Achieving PCI DSS compliance when managing retail devices with Intel® vPro™ technology

January 2013
# Contents

Introduction .......................................................................................................................... 3  
References ............................................................................................................................ 7  
Intel® AMT Overview ............................................................................................................. 7  
   Benefits for PCI DSS compliance environments ............................................................... 8  
      Strong Role Based Access Control .............................................................................. 8  
      Account Authentication Options ............................................................................... 9  
      System level and User level logging ...................................................................... 10  
      Monitoring Cardholder data environment with Alerting ........................................ 11  
      Monitoring Critical Software .................................................................................. 11  
      Inventory Management ............................................................................................ 12  
Standards and Security ........................................................................................................ 12  
Network Connectivity for PCI DSS Environment ............................................................... 13  
      Wired Connectivity ................................................................................................ 13  
      Wireless Connectivity ............................................................................................ 13  
      802.1x Support for Wired and Wireless ................................................................. 13  
Setup and Configuration of Intel AMT devices .................................................................... 13  
      Default Password .................................................................................................... 14  
      Using accounts with real user names ................................................................. 14  
Common Retail Remote Management Challenges ............................................................ 15  
      Remote Management with Segmented PCI DSS Environments .............................. 17  
      Internet connected Store Locations (behind routers/NAT) ...................................... 19  
      Air gapped or “Jump” Server .................................................................................. 21  
      Third Party Managed Service Provider (IT Outsourcing) ....................................... 23  
Conclusion ............................................................................................................................ 24  
Acknowledgements ............................................................................................................. 25
Achieving PCI DSS compliance when managing retail devices with Intel® vPro™ technology

Introduction

This paper will show that using Intel® Active Management Technology (Intel® AMT, a capability of Intel® vPro™ Technology) provides an effective remote management solution for environments needing to comply with the Payment Card Industry Data Security Standard (PCI DSS) requirements. The paper will map Intel AMT capabilities back to the relative PCI DSS requirements and provide some advice about using Intel AMT in common retailer network topologies.

Confusion may arise when moving to structured management solutions such as Intel AMT because it appears to create new PCI DSS challenges, when in fact the implementation preparations are simply exposing latent PCI DSS issues that have somehow missed consideration until this point. If an implementation decision around a management solution appears to be impacted by PCI DSS, an organization should first ask “how are the organization’s tools processes avoiding the same problem today?” As an example, if a debate is raging about whether a central command console is pulled into PCI DSS scope by managing a particular point of sale network, ask the question: who is providing management today to that network, and where are they connecting from? Is today’s solution more or less desirable than using a central command console with rigorous access controls, logging, and auditing? The practical PCI DSS-related benefits of solutions such as Intel AMT typically outweigh ad-hoc or limited feature management solutions.

More important than in-band vs out-of-band management is whether the organization maintains compliance with the deployed tools and practices.

Figure 1 - The ultimate challenge is to maintain PCI DSS compliance while using an effective remote management solution

Further compounding matters is the fact that Intel AMT is an Out of Band (OOB) management solution, which means that the machine can be managed even when the operating system is not running properly. There exists a false impression that OOB management solutions create more PCI DSS challenges than in-band solutions. The reality is that many organizations only discover
these challenges when they start seriously evaluating any structured management solutions.

When moving to structured solutions an organization is likely originating from one of two starting points:

1) They are already using remote management solutions and understand how they impact their PCI compliance efforts, or

2) They are using remote management solutions and do not understand how they impact their PCI compliance efforts.

In both cases reality dictates; someone, somewhere, is using some form of remote management technology and the only difference is if the organization has an adequate grasp of the PCI DSS impact.

One thing most managers do understand is that incentives, stated or implicit, drive behaviors in their organizations. Task somebody with managing 10,000 point of sale computers and they will quickly deploy tools and automation to create frictionless maintenance with a preference for easy addressability of all devices under management. Task somebody with achieving and maintaining PCI DSS compliance and they will push for a highly segmented, complex and static network architecture that isolates card handling systems to ease compliance activities. Combine those two incentives, and the organization can get paralyzed trying to resolve the priorities. Combined with other realities such as complicated store network connectivity, outsourced IT services, and network diversity due to mergers and acquisitions, and PCI DSS compliant remote management takes a backseat and is addressed instead with insecure desktop sharing programs or other inappropriate solutions.

Another motivation of organizations tasked with maintaining PCI DSS compliance is the reduction of scope, such that the organization can cleanly declare computing resources “in scope” or “out of scope” for PCI DSS compliance activities. The smaller the number of “in scope” systems, the lower the workload and resources needed to achieve and maintain PCI compliance. This is a well understood and measureable indicator, and as a result most organizations strive to segment PCI DSS related networks into separate domains, limit employee access, and reduce utility of the devices by restricting network and internet connectivity. These actions fly directly in the face of remote management solutions, which by design require remote network connectivity, and often require non-automated interaction with the device when remediating on a case-by-case basis. Enterprises with many nodes under management typically centralize on command consoles which help maintain trouble tickets, manage technical support activities, summarize device status, and provide easy device connectivity.

Unlike in-band management solutions which rely on software agents running on the managed device, Intel AMT offers out-of-band remote access to devices by utilizing a secure microcontroller embedded into many Intel platforms and operates independently of the main computer processor. This
distinction proves valuable because the device can be remotely managed as long as it is plugged into wall power and has network connectivity. Regardless of whether the device is powered on or off, running or blue screened, booted or paused at a BIOS prompt; a remote management console can connect to the device, check status, take control of keyboard/video/mouse, reboot it, power it on, modify BIOS settings, boot to another O/S, and much more. Of course, with great power comes great responsibility, and so Intel AMT offers fine grained account privileges, authentication, logging and auditing to map the technology to the security controls required by an organization. In general, out-of-band solutions complement in-band management solutions by making overall device management more comprehensive. Typically in-band solutions are used to provide routine and recurring management when the OS is up and running, and out-of-band is used when the OS is not running or the system is powered off, such as break-fix situations that provide faster responses, reduce unnecessary truck rolls, and decrease total cost of ownership.

From observed experience, retailers are often challenged with these PCI DSS compliance requirements with respect to retail endpoint devices [1]:

- **PCI DSS Requirement 5**: Use and regularly update anti-virus software or programs. Normally this is a challenge when network topologies make it challenging to push or pull .DAT file updates, or when configuration management tools do not have access to systems to monitor software versions for compliance.

- **PCI DSS Requirement 8**: Assign a unique ID to each person with remote access. Challenges of managing fleets of far flung devices combined with large numbers of technicians create logistical problems for maintaining uniqueness on remote platforms. Throw in outsourced IT, vendor and service provider access and the problems keep growing. Even enterprises with strong identity services get challenged when storefront networks effectively prohibit the use of central directory services, creating islands of devices without enterprise authentication services.

- **PCI DSS Requirement 10**: Tracking and monitoring access to network resources and cardholder data. Between insufficient logging tools, business practices which complicate unique accounts, network access issues, and inadequate separation of roles, enterprises struggle to show solid controls to meet this requirement.

A common theme in the above challenges is that complicated enterprise and store networks create challenges in using the tools IT normally applies for credential management, log collection, PKI services, and so on. While ideally suited for managing fleets of devices under normal IT purview, Intel AMT offers a number of capabilities that offer key benefits in these complicated retail environments:
Achieving PCI DSS compliance when managing retail devices with Intel® vPro™ technology

- Auditing and Logging: Separation of administrator and audit roles, along with the use of least privilege permit Intel AMT to track and log all system activities such as remote access, configuration changes, alerts, and system power events. Audit logs cannot be tampered with by non-auditor users, and Intel AMT cannot be re-provisioning while audit logging is enabled (preventing intentional log erasure). PCI DSS Requirement 10 compliance will benefit greatly from these features, and later this paper will demonstrate some automated scripting solutions for collecting Intel AMT device audit and history logs.

- Granular user privilege and role management: Intel AMT offers a number of platform capabilities, and these features can be selectively enabled to support the rule of least privilege. Users can also be mapped to Active Directory accounts where feasible.

- Use of strong cryptographic capabilities where possible. Remote connections and provisioning can be forced to use PKI/TLS for mutual device authentication. Remote logins can use Kerberos or HTTP Digest (with nonce and replay attack defenses) authentication.

- Strong provisioning methods help organizations efficiently bring new devices online and deter attackers from using the provisioning process for their own benefit.

- Watchdog timers and sensing of software execution can be used to alert management consoles that something is amiss. For example, Intel AMT can monitor when an A/V agent stops executing and inform the IT staff.

- Hardware Asset Lists allow a central monitoring console to query individual asset and system details and whether the system is currently powered on.

- Third party data storage can be customized by an enterprise to store enterprise-specific information in non-volatile memory on the platform. Examples include storing peripheral information lists useful for when the O/S has to be reinstalled, DAT file versions or other software versions installed, certificates, O/S patches installed, or a description of the physical location of the system. These can be pulled and made available to a remote technician.

These features and more will be described in more detail throughout the remainder of the document. Additionally, this paper will describe these particularly problematic retail enterprise challenges and how to cope with them:

- “Air gapped” store servers. Some merchants use an air gap in their store networks to prevent direct network connections from external networks into the store network. While seemingly problematic for
remote management solutions, Intel AMT has configuration options that can work within this requirement.

- Remote management behind NAT or firewalls where it is not possible to punch through from external networks. This is often the case in small stores, franchises, or vending environments.

- Understanding how to support IT outsourcing (ITO): While this is not uniquely challenging for Intel AMT, ITO and remote management is always a problem.

References


[4] Intel AMT SDK


[6] Intel AMT Functionality to Realm Mapping

[7] Digest Master Password

Intel® AMT Overview

Intel® AMT is a capability embedded in Intel® vPro™ technology-based platforms that enhances the ability of IT organizations or service providers to manage retail systems. Intel AMT operates independently of the platform processor and operating system, providing out-of-band management. Remote management console applications can access Intel AMT securely, even when the platform is turned off, as long as the platform is connected to line power and to a network. While most mainstream consoles already support Intel AMT directly, Independent Software Vendors (ISVs) can use the Intel AMT SDK [4] to build applications which take advantage of these features.
Benefits for PCI DSS compliance environments

Intel AMT addresses PCI DSS compliance concerns with capabilities not addressed by in-band management tools alone. These enhanced capabilities help IT managers flexibly define security policies meeting the practical needs of organizations (such as employee role changes and complex network topologies) which ultimately help the organization achieve and maintain PCI DSS compliance.

Strong Role Based Access Control

PCI DSS Requirement 7 addresses the restricting access to cardholder data by authorized personnel, systems, and processes as well as requiring the rule of least privilege. Intel AMT meets these needs by providing a strong access control list which can assign various device management tasks to authorized users. Remote access and device management is not an “all or nothing” activity, and Intel AMT allows the organization to map the actions to an individual’s needs by role. This mapping is achieved by “Access Control Lists”, and the mapped activities are called “Realms”.

Access Control Lists

The Intel AMT Access Control List (ACL) manages who has access to which capabilities within the managed device. An ACL entry comprises a user ID and a list of one or more realms (activities) to which a user has access.

There are two kinds of ACL entries based on their authentication method: Kerberos and Digest. Kerberos entries use an Active Directory SID to identify a user or a group of users. Digest entries use a username and password for account identification. The simplest activation of Intel AMT enables a single default user named “admin” with privilege set to all Intel AMT realms. The admin user is always a Digest user. It is not recommended that the admin role be used for day-to-day system management, but rather that the admin
role only manage the ACL entries to assign privileges and realms for those that will provide routine maintenance. The admin user should not be used as a shared account, and therefore the admin credentials should utilize strong passwords. Additionally, in a subsequent section the paper describes how to audit and track the actions of all accounts, including the admin account.

ACLs can be established during initial device provisioning, and updates to the ACL can be managed either by managing roles in the Active Directory server, or by using console tools and directly updating the ACL on the devices under management.

**Activities and Realms**

Realms are the granular management activities assigned to an ACL entry. Example realm titles include: Security Administration, Power Settings, Remote Control, Secure Audit Log, etc. For a list of all realms supported by Intel AMT, refer to the web page as listed in Reference [6].

**Account Authentication Options**

As mentioned in the Access Control List section, Intel AMT supports both Digest and Kerberos authentication for user login. The authentication options are discussed below.

**Kerberos Authentication**

Intel AMT provides for a standard, single-sign-on style of authentication by utilizing Microsoft* Windows* Active Directory infrastructure, which manages domain authentication based on the Kerberos protocol.

This authentication method eliminates the need for management applications and consoles (including setup and configuration services) to manage unique and strong username/password pairs for all Intel AMT systems. Instead, the organization can extend standard methods and tools to manage deployed fleets; users wanting to manage Intel AMT systems need only to authenticate to the Windows domain to gain access to Intel AMT devices.

It is possible to define up to 32 Kerberos Security Identifiers (SID) and each SID can represent an individual user or an Active Directory group.

**Digest Authentication**

Kerberos infrastructures are not always available or practical for some merchant network topologies, and so Intel AMT supports HTTP Digest Authentication based on RFC2617 for these cases.

While RFC2617 permits some basic (and weak) Digest authentications, Intel AMT uses the advanced options to make the authentication as strong as the RFC allows. The password is never sent to the managed system in the clear. Rather a cryptographic hash is computed based on the username, password and other parameters and is sent to the managed system to prevent replay.
attacks. The cryptography method used in Intel AMT meets the strong cryptography requirement in PCI DSS Requirement 3.4.

Depending on the Intel AMT version in the managed client, you can define up to eleven digest users. The passwords defined must meet the criteria outlined in the Intel AMT SDK [4].

Digest master password. As each Intel AMT system has a default admin user with Digest authentication, the Intel AMT team has suggested a process for managing fleets of deployed devices using a derived password technique called “Digest Master Password”, or DMP. For more information on DMP, refer to Reference [7].

System level and User level logging

Section 10 of the PCI DSS calls out system and user logging as a critical piece of an organization’s security processes. Intel AMT technology provides a powerful logging capability that captures high level system event information such as boot sequence, OS hangs, and chassis intrusion, as well as administrative logging that covers remote management history, password attacks, and so on. The logging is separated into two types of log histories: the system level event log (focusing more on platform events) and the audit log (focusing more on the actions initiated by the management user).

Because management can occur when systems are powered on or powered off, a platform level logging capability is required to record activities even if the operating system is not running. Further, the audit log is critical to monitoring the activities of even fully privileged administrator roles. There is a risk that an administrator may be tempted to abuse their privileges, and so Intel AMT can be configured to have an “Auditor” role such that even a fully privileged admin cannot erase audit logs and histories. Further, Intel AMT cannot be deactivated or re-provisioned if an auditor is defined, allowing an organization to maintain checks and balances for the responsibilities of system administrators. Finally, as mentioned below, there are automated ways to periodically archive system logs into enterprise log management servers.

Event Log

Once the Intel AMT system has been successfully configured, it will send out events that are unfiltered (by default) indicating the successful booting of the system covering BIOS execution – hardware initialization, successful operating system boot and more. There are other events that Intel AMT sends which require prior subscription such as OS Critical stop, boot error, system firmware progress and much more. The event log will capture all of these events and save a copy locally on a secure location in the flash which only Intel AMT can read and write.
Access Monitor (Audit log)

The optional Access Monitor feature enables an organization to create an Auditor user to monitor activities performed on Intel AMT systems by users and administrators. The Access Monitor feature is implemented with the following conditions:

- An independent Auditor user that cannot be changed or deleted by an administrator
- A configurable list of auditable events
- A configurable list of alerts to send associated with the auditable events
- An interlock with administrators so that Intel AMT systems cannot be unconfigured without cooperation from the Auditor

Intel AMT writes the configured events to the audit log. The Auditor and others can review the audit log to detect break-in attempts, abuse of privilege, or trace events to identify the root cause of various problems.

Backing up logs onto log server

Archiving logs maintained by Intel AMT is often a critical activity for organizations to manage system health and security. Intel AMT logs can be exported to different formats such as .TXT, .LOG or even .CSV for import into external log servers as covered by PCI DSS Requirement 10.5.4.

For example solutions to export log files that can be imported to a log server, visit the link http://communities.intel.com/community/vproexpert/blog/2012/05/17/ways-to-save-amt-log-data-using-powershell.

Monitoring Cardholder data environment with Alerting

Intel AMT offers alerting capabilities that send notices over Out of Band connections to remote management consoles, and these alerts can be used to monitor access to the cardholder data environment. Alerts can be sent based on detection of brute force Intel AMT password attacks as well as upon chassis intrusion.

Monitoring Critical Software

Intel AMT offers watchdog timers to monitor the operation of critical software components in the operating system. Typically this capability, called "Agent Presence" is used to monitor if someone has disabled anti-virus protections or other security related tasks. This can be used to help meet PCI DSS

---

1 These capabilities need sensors installed on the motherboard.
Achieving PCI DSS compliance when managing retail devices with Intel® vPro™ technology

Requirement 5.2 which requires the latest anti-virus software is running. Intel AMT agent presence has the ability to detect abnormal exit of anti-virus software and notify remote administrator via Intel AMT alerting. After the notification has been received, the administrator can connect to the remote device and remediate the problem.

**Inventory Management**

A configured Intel AMT system will provide on-demand hardware asset information such as the type of the CPU, hard disk information, physical memory and other information. This information can be archived in a centralized database or retrieved irrespective of the power state or the system. If desired, detection of physical tampering of the hardware could be tracked by reviewing the current hardware and comparing with the last known good asset information. PCI DSS Requirement 9.9.1 indicates to maintain inventory logs of all media. This capability would be beneficial to track easily removable items such as individual hard disk drives.

On the software side, Intel AMT provides access to 192KB space of NVRAM access to authorized users via applications supporting Intel AMT. This space can be used to store any critical information from the host operating system. The information can then be read locally or remotely even in out of band mode and enables a wide range of retail use cases and can be useful with PCI DSS compliance. For example, tools could write the version number of the latest anti-virus .DAT file to the NVRAM space, and later all systems could be scanned to identify out of date installations.

**Standards and Security**

Intel AMT was designed keeping security at the core of the architecture. While Intel AMT is thought of as a hardware platform capability, Intel AMT also includes firmware and software components such as application, services and drivers to support the capabilities described above. The software and firmware components of Intel AMT follow best in industry coding standards, change control process as defined by SDL. As a result, Intel AMT software components meet and exceed the PCI DSS Requirement 6.5.

Intel AMT has the option to secure network communications with Transport Layer Security (TLS). This protocol prevents man-in-the-middle class of attacks by providing communication security and privacy between two endpoints over the internet and intranets. Network communications use the standard IANA ports 16992-16995 to communicate with Intel AMT capable platforms over Ethernet LAN or WIFI. Organizations can configure Intel AMT in the PCI DSS environment with TLS enabled to address PCI-DSS Requirement 4.1.

For details on the security of the following areas, refer to the security white paper [3]:

- Securing the Intel Management Engine Firmware storage and update
Achieving PCI DSS compliance when managing retail devices with Intel® vPro™ technology

- Isolation of Intel Management Engine Code Execution
- Secure setup and configuration of the systems
- Remote Network Interface authentication - HTTP Digest or Kerberos authentication based
- Securing an Intel AMT connection using TLS certificates.

Network Connectivity for PCI DSS Environment

The Intel AMT system can communicate with an external entity such as management console via Ethernet LAN, i.e., wired or using Wireless LAN in Out-of-band mode in a standard secure way and as a result meeting PCI DSS Requirement 4.1. The following subsections will review in brief:

Wired Connectivity

In mainstream computing devices, all network traffic normally passes through the system’s Ethernet controller to reach the respective operating system. But Intel AMT traffic is routed directly to Intel AMT firmware in the chipset without passing through the operating system.

Wireless Connectivity

On supported platforms Intel AMT traffic can pass through the wireless LAN in out-of-band mode and requires WPA or WPA2 to secure the communication.

In a PCI DSS environment, Intel AMT devices configured to operate in wireless LAN is strongly recommended to use WPA2 security option.

802.1x Support for Wired and Wireless

Intel AMT meets and exceeds the PCI DSS requirement of ensuring wireless network transmission use industry best practice as stated in subsection 4.1.1. Intel AMT supports 802.1x with EAP over both wireless and wired network connections in out-of-band mode.

Setup and Configuration of Intel AMT devices

Setup and configuration is the process that initializes Intel AMT features on a computing device and makes the device accessible to remote management applications. Intel AMT devices, by default, are delivered in an un-configured state. Configuration is required to populate various settings such as network parameters, individual feature enablement, access control lists, authentication, and remote network accessibility.

There are multiple supported methods for individual device setup and configuration, ranging from high touch to zero touch, and with various security aspects. We recommend using the method titled “Remote
Configuration (PKI)” with TLS encryption which offers a zero-touch configuration while maintaining the security that PCI DSS requires.

The whitepaper in Reference [3] covers different ways to setup and configure Intel AMT under the section “Provisioning the System”.

Software tools to configure Intel AMT in different methods can be downloaded from the website in Reference [5].

**Default Password**

Consistent with PCI DSS Requirement 2.1, Intel AMT mandates changing of the factory default password during the configuration process.

**Using accounts with real user names**

PCI DSS requires that user accounts be allocated to individual users rather than generic shared accounts (for user accountability). As Intel AMT devices ship with an “admin” account, a few extra steps should be taken to adhere to the PCI DSS requirements.

The recommended approach to creating unique user accounts for Intel AMT devices is outlined below:

1. Using the default admin account, create properly named user accounts with admin privileges (as well as any other accounts with limited privileges) identified by the individual’s name. For example the recommended way to create a new user is “Joe.Smith” user versus a generic user name such as “level1_helpdesk”. It is up to the organization to decide on the normal distribution of privileges and realms, but typically at least one user retains full administrative privileges (to insure that the system remains manageable should the user account be removed).

2. Reduce the privileges of the default admin account as much as the system allows.

3. Change the default admin account password to a very strong, random password which is unique to each device, ideally using the maximum password length supported.

4. The intent of this step is to ensure that the generic admin account is never to be used again, and only named accounts are used moving forward. To achieve this, either permanently destroy the newly assigned password (effectively disabling the default admin account), or securely store the password in a safe location, and where access to the location is auditable. This is a non-trivial decision, and if an organization chooses to retain the password in some form, the organization should demonstrate how it is preventing the general use of the password and the default admin account.
Common Retail Remote Management Challenges

This section describes how to use Intel AMT remote management within some challenging retail infrastructures that are commonly seen. These scenarios have posed manageability challenges for merchants and they are presented here to illustrate how Intel AMT can be successfully introduced to improve PCI DSS compliance and improve device remote manageability.

Figure 3 – Everything is in scope
The figure represents retail networks that include internal IT helpdesk and other systems including credit card processing systems under a flat structure without any network segmentation intended to isolate PCI DSS systems or network traffic. The internal IT helpdesk communicates to geographically dispersed retail store locations over the internet using a secure VPN (Layer 2 tunnel) connection, and the devices in the retail stores are directly addressable from anywhere in the network.

As PCI DSS scope is often determined by the connectivity of PCI DSS affected systems, and the perceived challenge is the question of whether a centralized management help desk spreads PCI DSS scope to other, previously out-of-scope managed devices. This is the classic example described in the introduction, and the response is to treat the Intel AMT enabled console with the same scope considerations as in-band management solutions already being used for software updates and anti-virus .DAT file pushes. This is an organizational decision, but the PCI DSS compliance is improved by utilizing an Intel AMT enabled help desk’s role based access controls. Others may choose to install a parallel help desk which is dedicated to in-scope PCI DSS devices, and maintains a clear separation of roles for PCI and non-PCI devices.

After Intel AMT is deployed, the organization will be able to realize these benefits to aid in ongoing PCI DSS compliance:

- Remote management using secure TLS connection and optimally using mutual authentication.
- Well defined role based access controls with privileges assigned to individual users based on business need to know.
- Better system level tracking and user level tracking via Intel AMT event log and access monitors.
- Integration with directory services such as Microsoft* Active Directory to ease the process of user management.
- Maintaining software and hardware compliance via Intel AMT asset tracking capabilities.
Remote Management with Segmented PCI DSS Environments

Figure 4 - Remote Management with Segmented PCI DSS Environments

This illustrative example represents retail infrastructures with devices processing credit cards that are logically isolated from the store and enterprise networks. As a result of the network isolation, the PCI DSS scope is reduced, which is a key motivation for organizations trying to maintain PCI DSS compliance.
A retailer can address isolation in two ways in an attempt to reduce the PCI DSS scope. The first approach is to build an infrastructure for in-scope devices and build another infrastructure with out-of-scope. While this is possible, for some retailers this may not be practical.

The second approach is to maintain one infrastructure with in-scope and out-of-scope devices. But any remote access to the in-scope devices is to be challenged with two-factor authentication.

In this scenario, the store routers (or firewalls) have been configured with appropriate role based access controls which will limit, if not prohibit, remote access to systems processing credit cards. Additionally as seen in Figure 4, a credit card processing kiosk is connected over a private Wi-Fi network.

First, connectivity is required for a help desk to manage the PCI DSS scoped devices. As in scenario 1, the responsibility of managing help desk technician privilege and access control will be shifted to the help desk administrators, just as they perform for all other management activities. That leaves the Intel AMT deployment challenge primarily as a connectivity issue: allowing help desk network access while maintaining the desired network segmentation.

This is achieved through 1) two-factor authentication to firewall permissions 2) permitting the standard IANA ports 16992-16995 through the store firewalls (but still private via the VPN tunnel to corporate), 3) using TLS connections to avoid communication observation, and 4) using mutual authentication to avoid man in the middle attacks. The two-factor authentication can be done by using two of the three authentication methods in addition to a unique username:

- Something you know, such as a password or passphrase
- Something you have, such as a token device or smart card
- Something you are, such as a biometric

Further, for the wireless devices, be sure to enable the supported 802.1x for strong encryption and authentication. The combination of these actions should allow an organization to "trust, but verify:" trust that the network isolation and management access is achieved, while using the other stated benefits of Intel AMT such as audit logging to monitor for undesired activities.

After Intel AMT is deployed, the organization will be able to realize these benefits to aid in ongoing PCI DSS compliance:

- Remote management using secure TLS connection and optimally using mutual authentication.
- Well defined role based access controls with privileges assigned to individual users based on business need to know.
• Better system level tracking and user level tracking via Intel AMT event log and access monitors through central log collection.
• Integration with directory services such as Microsoft Active Directory to ease the process of user management
• Maintaining software and hardware compliance via Intel AMT asset tracking capabilities

Internet connected Store Locations (behind routers/NAT)

Figure 5 - Internet connected Store Locations (behind routers/NAT)
This figure represents the retail infrastructure where the devices under management are remotely located behind firewalls or routers and are not directly addressable by the central management console.

This infrastructure does not have site-to-site VPN tunnels between the corporate networks and the retail stores and to compensate uses an Intel vPro technology based Gateway sitting in the enterprise DMZ to receive connections coming from managed devices in retail stores. Optionally, there could be multiple Intel vPro technology based Gateway servers installed in the DMZ to handle multiple retail store locations if desired.

In this usage, remote management sessions are always initiated by the Intel vPro technology based system to the Intel vPro technology based Gateway located in the DMZ, which allows the devices to navigate through firewalls or NAT to reach the Intel vPro technology based Gateway (via standard ports such as 80, 8080 ..). Alerts and scheduled device initiated connections are handled automatically, but help desk driven tasks need to be queued or coordinated with the expectation that the device may not be currently connected.

The devices can initiate a connection to the Intel vPro technology based Gateway in three ways:

(a) User initiated on demand – from the BIOS interface or from an Intel AMT supported application running on the device.

(b) Alert initiated – Connections can be automatically established when an Intel AMT alert is triggered. See section titled “Monitoring Cardholder data environment with Alerting” for more information about AMT alerts.

(c) Scheduled Maintenance – connections can be established at a defined interval.

Once the Intel vPro technology based system establishes a connection to the Intel vPro technology based Gateway, the help desk can be notified about the active connection. At that point, helpdesk personnel would want to connect to the Intel vPro technology based system and perform the desired management actions, but the helpdesk user should be authenticated via two-factor authentication before being granted access to the device. Capable consoles could automate these actions to notify specific technicians or alert on specific devices that need attention. The device will remain connected indefinitely but can be configured to time out due to inactivity.
Air gapped or “Jump” Server

Figure 6 - Air gapped or “Jump” Server

Like the previous scenario, the devices under management are remotely located behind firewalls or routers and are not directly addressable by the central management console. Unlike the previous scenario, these devices do not have direct networked access to the internet and are isolated behind an “air gap” or “jump server”. Access to the devices requires first accessing the jump server, and then accessing the device under management.

The recommended solution is to use an AMT enabled jump server that maintains a persistent connection to the Intel vPro technology based Gateway in the DMZ, so that the helpdesk can achieve immediate access on demand to
the jump server (as in the previous scenario, two-factor authentication should be used when accessing devices situated in-scope). Once logged into the jump server via Intel AMT KVM, the technician then connects to the targeted Intel AMT device from the jump server. This last step can be a manual process, or can be automated by using a locally installed, simplified management console (for example, the Intel® Manageability Reference Console). Alternately, the devices could be managed directly via their embedded management web server using strong Digest authentication. Either way, the jump server assumes the role of the store’s local management console responsible for managing the store’s connected devices; the jump server utilizes Intel AMT capabilities on the smaller store scale just as the capabilities would map to the larger enterprise needs.
The scenario represents an environment where a third party managed service provider is delivering the device management and help desk services. There is some debate among PCI professionals whether the third party is considered simply a contingent work force, or truly a service provider as referenced in PCI DSS Requirement 12.8. Intel AMT is able to function with this as well as to support the controls required for these situations. For purposes of the discussion, the scenario reflects the more difficult situation of a “true” service provider.
In this scenario, the merchant’s infrastructure is maintained entirely within the merchant’s property, including networking assets, servers, and the actual remote management console. The third party IT help desk personnel are located external to the network, and will log into the merchant’s management console via web access from the merchant’s infrastructure. The merchant retains administrative rights to the management console, and creates the account roles and permissions for the external help desk personnel. Those accounts need to be created with the same role based access controls in the same manner as internal resources, and their actions would be tracked via the normal console and Intel AMT device logging capabilities.

In Figure 7, the management console is running on the “gateway” server, from which helpdesk personnel can access the PCI scoped devices. It is recommended to place the gateway in front of a router which can provide another layer of access controls for the devices under management.

PCI DSS controls unique to third party service providers can be applied to the web connectivity of the ITO. Standard practices such as opening access windows on demand or using two-factor authentication can be utilized to control ITO access to the enterprise network, and then the normal access controls and auditing of the command console can provide oversight for when technicians are connected and performing their duties.

**Conclusion**

Merchant IT organizations are grappling with two competing priorities. They need to maintain PCI DSS compliance, and they need to efficiently manage hundreds or thousands of remote devices. Not to mention that new devices are always being added, and those devices may have different form factors, support requirements, and transactional security needs.

Intel® Active Management Technology can deliver on both priorities, and likely helps an organization exceed compliance requirements while supporting the device uptime metrics today’s merchants require.

For any questions check with your equipment sales representative or read more about Intel AMT details in the reference. Most major retail OEMs offer Intel AMT-enabled cash registers, kiosks, self-service checkouts, digital signage, and office computing devices. There’s even a possibility your enterprise has already been deploying Intel AMT capable devices.

Achieving PCI DSS compliance when managing retail devices with Intel® vPro™ technology

Acknowledgements

The authors would like to thank Todd Aument and Walter Conway of 403 Labs for their reviews and feedback on this paper.

Authors

Brad Corrion is a Platform Architect with the Intelligent Systems Group at Intel Corporation.

Naren Kumar is a Solutions Architect with the Intelligent Systems Group at Intel Corporation.

Manoj Punamia is a Platform Architect with the Sales and Marketing Group at Intel Corporation.

Acronyms

ACL  Access Control List
AD   Active Directory
AMT  Intel® Active Management Technology
API  Application Program Interface
CA   Certificate Authority
DNS  Domain Name Service
EAP  Extensible Authentication Protocol
HTTP Hypertext Transfer Protocol
ISV  Independent Software Vendor
ITO  IT Outsourcing
NAT  Network Address Table
OOB  Out-Of-Band
PCI DSS Payment Card Industry Data Security Standard
POS  Point Of Sale
SDL  Software Development Lifecycle
SID  Security Identifier
SOL  Serial Over LAN
TCO  Total Cost Of Ownership
TCP  Transmission Control Protocol
TLS  Transport Layer Security
VPN  Virtual Private Network
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.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL’S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

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 go to: http://www.intel.com/design/literature.htm

Intel and the Intel logo are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2013 Intel Corporation. All rights reserved.