Intel Software Network
Connecting Developers. Building Community.

Intel® vPro™ Technology
Virtual Seminar 2010

Getting to know Intel® Active Management Technology 6.0
Remote Encryption Management

Andy Schiestl
Application Engineer
Software and Services Group

March 3, 2010
Agenda

• Existing challenge and solution model
• Technical details of the solution (for a Security ISV)
• Use cases
Intel® vPro™ technology
Manageable Data Protection with Remote Encryption Management

Challenges
- Pre-boot authentication (PBA) mechanisms require user presence at the PC
- Protecting data often means giving up some remote manageability
  - Remote power on & manage
  - Applying unattended patches that require reboots
- PCs left in “unlocked” state to remotely manage
  - Data exposed when user not present
  - Unnecessary power consumption

Solution
- Intel® vPro™ Technology extends to include a wide set of data protection options with full management capabilities, even across power cycles & reboots
- Protection without compromise to manageability or energy-efficient performance.

Manageable data security with Intel® vPro™ technology
Intel® vPro™ technology
Expanding Manageable Data Protection Options with Remote Encryption Management

More data protection choices with the industry-leading manageability of Intel® vPro™ technology:

- Encrypting hard drives
- Data encryption software
- Hard drive passwords

For current & future Intel® vPro™ technology platforms starting in 2009
Enabled by new innovation from Intel & integration from ecosystem leaders
Grow value of Intel® vPro™ Technology

• Addresses key market segment concern for end customers
• Increases flexibility in solution choice
• Embraces & innovates on existing market offerings
• Removes barrier for customers that require Intel® vPro™ Technology and drive-level data protection
• Reinforces key value prop and differentiation of Intel® vPro™ Technology platforms

Security, Manageability and Energy-efficient Performance
Have it all with Intel® vPro™ Technology
Deployment Environment

• Two distinct audiences, ISV’s that currently handle hard disk encryption (Security ISV’s), and ISV’s that are interested in unlocking systems for patching and fixing (Manageability ISV’s)
Remote Encryption Management
Building Blocks

**Client PC**
- vPro HW & FW
- Intel
- PBA***
  - ISV

**IT Administrator**
- Remote Console
- ISV

**Remote Encryption Management SDK**
- ATA over LAN Bridge Application & DLL
- Remote Encryption Management Image
- AMT Stack DLL
- Remote Encryption Management Utility
  - Intel

*** Integration of the ATA over LAN Bridge into PBA is optional
Remote Encryption Management Security Solutions

1. **Intel® vPro™ Technology-based Management of FDE HDD Solutions**
   - Ex. Seagate* DriveTrust*, Fujitsu* FDE, Hitachi* FDE HDDs
   - Requires Remote Console & ISV PBA (optional)

2. **Intel® vPro™ technology-based Management of FDE Software Solutions**
   - Requires ISV PBA & Remote Console support

**Use Cases**
- Remote Wake & Patch
- Data Protection Enablement/Disablement
- Remote User / Password Management
- HDD Repurposing
Remote Encryption Management
Usage Example

IT Administrator

Client PC

1. Establish Secure Connection for Communication - TLS
2. Initiate Serial over LAN
3. Initiate IDER
4. Send Remote Wake Command
5. Confirm SATA over LAN Bridge Listening
6. Send SATA over LAN command
7. Confirm action
8. Reboot
ATA over LAN Bridge

• Execution environment to translate SOL communication from the Remote Console into commands

• Can be used in multiple environments
  – Within the ISO image provided by the Remote Console
  – Integrated within an ISV PBA environment
Remote Encryption Management Image (ISO)

• Optional usage versus integration of the ATA over LAN bridge into your PBA
  – SW Environment which stores the ATA over LAN bridge

• Downloaded onto client platform by the Remote Console (via IDE-R)

• May be utilized in to manage FDE HDDs
Remote Encryption Management
Use Cases
Remote Encryption Management Usage #1

Allows Remote Management of FDE HDDs via Intel ISO

IT Administrator

Remote Management Console

Remote Security Console

AMT Stack DLL / ATA over LAN Bridge DLL

1. Establish Secure Connection for Communication - TLS
2. Initiate Serial over LAN
3. Initiate IDER
4. Send Remote Wake Command
5. Confirm SATA over LAN Bridge Listening
6. Send SATA over LAN command
7. Confirm action
8. Reboot

Client PC

ME Common Services FW

BIOS

ATA over LAN Bridge
Remote Encryption Management Image

DRAM

No BIOS Changes Required
Remote Encryption Management Usage #2

Allows Remote Management of FDE HDDs via PBA

**IT Administrator**

1. Establish Secure Connection for Communication - TLS
2. Initiate Serial over LAN
3. Send Remote Wake Command
4. Confirm SATA over LAN Bridge Listening
5. Send SATA over LAN command
6. Confirm action
7. Continue Boot

**Client PC**

- ME Common Services FW
- BIOS
- DRAM
- FDE PBA
- ATA over LAN Bridge
- AMT Stack DLL / ATA over LAN Bridge DLL

**Distribution Legend**

- Intel
- OEM
- ISV

**Remote Security Console**

Send List of machines to unlock (optional)

**Remote Management Console (WS-MAN Library)**
Remote Encryption Management Usage #3
Allows Remote Management of FDE SW via PBA

IT Administrator

Remote Management Console (WS-MAN Library)
Remote Security Console

Send List of machines to unlock (optional)

Client PC

1. Establish Secure Connection for Communication - TLS
2. Initiate Serial over LAN
3. Send Remote Wake Command
4. Confirm SATA over LAN Bridge Listening
5. Send SATA over LAN command
6. Confirm action
7. Continue Boot

No BIOS Changes Required
Remote Encryption Management SDK Components

Remote Encryption Management SDK (Under development)
• ATA-over-LAN Bridge Application
• ATA-over-LAN Bridge DLL
• Remote Encryption Management Image (ISO)
• Remote Encryption Management Utility (Demo Security Console)
• AMT Stack DLLs

Remote Encryption Management SDK will be available on the Manageability site.
# Remote Encryption Management SDK Components

<table>
<thead>
<tr>
<th>Remote Encryption Management Component Name</th>
<th>Description</th>
<th>SDK Kit</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATA-over-LAN Bridge Application</td>
<td>An unmanaged/native application that may be hosted within the Remote Encryption Management Image. The purpose of this component is to enable management of remote encryption hard technologies via Intel® AMT.</td>
<td>Remote Encryption Management</td>
</tr>
<tr>
<td>ATA-over-LAN Bridge DLL</td>
<td>A Windows .NET Framework DLL that provides the supporting interfaces and methods for the unmanaged/native ATA-over-LAN Bridge application. This component allows 3rd party applications to leverage the ATA-over-LAN Bridge application for the purpose of remote encryption management.</td>
<td>Remote Encryption Management</td>
</tr>
<tr>
<td>Remote Encryption Management Image (ISO)</td>
<td>A Linux-based CD-ROM ISO image file that will host the unmanaged/native ATA-over-LAN Bridge application. This image will be used for remotely booting an Intel® AMT system via serial over LAN (SOL) and IDE redirection (IDE-R) and would not be installed or otherwise persist beyond the intended usage of remote encryption management.</td>
<td>Remote Encryption Management</td>
</tr>
<tr>
<td>Remote Encryption Management Utility (Demo Security Console)</td>
<td>A Windows .NET Framework application (command line or graphical interface) that provides the complete functionality for remote disk encryption drive management using the other components.</td>
<td>Remote Encryption Management</td>
</tr>
<tr>
<td>AMT Stack DLLs</td>
<td>AMT routines used to connect to the remote, establish SOL, determine client power state, etc.</td>
<td>Remote Encryption Management</td>
</tr>
</tbody>
</table>
Serial-over-LAN (SOL)
IDE-redirect (IDE-r)
SOL/IDE-R in Remote Encryption Management

• Your console uses IDE-R to boot the client to the Remote Encryption Management ISO

• Remote Encryption Management uses SOL/IDE-R for Remote Management of:
  – Seagate* DriveTrust* Devices
  – Opal* Devices

• The network connection between the ISV Console and the encrypted (locked) device is by SOL
IDE Redirection

• IDE Redirection (IDE-R)
  – Capability of emulating an IDE CD drive or a legacy floppy or LS-120 drive over a standard network connection
  – Enables a management machine to attach one of its local drives to a managed client over the network
  – Managed client can use the remote device as if it were directly attached to one of its own IDE channels
  – Based on SOL/IDE-R Protocol

• Reference Documentation
  – Redirection Library Design guide in Intel® AMT SDK
  – Network Interface guide in Intel® AMT SDK
Remote Control - IDE-Redirection

Helpdesk connects to ME
Separate PCI function supports standard IDE register set
Boot option can be remotely set to indicate to BIOS that it should Boot from IDE-R
ISV SW integration needed – Intel supports both and ISVs
Speed CDx7

BIOS

OS
(IDC Class Driver)

<interface>
IDE Class Interface

ME
(IDER/SOL)

(OOB Network Stack)

Helpdesk PC

IDER Service

Image Stream

SOAP

TLS/TCP
Serial-Over-LAN

• Serial-Over-LAN (SOL)
  – Capability to send console text to a remote destination and to receive keystrokes from a remote source
  – Emulates serial port communication over a standard network connection
  – Implemented using a virtual serial port
  – Works without operating system
  – Based on SOL/IDE-R protocol
Remote Control - SOL

Manageability Engine (ME) listens on TCP port
- Helpdesk connects to ME
Separate PCI function supports standard 16550 COM port registers
Boot option can be remotely set to indicate to BIOS to enable SOL
- Text based:
  - BIOS configuration screens
  - DOS console
  - OS EMS redirection

<table>
<thead>
<tr>
<th>&lt;interface&gt;</th>
<th>Serial Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS (Console Redirect)</td>
<td>Remote Control Application OS</td>
</tr>
<tr>
<td>ME (IDER/SOL)</td>
<td>(OOB Network Stack)</td>
</tr>
</tbody>
</table>

Helpdesk PC
- SOL Service
- SOL Stream
Remote Encryption Management SDK Flow

ISV console checks the power state of the client (GetSystemPowerState)

ISV console Enables IDE redirection to HLK ISO
StartRedirect(floppyImage, IDErTmage,IDER_SET_ONRESET)

ISV console Enables SOL for communication to Remote Encryption Management ISO (StartSerialRedirect)

ISV console sends remote wake command to client (SendRemoteControl)

HLK ISO boots up and loads ATA over LAN Bridge

ATA over LAN bridge listens for SOL communication, interprets the command, writes data to the drive

ISV console sends the command to reboot the client
Thank you for attending
Intel® vPro™ Technology Virtual Seminar 2010

Intel® Active Management Technology (Intel ® AMT) Developer Resources

− Intel Software Network Manageability Community: www.software.intel.com/en-us/manageability/
− ISN Manageability Forums: www.intel.com/software/manageability/forums
− ISN Manageability Blogs: www.intel.com/software/manageability/blogs
− Intel ® vPro™ Expert Center: www.communities.intel.com/community/openportit/vproexpert
− Intel Software Partner Program: www.intel.com/partner
Notices

- Copyright © 2010, Intel Corporation. All rights reserved.
- Intel®, Xeon® and Core Inside are trademarks of Intel Corporation in the U.S. and other countries.
- *Other names and brands may be claimed as the property of others
- Intel processor numbers are not a measure of performance. Processor numbers differentiate features within each processor family, not across different processor families. Go to: [http://www.intel.com/products/processor-number/](http://www.intel.com/products/processor-number/)
- Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance. Buyers should consult other sources of information to evaluate the performance of systems or components they are considering purchasing. For more information on performance tests and on the performance of Intel products, Go to: [http://www.intel.com/performance/resources/benchmark_limitations.htm](http://www.intel.com/performance/resources/benchmark_limitations.htm)
- Results have been simulated and are provided for informational purposes only. Results were derived using simulations run on an architecture simulator or model. Any difference in system hardware or software design or configuration may affect actual performance.
- Results have been simulated and are provided for informational purposes only. Results were derived using simulations run on an architecture simulator or model. Any difference in system hardware or software design or configuration may affect actual performance.
- 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 go to: [http://www.intel.com/#en-US-01](http://www.intel.com/#en-US-01)