configuration", section 7.1)

Option	Recommended Setting	InsydeH2O Support
USB boot support	Disable	Option provided to enable or disable booting from USB devices. See below.
USB power share	Disable	Charges devices through USB power.

InsydeH2O Example

InsydeH2O provides the option to disable all boot attempts from USB devices. Refer to the following picture for more information:

Figure 8 USB Boot Disabling

Network

Appendix 7.1 of the NSA guidelines give an additional set of recommended settings for the BIOS and network devices. See Appendix A for a full list of the ways that InsydeH2O provides control of the relevant options.

Table 6 Network Recommendations (from "UEFI Lockdown Configuration", section 7.1)

Option	Recommended Setting	InsydeH2O Support
UEFI Network Stack	Enable	Network stack can be enabled. See below.
Integrated NIC	Enable	Network boot can be enabled or disabled for IPv4 or IPv6. See below.

Networking can provide substantial benefits for the firmware, such as booting from network attached storage, remote platform management and remote debug capabilities. However, with these capabilities comes the potential risk of hacking via the network. As a result, the NSA has provisionally recommended that the UEFI Network Stack be left enabled "if PXE or image servers are used by the organization. Disable if not used."

InsydeH2O Example

InsydeH2O provides a full networking stack and is configurable to enable or disable both the general network support and booting over the network. Refer to the following picture to see how to enable the network stack:

Figure 9 - Network Stack Control

Additionally, InsydeH2O allows the ability to boot from PXE servers to be enabled or disabled. Per the NSA recommendations, this should be disabled unless network boot is required.

Figure 10 - Network Boot via PXE Control

4. Set Strong Administrator Passwords

The fourth recommendation shows the importance of strong administrator passwords that are appropriate for the device's capabilities and use case. Since the administrator has the ability to alter nearly all UEFI Secure Boot-related settings and configuration, InsydeH2O supports industry best practices for creating and maintaining administrator passwords, including requiring regular password updates, enforcing password length and strength checks and comparing against recently used or easily guessed passwords.

Table 7 - Strong Administrator Password recommendations (as described in Appendix 7.1)

Option	NSA Recommended Setting	InsydeH2O Support
Admin Password	Set	There are two levels of passwords provided: user and supervisor. The user can be prompted to set their admin password before boot or before entering setup.
Non-admin password changes	Disable	User-level access cannot change administrator passwords, Secure Boot and security related configuration options.
Non-admin user setup lockout	Enable	User level access grants access to severely limited configuration options.
Strong passwords	Enable	Length and complexity requirements can be configured. Prevent re-use of recent passwords. Common bad passwords prohibited.
System Password	Disable	Must be disabled to allow automatic firmware updates.
User Password	Set	H2O allows user password to be set.

InsydeH2O Example

InsydeH2O can be configured to prompts the user to set the administrator password, as shown in the following picture:

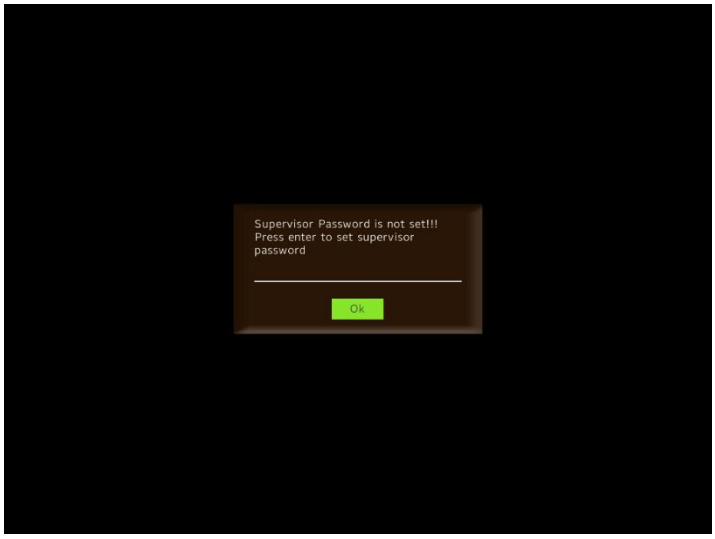

Figure 11 - Administrator Password Prompt

The administrator password can be modified after confirming the original password:

Figure 12 - Set Supervisor Password

5. Update BIOS Regularly

The fifth recommendation points out the necessity of regular firmware updates. InsydeH2O provides world-class firmware update tools, and is fully integrated into the firmware update services provided by Microsoft Windows Update and the fwupd service found in most Linux distributions. Also, in conjunction with the appropriate supporting hardware, InsydeH2O supports the recommended NIST 800-193[2] regimens for reliable update with rollback protection.

6. Verify Firmware Code/Data Integrity with a TPM

The sixth recommendation from the NSA leverages a Trusted Platform Module (TPM) to check the integrity of firmware and the Secure Boot configuration. InsydeH2O uses the TPM to measure firmware code and data and then log those measurements of so that an OS can look back and see whether something essential has changed.

[2] NIST Special Publication 800-193: Platform Firmware Resiliency Guidelines, Andrew Regenscheid, May 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf

Table 8 - TPM recommendations (as described in Appendix 7.1)

Option	NSA Recommended Setting	InsydeH2O Support
TPM ACPI Support	Enable	Supported when TPM's are enabled.
TPM PPI Deprovision Override	Enable	Supported when TPM's are enabled.
TPM PPI Provision Override	Enable	Supported when TPM's are enabled.
TPM Security	Enable and Activate	Administrator can enable and activate the TPM. See below.

InsydeH2O Example

The TPM can be hidden from the OS. Per the NSA recommendations, InsydeH2O allows the TPM to be made visible to the OS:

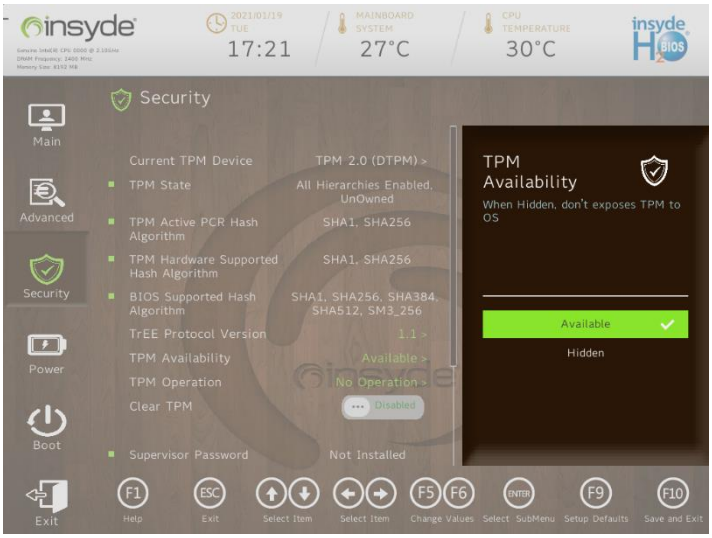

Figure 13 - Make TPM Visible

The TPM can be activated, which will start the measuring of firmware code and data and log the results.

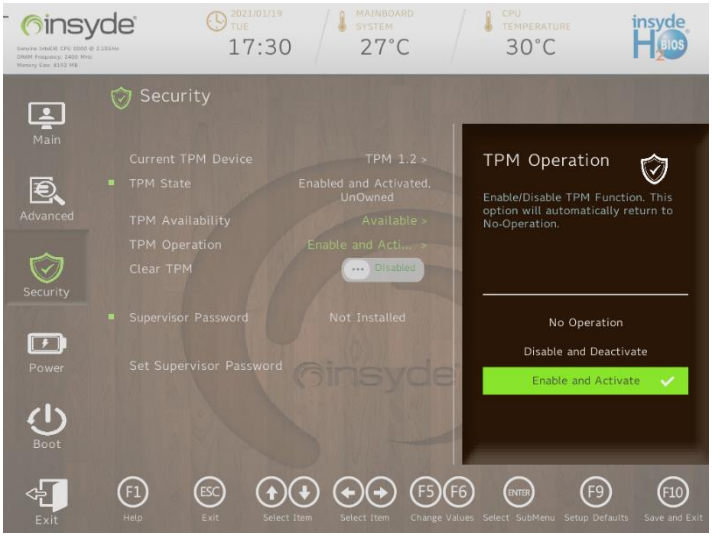

Figure 14 - TPM Enable and Activate

7. Conclusion

The NSA guidelines provide excellent recommendations for configuring UEFI platforms for security using UEFI Secure Boot. InsydeH2O provides all of these foundational capabilities and options to support these recommendations. On this foundation, InsydeH2O can be further customized to deliver additional firmware security capabilities that customers require.

About Insyde Software

Insyde Software (www.insyde.com) is a leading worldwide provider of UEFI firmware, systems management solutions and custom engineering services for companies in the mobile, server, desktop and IoT (Internet-of-Things) computing industries. The company is publicly held (GTSM: 6231) and headquartered in Taipei, Taiwan with U.S. headquarters in Westborough, MA. The company's customers include the world's leading computing, communications and storage device designers and manufacturers.

Disclaimer

Insyde Software provides this document without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose.

This document could contain technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in future revisions of this document. Insyde Software is under no obligation to notify any person of the changes.

The following trademarks are used in this document:

Insyde and InsydeH2O are registered trademarks of Insyde Software. All other trademarks or trade names are property of their respective holders.