WHITE PAPER
4th Generation Intel® Core™ Processors

Intel® Hardware-based Security Technologies for Intelligent Retail Devices

Based on 4th Generation Intel® Core™ Processors

Protecting intelligent retail systems, and the customer and transaction data they generate, against malware, theft, and other attacks has never been a more critical issue for retailers.

Intelligent devices are transforming the world of retail by bringing the convenience, variety, and ease of use of the Internet shopping experience into the store.

Traditional and mobile point of sale (POS) devices with Internet connectivity share vast amounts of data and enable retailers to use the power of data analytics to support informed business decisions. Digital signs, interactive kiosks, POS terminals and interactive vending machines based on Intel® architecture have the intelligence to run anonymous viewer analytics through Intel® Audience Impression Metrics Suite (Intel® AIM Suite) and transform consumer experiences with relevant messaging delivered through rich and compelling graphics and video. “Digital Wallet” applications enable shoppers to make transactions on in-store devices using their smartphones.

Protecting intelligent retail systems, and the customer and transaction data they generate, against malware, theft, and other attacks has never been a more critical issue for retailers. Intel security capabilities are now available to help retailers meet a broad range of threats.

Introduction

Intelligent retail devices are designed to aggregate, analyze, and share data so retailers and their customers can conduct transactions and make informed decisions. Beyond traditional point of sale (POS) devices and cash-and-carry registers with Internet connectivity, today’s new generation of retail systems now includes mobile intelligent POS systems, interactive digital signs, interactive kiosks, and interactive vending machines. In addition, some devices are equipped with Intel AIM Suite for anonymous viewer analytics.

It is no exaggeration to say that all of the data shared by intelligent devices in retail has great value to retailers and their customers and is therefore sensitive in nature. Devices including POS terminals, interactive vending machines and ATMs are used to perform financial transactions, retrieve customer information, loyalty identification and inventory information. Interactive digital signs carry viewer analytics data, targeted advertising messages, and applications for content management. Intelligent devices inside the store, including intelligent signs and kiosks, share data with the retailer’s inventory database and are used to support mobile POS applications.

The sharing of this high-value retail data is spawning a spectrum of sophisticated threats, ranging from data theft and identity theft to the display of malicious digital graffiti intended to harm retail brands on digital signs or interactive devices. Attackers are using firmware to gain access to a device’s operating system and applications, in addition to creating viruses and malware that can disable a retail system or provide thieves with access to sensitive data.

Protecting systems, networks, and data itself is a critical challenge for the retail industry. As the industry prepares to address threats with existing software-based security solutions, Intel provides a comprehensive range of security capabilities built-in to hardware. These security capabilities begin at the platform level and include protection of the BIOS, firmware, and platform hardware itself.

Intel takes a comprehensive approach to platform, software, and data security and readers should understand that the platform technologies described in this paper complement other security-related components of Intel® vPro™ technology, including Intel® Active Management Technology (Intel® AMT)[1], Intel® Virtualization Technology (Intel® VT)[2],and Intel® Trusted Execution Technology (Intel® TXT)[3]. Intel's platform security technologies are also designed to complement comprehensive software security solutions from McAfee* designed to protect systems against attacks, viruses, and malware, including providing security protection below the operating system. For details about these Intel security technologies, please refer to the resources section at the conclusion of this paper.

Intel's platform security technologies provide the foundation for protecting data integrity, availability and confidentiality. Retailers can modify their existing security solutions to take advantage of the hardware features of systems based on Intel Core processors, or they can use software solutions that have been optimized for use with Intel's hardware-based security capabilities, giving them hardware-enhanced security.

This paper provides an overview of the hardware-based security technologies enabled by 4th generation Intel Core processors that can help address security threats in retail:

- **Intel® Data Protection Technology with Intel® AES New Instructions (Intel® AES-NI):** hardware-accelerated data encryption and decryption, with high levels of processing performance for secure and responsive user experiences.
- **Intel® Platform Protection Technology with BIOS Guard:** hardware-assisted authentication and protection against BIOS recovery attacks.
- **Intel® Platform Protection Technology with Platform Trust:** integrated solution for credential storage and key management for Microsoft Windows* 8.
- **Intel® Platform Protection Technology with Boot Guard:** authenticated code module (ACM)-based secure boot that verifies a known and trusted BIOS is booting the platform.
- **Intel® Identity Protection Technology with Near Field Communication (NFC):** identity protection for customers using NFC enabled smartphone or smartcard in "Tap-and-Pay", "Tap-to-Authenticate', or "Tap-to-Connect" use cases with their personal systems to securely access online services and e-commerce.

Intel® Data Protection Technology with Intel® AES New Instructions (Intel® AES-NI)

Intel AES New Instructions refer to the set of instructions available with the Intel 4th generation Intel Core processor family. The instructions enable rapid and secure data encryption and decryption based on the Advanced Encryption Standard (AES) as defined by FIPS Publication No. 197. AES is currently the dominant block cipher used in various protocols, and the new instructions are valuable for a wide range of applications. Although the instructions were first introduced in 2010 with Intel® microarchitecture formerly code-named 'Westmere,' the 4th generation Intel Core processor family enables performance improvements targeted at up to 15 percent with approximately 25 percent lower design power (TDP) compared to previous generation Intel processors (source: Intel). Intel AES New Instructions are supported on Intel® Core™ i5 and i7 processors only.

> Intel's platform security technologies are also designed to complement comprehensive software security solutions from McAfee* to protect systems against attacks, viruses, and malware, including providing security protection below the operating system.

The architecture includes instructions that offer full hardware support for AES. Four instructions support AES encryption and decryption, and two other instructions support AES key expansion. The instructions accelerate the execution of AES algorithms by using hardware to perform some of the performance intensive steps of the AES algorithm. A seventh instruction allows carry-less multiplication.

The performance improvement that can be achieved with Intel AES-NI depends on the specific application and the proportion of application time spent in encryption and decryption. At the algorithm level, using Intel AES-NI can provide a significant speedup of AES. For non-parallel modes of AES operation such as CBC-encrypt, Intel AES-NI can provide a 2-3 fold gain in performance over a completely software approach. For parallelizable modes such as CBC-decrypt and CTR, Intel AES-NI can provide a 10x improvement over software solutions (source: Intel). Performance improvements apply to typical AES

implementations, including standard key lengths, standard modes of operation, and even some nonstandard or future variants.

AES instructions also provide important security benefits. By running in data-independent time and not using tables, they help to eliminate the major timing and cache-based attacks that can threaten table-based software implementations of AES. The instructions also simplify AES implementation by reducing code size and reducing the risk of accidentally introducing security flaws. Because Intel AES-NI perform the decryption and encryption completely in hardware without the need for software lookup tables, Intel AES-NI can lower the risk of side-channel attacks.

RETAIL USE CASE: DISK ENCRYPTION PROTECTS DATA AGAINST THEFT, WITHOUT COMPROMISING SYSTEM PERFORMANCE

Disk encryption using Intel® AES New Instructions (Intel® AES-NI) can be applied to all retail devices including POS terminals, kiosks, mobile POS devices, interactive vending machines, ATMs, and interactive digital signage. These devices store data related to software, content relating to advertisers, and user data. Disk encryption is used to protect this valuable data. In some devices, advertising content continuously plays in the background while it acquires new data relating to anonymous viewer demographics. Kiosks in malls, airports, and train stations handle customer logins and process transaction-related data.

Information is continuously being fed into the system while the device continues to display user-friendly advertising and informational content, which places heavy processing demands on the system. Moving disk encryption to hardware using Intel AES-NI can reduce the software application-based workload while simultaneously providing more security.

Intel® Platform Protection Technologies

Intel® Platform Protection Technology with BIOS Guard

A device's BIOS is contained in a privileged space that is invisible to anti-virus software. In addition, malware infecting BIOS remains persistent, and it does not go away even after a cold boot.

To avoid detection, attackers are now digging deeper into the platform. Vulnerabilities in System Management Mode (SMM) and System Management Interrupt (SMI) handlers have been identified. The complexity of SMM hardware and software makes it very likely that BIOS update vulnerabilities will continue to be exploited in the future.

For this reason, platform security begins with the BIOS.

Intel® Platform Protection Technology with BIOS Guard, a new feature on

4th generation Intel Core processors (U-series), ensures that updates to system BIOS flash and Embedded Controller (EC) flash are secure. BIOS updates are cryptographically verified by the BIOS Guard module, using a protected agent running in AC-RAM (Authenticated Code RAM), to perform authentication and updating of flash control hardware.

For EC updates, BIOS Guard employs early BIOS POST provisioning of a random secret that is shared between the CPU and the EC. The BIOS Guard module uses this value to identify itself to the EC, which will reject all protected operations without this identification.

Each protected component of a BIOS Guard protected BIOS update is cryptographically signed by the device manufacturer, checked, or signed and checked, before it is allowed to update a system. BIOS Guard helps ensure that malware stays out of the BIOS by blocking all software-based attempts to modify protected BIOS without the platform manufacturer's authorization.

As shown in Figure 1, BIOS Guard addresses SMM vulnerabilities by strengthening the update trust boundary.

RETAIL USE CASE: HARDWARE-ASSISTED AUTHENTICATION PROTECTS AGAINST UNAUTHORIZED BIOS UPDATES

BIOS Guard helps to ensure that connected retail systems are updated only with correct firmware provided by the device manufacturer. Retail devices are customized with OEM specific information in addition to the retailer's proprietary data. Unauthorized access to devices allows hackers to attack a system.

POS terminals, interactive vending machines, and ATMs are typically serviced by a variety of technicians, and OEMs need to ensure that only authorized personnel are allowed to update the device's BIOS or EC. BIOS Guard will ensure that only OEM-authorized BIOS and firmware is updated, regardless of who performs the update.

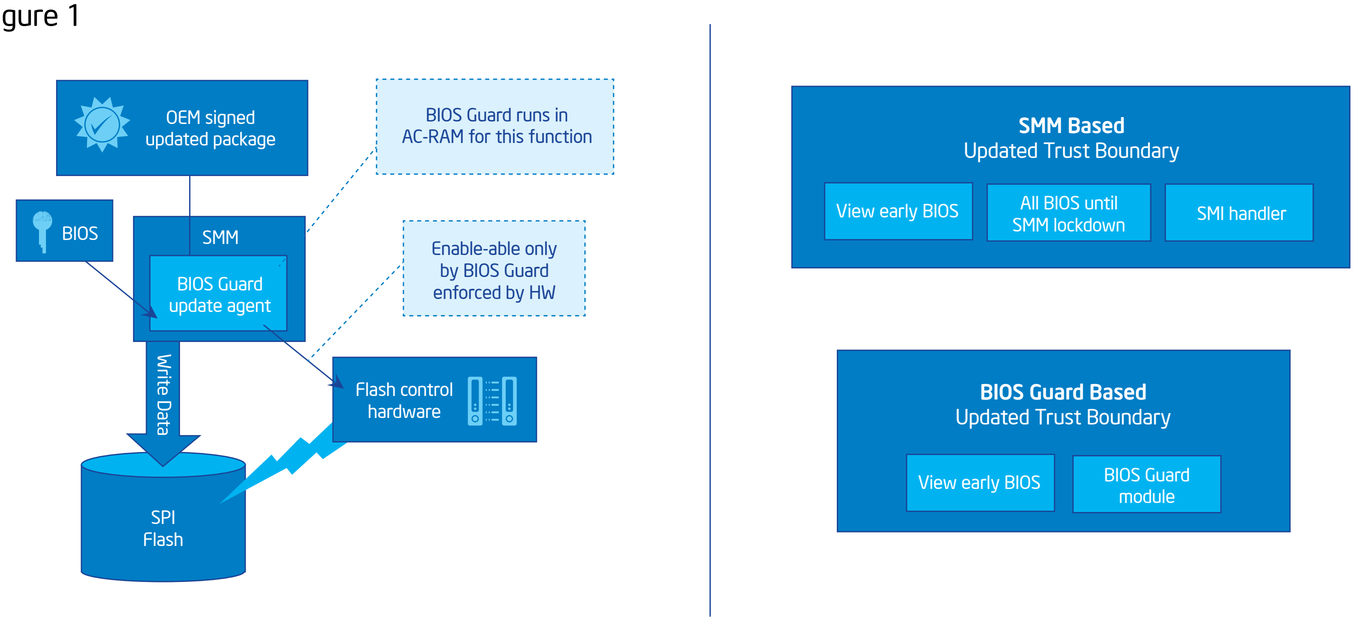
Intel® Platform Protection Technologies

Intel® Platform Trust technology (Intel® PTT) is a platform functionality for credential storage and key management used by Microsoft Windows 8. It supports Windows 8 secure and measured boot and supports all the Microsoft mandatory commands for Trusted Platform Module (TPM) 2.0 v.0.88. It is an integrated solution in the Intel® Management Engine for 4th generation Intel Core processors for ultra-low TDP (ULT) platforms.

This integrated solution provides a secure trust element to meet Windows 8 Connected Standby (CS) requirements with reduced power consumption in ultra-low power state S0iX environments. Functional integration reduces BOM cost and board real estate requirements.

Intel Platform Protection Technology with Boot Guard technology works with Intel PTT, reducing the complexity of the Windows 8 boot process and meeting all Windows 8 requirements. Boot Guard protects against boot block-level malware and provides an added level of hardware-based platform security to prevent repurposing of the platform to run unauthorized software. The technology

Figure 1



is rooted in a protected hardware infrastructure and is designed to prevent the execution of an unauthorized boot block. An Authenticated Code Module (ACM) is provided by Intel and signed to the hardware. When invoked by the processor on platform reset it executes in protected AC-RAM space.

Boot Guard covers three configurable boot types:

- *Measured Boot* measures the Initial Boot Block (IBB) into the platform protected storage device such as Trusted Platform Module (TPM) or Intel PTT.
- *Verified Boot* cryptographically verifies the platform IBB using the boot policy key.
- *Measured +Verified Boot* measures and verifies the IBB.

RETAIL USE CASE: AN AUTHENTICATED CODE MODULE (ACM) VERIFIES THAT A KNOWN AND TRUSTED BIOS IS BOOTING THE PLATFORM

Boot Guard technology addresses the threat of viruses and malware by ensuring that only authorized firmware and an authorized operating system are running on the system.

In mobile POS (mPOS) devices running Windows 8, using Boot Guard technology reduces BOM cost by avoiding the need for a discrete trusted platform module while providing the same level of security through measured and verified boot.

Intel® Identity Protection Technology with NFC

Originally designed for desktop, notebook, and Ultrabook™ devices, Intel® Identity Protection Technology (Intel® IPT) is now available in intelligent retail devices based on 4th generation Intel Core processors. Intel IPT is suite of four technologies: One Time Password, Protected Transaction Display, Embedded PKI and Near Field Communications (NFC). The identity protection technologies address identity theft by introducing a second factor of authentication that relies on a tamper resistant area within the intelligent hardware.

This paper introduces Intel IPT with NFC as an identity protection solution for customers using the "Tap-and-Interact" use case to interact with a digital sign, vending machine, and other devices. For details about other IPT technologies, please refer to the resources section at the conclusion of this paper.

NFC is a short-range wireless communication technology with a protocol for peer-to-peer data exchanges between two endpoints. The current usage model for NFC enables customers to connect to a device to interact, exchange data, check-in, set up a transaction, scan devices, and pay for a product by tapping their NFC-enabled smart card or smartphone against a NFC sensor in a retail device, then complete the transaction, with positive identity confirmation protected through cryptographic binding. All this is done through a software application running on the OS.

Intel IPT includes similar use cases for NFC such as "Tap-to-Pay" and "Tap-to-Authenticate" capabilities which enable users to securely access online resources and e-commerce payments simply tapping their smart card on their NFC-enabled PC. Intel IPT use case for NFC as "Tap and Interact" allows secure interaction with interactive devices. Intel IPT is an integrated chipset-based security feature that introduces security by isolating the data received by NFC from the operating system. Intel's solution adds value by introducing an integrated secure element in the chipset within the retail device.

RETAIL USE CASE: IDENTITY PROTECTION FOR RETAIL CUSTOMERS USING SMART CARDS AND SMARTPHONES

'Tap-to-Connect' with a retail device using a smartphone is becoming a popular way for customers to use their smartphones to download electronic coupons from digital signage in an airport or mall, obtain movie tickets, get loyalty information in stores, check-in to transit venues, and perform non-payment transactions using a broad range of interactive devices.

With current NFC usage models, downloading user identity data from a smartphone is processed by the OS-based application running on the intelligent device. Malware may be able to hack the system and retrieve the user's identity.

Intel® Identity Protection Technology (Intel® IPT) with NFC changes this paradigm. After a user taps to connect using their smartphone, the information is transferred to Intel® Management Engine (Intel® ME) on the retail device. Intel IPT introduces protection of data received by NFC by isolation. The OS is not aware of data used in transaction, preventing potential malware from gaining access to the customer's identity information.

Conclusion

Intelligent systems require smart security, and Intel provides essential security technologies for platforms, software, and data.

Intel's approach to security in intelligent retail devices begins at the platform level, with hardware-based security capabilities built-in to 4th generation Intel Core processors. Integrating security functionality on the platform, beginning with the protection of the BIOS, firmware, and platform hardware itself, creates a strong foundation for protecting intelligent retail devices against security threats. Hardware-based security works with existing software-based security solutions, which can be modified to take advantage of the hardware features of systems based on Intel Core processors. In addition software solutions from third-party vendors have been optimized for use with Intel's hardware-based security capabilities.

Hardware-enhanced security, enabled in 4th generation Intel Core processors, means that powerful security mechanisms are built-in to every intelligent device based on Intel architecture, providing a foundation of security for intelligent retail devices and applications.

Resources

Intel® Data Protection Technology with Intel® AES New Instructions (Intel® AES-NI)

Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI)

Intel® AES New Instructions (Intel® AES-NI)

Accelerate McAfee Endpoint Encryption* with Intel® AES New Instructions (Intel® AES-NI)

Intel® Data Protection Technology with Secure Key (Digital Random Number Generator [DRNG])

Intel® Identity Protection Technology

Role of NFC in the future of Digital Wallet

Developers, NFC, and the Ultrabook™: What this Technology Can Do for Your App

Technology Brief: Intel® Identity Protection Technology

Intel® Platform Protection Technology

Contact your Intel representative for more information.

Other Intel® Technologies

Enhanced Data Protection with Hardware-Assisted Security

Intel® Active Management Technology

Intel® Trusted Execution Technology

Intel® Virtualization Technology

Intel® Anti-Theft Technology

Software

McAfee* Embedded Control Provides 'White Listing' Capabilities to Enhance Virus and Malware Security

[1] Requires activation and a system with a corporate network connection, an Intel® Active Management Technology (Intel® AMT)-enabled chipset, network hardware, and software. For notebooks, Intel AMT may be unavailable or limited over a host OS-based VPN, when connecting wirelessly, on battery power, sleeping, hibernating, or powered off. Results dependent upon hardware, setup, and configuration. For more information, visit www.intel.com/technology/vpro/index.htm.

[2] Intel® Virtualization Technology (Inte® VT) requires a computer system with an enabled Intel® processor, BIOS, virtual machine monitor (VMM) and, for some uses, certain platform software enabled for it. Functionality, performance, or other benefits will vary depending on hardware and software configurations and may require a BIOS update. Software applications may not be compatible with all operating systems. Please check with your application vendor.

[3] No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel®_TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules, and an Intel TXT-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit www.intel.com/content/www/us/en/data-security/security-overview-general-technology.html.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.

Printed in USA 0513/BR/ICMCRC/PDF ♻ Please Recycle 328987-001US