HP WOLF SECURITY

HP TAMPERLOCK

PROTECTING DEVICES FROM PHYSICAL ATTACKS

TECHNICAL WHITEPAPER

HP TAMPERLOCK DETECTS AN ATTACKER

When an attacker opens the case of your PC, HP TamperLock[1] provides configurable protection mechanisms against physical attacks on PC internals.

TABLE OF CONTENTS

HP TAMPERLOCK OVERVIEW

Physical attacks on devices (when a target device is disassembled in order to modify or directly probe the system board) are an increasing concern, especially as the tools to perform these sophisticated attacks become more readily available. Examples include the following:

- **Flash memory replacement attacks –** *Flash memory is an electronic nonvolatile computer memory storage medium that can be electrically erased and reprogrammed. Industry-standard PC architecture uses a flash component on the system board for storage of firmware code and settings.* These types of attacks involve an attacker replacing or modifying the contents of flash memory chip with malicious firmware code or firmware policy changes in order to compromise the system.
- **Trusted Platform Module (TPM) probing attacks –** *The TPM is an industry-standard component on a PC system board that provides isolated cryptographic processing and provides secure storage for secrets, such as Microsoft BitLocker disk encryption keys.* This type of attack involves attaching a probe capable of intercepting and modifying all traffic that is sent across the TPM chip electrical interface with the intention of obtaining critical secrets, for example, the BitLocker encryption keys.
- **Direct Memory Access (DMA) attacks –** Here, an attacker connects specialized hardware to an internal electrical interface on the system board to bypass all existing OS memory access controls and is able to read and write the target system's OS main memory without any dependency on the main CPU processor. This type of attack can be used to exfiltrate secrets used by the OS to secure the platform or to inject malicious code by modifying the main memory.
- **Side channel attacks –** These types of attacks involve probing the system board while it is performing sensitive operations and using that "indirect" information to extract secrets from the system. As an example, an attacker could install a probe to observe the power consumption of a device performing an encryption operation in an attempt to derive the encryption key from analyzing that power consumption data.

HP TamperLock provides a general protection mechanism against all classes of physical attacks that involve removal of the system cover to obtain access to the system board, including, but not limited to, the attacks described above. This is achieved by providing a cover removal sensor to detect and lock down a system that is disassembled, along with fully manageable policy controls to configure what action to take in the event a cover removal is detected. Cover removal events and history are stored in platform hardware and can be queried by a remote administrator.

HP TamperLock policies include the optional capabilities of blocking system boot at the BIOS level until valid BIOS administrator credentials are entered; clearing the TPM to delete all user keys (for example, BitLocker keys that render the data stored on the local drive accessible only via a remotely stored BitLocker recovery key); and the ability to power-off the system immediately when the cover is removed.

Additionally, systems with HP TamperLock include advanced capabilities to provide focused protection from the sorts of physical attacks that could otherwise be used to defeat the HP TamperLock protection itself.

Advanced protection from DMA attacks use IO Memory Management Unit (IOMMU) hardware to block illegal DMA access to main memory in order to provide protection against an adversary attempting to use a system board implant to defeat the HP TamperLock feature. Protected storage rooted in the HP Endpoint Security Controller hardware provides physical attack protection for BIOS/firmware data and settings stored in flash memory. Protected storage is designed to provide confidentiality, integrity, and tamper detection even in scenarios where attackers attempt to modify the HP TamperLock policy settings by disassembling the system and establishing direct connections to the nonvolatile flash storage device on the circuit board. Protected storage is always present on systems that support HP TamperLock and cannot be disabled.

HP TAMPERLOCK OPERATION

When the HP TamperLock feature is configured to lock the system due to unauthorized access, it is designed so cover removal detection is active regardless of the power state of the system. Specifically, HP TamperLock will detect a cover removal event in all of the following system power states when HP TamperLock is configured with HP-recommended settings (as shown in the table on page 4):

- System On (OS running)
- System Off (OS shutdown or OS in hibernated state)
- System in Sleep state (OS in ACPI S3 state or Modern Standby)

Additionally, the HP TamperLock cover removal sensor will be triggered even in a scenario where all power sources are removed, including internal battery and Real-Time-Clock (RTC) coin cell, while the cover is removed.

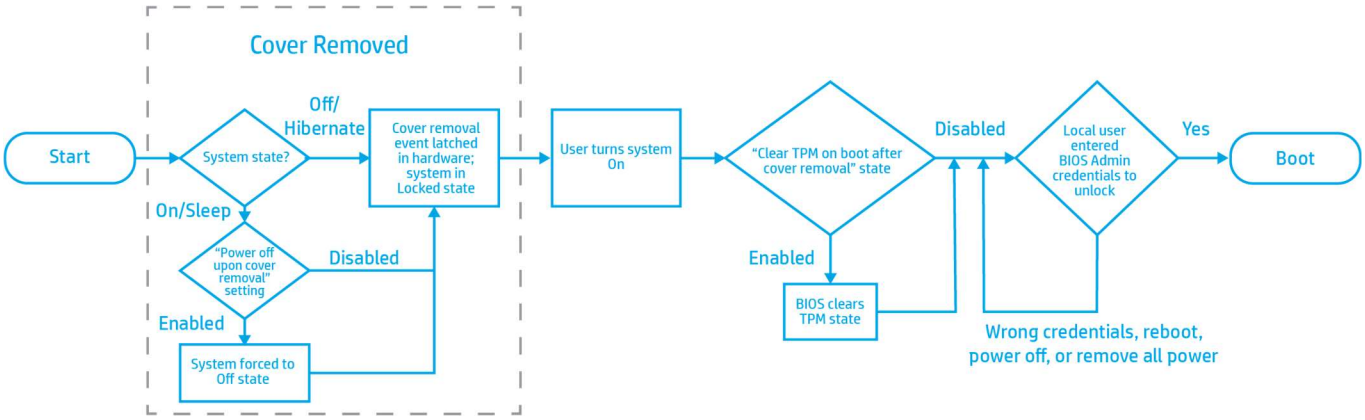
When HP TamperLock detects a cover removal while the system is On or in the Sleep state (using HP-recommended settings), the system will immediately be forced to the Off state and all OS context will be lost.

If the optional policy to clear the TPM state on cover removal detection is Enabled, the BIOS will clear the TPM. The BIOS will not boot to the OS after the cover removal is detected and will, instead, prompt the local user to enter the BIOS administrator password or (in Sure Admin mode) a one-time-use PIN to unlock the system and boot normally.

HP TamperLock status can be obtained via query of the associated BIOS setting or via the Windows Event viewer when HP Notifications software is installed.

Note: RTC power loss will automatically trigger the HP TamperLock cover removal sensor feature; therefore, systems that remain in storage without any power supply attached for longer than 2 years will trigger HP TamperLock cover removal sensor even when the cover has not been removed.

Figure 1: HP TamperLock Operation



HP TAMPERLOCK POLICY SETTINGS

HP TamperLock policy settings are exposed as BIOS settings and can be configured locally or managed remotely using HP Client Management tools[1]. The associated settings control the HP TamperLock capability enablement, as well as the actions taken when the cover is removed.

Table 1: HP TamperLock Policy Settings

Setting	Description	Default	HP Recommended
Cover Removal Sensor	• *Disabled* – No action taken on cover removal. • *Notify the User* – Displays warning message on the next startup if opened. • *Administrator Credential* – This setting requires entering the Administrator password or the one-time-use PIN (when Sure Admin is enabled) before continuing to startup after the cover is opened. To enable this setting, a password must be set or HP Sure Admin[3] Enhanced BIOSAuthentication Mode must be enabled with a Local Access Key set. • *Administrator Password* – Same behavior as Administrator Credential. (This setting name alias is present to maintain compatibility with pre-Sure Admin BIOS setting management solutions that supported the "Cover Removal Sensor".)	Disabled	Administrator Credential or Administrator Password
Power off upon cover removal	Only available when Cover Removal Sensor is not set to Disabled. *Disabled* – If system is in On or in Sleep state when the cover is removed, it remains in that state. *Enabled* – The system immediately turns off if the cover is removed while the system is On or in Sleep state (S3 or Modern Standby).	Disabled	Enabled

Setting	Description	Default	HP Recommended
Clear TPM on boot after cover removal	Only available when Cover Removal Sensor is not set to Disabled. *Disabled* – No change to TPM state when cover is removed. *Enabled* – TPM is cleared on the next startup after the cover is removed. Be aware that all customer keys in the TPM are cleared. This setting should only be Enabled in a situation where manual recovery is possible using remote backups, or no recovery is desired. In the case of BitLocker being enabled, the BitLocker recovery key is required to decrypt the drive.	Disabled	Depends on Customer Requirements
Pre-boot DMA Protection	*Thunderbolt Only* – Input-Output Memory Management Unit (IOMMU) hardware-based DMA protection is enabled in a BIOS pre-boot environment for Thunderbolt-attached PCI-e devices. *All PCI-e devices* – IOMMU hardware-based DMA protection is enabled in a BIOS pre-boot environment for all internal and external PCI-e attached devices.	Thunderbolt Only	All PCI-e Devices
DMA Protection	*Disabled* – BIOS will not configure IOMMU hardware for use by operating systems that support DMA protection. *Enabled* – BIOS will configure IOMMU hardware for use by operating systems that support DMA protection.	Enabled	Enabled

HP TAMPERLOCK STATUS

The BIOS setting defined below can be queried to determine TamperLock status using existing BIOS setting management tools. This setting can only be cleared by providing the BIOS administrator password or BIOS Administrator Credential (Sure Admin mode).

Table 2: HP TamperLock BIOS Status

Setting	Description
Last Cover Removal and Count	When Cover Removal Sensor is not set to Disabled, this setting reports how many times and the last time the cover was removed and acknowledged since it was last cleared by the BIOS administrator. The format entry is: MM/DD/YYYY HH:MM:SS. X times. Depending on system factors (such as system in an Off state), consecutive cover removals will not increment the count. The date and time will be reported as all zeros in cases where the value cannot bedetermined, such as after a real-time-clock power loss.

The following events related to HP TamperLock are stored in the HP Endpoint Security Controller hardware and are pushed to the HP Sure Start[4] folder in the Microsoft WindowsEvent viewer when HP Notifications Software is installed. These events can also be viewed using HP Client Management tools such as the HP Client Management Script Library (CMSL), or the HP Manageability Integration Kit (MIK) for Microsoft System Center Configuration Manager.

Table 3: HP TamperLock Events

Source ID	Event ID	Event	Event Log Type
0x8A (138)	0x1E (30)	HP TamperLock – The system detected that the cover was opened.	Warning
	0x1F (31)	HP TamperLock – The user acknowledged a BIOS notification at boot, indicating the cover had been opened.	Informational
	0x20 (32)	HP TamperLock – The TPM was cleared due to cover removal based on current HP TamperLock policy settings.	Informational

CONCLUSION

Physical attacks on devices are increasing and they are difficult to detect or stop. HP TamperLock detects attackers' attempts to physically access a device and provides configurable protection mechanisms against physical attacks on PC internals.

[1] HP Client Management Solutions: https://www8.hp.com/us/en/ads/clientmanagement/overview.html

[2] HP Tamper Lock must be enabled by the customer or your administrator.

[3] HP Sure Admin is available on select HP PCs and requires HP Manageability Integration Kit from http://www.hp.com/go/clientmanagement and HP Sure Admin Local Access Authenticator smartphone app from the Android or Apple store.

[4] HP Sure Start Gen6 is available on select HP PCs and requires Windows 10.

Learn more at: hp.com/wolfsecurityforbusiness

Sign up for updates: hp.com/go/getupdated

HP WOLF SECURITY

4AA7-8167ENW, June 2021