Technology Brief

All new 2010 Intel® Core™ Processor family

Intel® Anti-Theft Technology

Protect Laptops and Data with Intel® Anti-Theft Technology

It's not your PC, it's your business. Lock it tight.

Keeping data secure in a mobile environment is not only a daunting challenge, but a critical requirement. HITECH, HIPAA, data-breach notification rules, and other increasingly stringent regulations in data security and privacy have added complexity for companies with mobile users. Loss and theft of systems and data is not only costly to your company, but can result in financial or legal exposure, and cause significant disruptions to business.

Laptops with a new 2010 Intel® Core™ processor with Intel® Anti-Theft Technology[1] (Intel® AT) provide IT administrators with intelligent protection of lost or stolen assets. Intel AT gives you the ability to disable your PC with a local or remote poison pill if the system is lost or stolen. This poison pill can delete essential cryptographic material from system hardware in order to disable access to encrypted data stored on the hard drive.[2] The poison pill can also block the laptop's boot process, rendering the system a "brick." Because the technology is built into PC hardware, Intel AT provides local, tamper-resistant protection that works even if the OS is reimaged, the boot order is changed, a new hard-drive is installed, or the laptop is disconnected from the network.

Local and remote detection mechanisms

Intel AT includes several hardware-based detection mechanisms to detect potential loss/theft situations. When a suspicious situation is identified, Intel AT can activate "theft mode" and respond according to your company's information technology (IT) policies. Because Intel AT has a flexible policy engine, you can specify the detection mechanism that asserts theft mode, the thresholds for timer intervals, and the theft-response action(s) to take. (See response mechanisms later in this brief.)

Detection of potential loss or theft can take place locally or remotely. For example, detection can occur based on local policy, or via a remote connection over the Internet to the theft-management server. Hardware-based detection and trigger mechanisms include:

- **Local: Excessive login attempts in the PBA (preboot authentication) screen.** The laptop enters theft mode after an IT-specified number of login failures in the PBA screen, and responds as specified by IT policy.

Intel® Anti-Theft Technology Feature[1]	How It Works	Benefit
PC disable	Local or remote poison pill renders the PC inoperable by blocking the boot process.	▪ Minimizes the potential of a stolen laptop being used and sensitive data being accessed by an unauthorized person. ▪ PC disable can be triggered locally or remotely.
Data access disable	Local or remote poison pill deletes essential cryptographic material, which is stored in hardware, thereby disabling access to encrypted data stored on the hard drive.[2]	▪ Fast, more secure way to protect encrypted data from unauthorized access, including disgruntled employees with access to passwords or in situations when a password has been compromised. ▪ Allows encryption solutions to store and manage essential cryptographic material in hardware (which is more secure than software), instead of solely on the hard disk. ▪ Tamper-resistant.
Reactivation	Return laptop to full functionality via: ▪ Local passphrase that was pre-provisioned by user. ▪ Recovery token (one-time use) provided by IT.	▪ Simple, rapid, inexpensive way to restore laptop to full functionality without damage to the PC or the data once it is in the hands of the authorized user.

Industry support and software development

- Intel® Anti-Theft Technology (Intel® AT) works independently of a Trusted Platform Module (TPM). You do not need TPM in order to take advantage of Intel AT. Intel AT also works independently of Intel® Active Management Technology (Intel® AMT).[3]
- Intel AT is designed to be easily integrated into existing solutions. Theft-management and security vendors who support Intel AT include Absolute Software Corporation, Phoenix Technologies, and WinMagic. Additional security ISVs, such as PGP, are planning to offer solutions in 2010.
- Laptops enabled with Intel AT are available from many OEMs. Visit http://intel.com/go/anti-theft for a list of OEM systems that support Intel AT. These laptops require specific Intel AT-capable BIOS and firmware versions, which will be included with the platform or available from the OEM as an update (please consult with the OEM).

- **Local: Rendezvous Timer.** IT can use this timer to help identify situations in which a laptop might not be under control of the authorized user. For this mechanism, the IT administrator (or IT service provider) defines a timeframe in which the laptop must check in (rendezvous) with the central server via the Internet. If the laptop does not communicate with the central server in the specified timeframe, the local timer expires. The laptop then enters theft mode and responds as specified by IT policy. Because timer expiry is a locally defined policy in hardware, the laptop can lock itself down even if the thief does not connect to the Internet.
- **Remote: Notification (encrypted) from the central server via wired or wireless LAN (IP Network).** Once notified of a laptop's loss or theft, the IT administrator can flag the laptop in the central server. The next time the system connects to the Internet, the laptop contacts the central server, synchronizes with the server, and receives an encrypted instruction to enter theft mode. The laptop then responds as specified by IT policy. (Companies/solution providers can host the central server on the Internet in order to allow communication with laptops outside the corporate firewall.)
- **Remote: Notification via encrypted SMS text message via 3G network.** Laptops with a 3G-enabled card can receive encrypted SMS text messages sent from the central server, even if the laptop is not connected to the Internet. As long as the laptop's operating system (OS) is functioning and is within the range of a 3G network, IT administrators can use this feature to send an encrypted SMS notification (a poison pill) to the laptop through a 3G network. The laptop then goes into theft mode and responds as specified by IT policy.

A key benefit of the Intel AT hardware-based detection mechanisms is that they can work even if a network connection is not available. They can also integrate with existing encryption solutions' PBA modules.

Flexible responses adapt to your needs

Intel AT provides IT administrators with flexible options for several automated loss/theft responses. These responses can be activated locally and automatically (based on the detection mechanism), or can be activated remotely by IT. Responses include:

- **Disable access to encrypted data,** by deleting essential elements of cryptographic materials that are required to access encrypted data on the hard drive.
- **Disable the PC ("poison pill"),** by blocking the boot process. Because the boot process itself is blocked, this response can work regardless of boot device (secondary hard drive, removable drive, CD, DVD, USB key, and so on). Because the boot process is blocked through the laptop's hardware, this response also works even if the boot order is changed or the hard drive is replaced or reformatted.
- **Disable both the PC and access to encrypted data.** Erases essential elements of cryptographic material and disables the PC by blocking the boot process.
- **Customizable "theft mode" message.** IT administrators can customize the message that is displayed after the laptop enters theft mode. For example, an IT administrator could define a message that says, "This laptop has been reported missing. Please call 1-800-555-1234 to return the system to ACME Corp."

IT can combine responses to provide different levels of lockdown for different users.

Excessive login attempts can trigger PC disable

In this example, an engineer's laptop and wallet is stolen in an airport, and the thief, after moving quickly to a better location, tries to log in to the PBA module using information from the engineer's wallet. However, based on IT policy, after five failed login attempts, the system reboots. After five more failed login attempts, the Intel AT trigger is tripped, the system enters theft mode and locks itself down. In this case, part of the user password required to access the engineer's encrypted hard drive is erased from hardware, and the PC's boot process is disabled. Even if the thief removes the hard drive and installs the drive in another device, the security credentials that provide access to encrypted data have been disabled. Until reactivated by the authorized user or IT, the PC will not boot, and the cryptographic material remains disabled so that the encrypted data cannot be accessed even through another PC.

Failure to check-in with the central server can trigger PC disable

In another example, a research scientist's laptop contains highly sensitive data about a new invention. In this case, IT has defined the policies on the scientist's laptop to require that the scientist log in daily. During a family event, the scientist takes time off and does not log in for two days. Based on locally stored policy for the rendezvous with the server, the rendezvous timer expiry threshold is reached. The laptop enters theft mode, disables itself, and renders the data inaccessible by erasing from hardware part of the encryption key and biometric data required to access the scientist's encrypted files. Even if the laptop is removed from the lab while the user is away, the laptop has secured itself until the scientist returns and reactivates the system.

Easy, rapid reactivation and full system recovery

To help return a laptop to service, Intel AT includes several mechanisms for easy, rapid reactivation:

- **Local passphrase,** which is a strong password pre-provisioned in the laptop by IT or by the user. To reactivate the system, the user simply enters this passphrase in a special pre-OS reactivation screen (via BIOS or a PBA module).
- **Reactivation code,** which is generated by IT or by the user's service provider via the theft-management console, upon request by the user. For reactivation, a one-time reactivation code is provided to the user via phone or other means. The user simply enters the code in the special pre-OS reactivation screen (via BIOS).
- **PBA-based authentication process.** Some PBA modules allow the IT administrator (or IT service provider) to define additional reactivation processes. These could include a security question, a set of challenge-response questions and answers, or a combination of passwords, biometric authentication, and/or token authentication to complete reactivation. PBA-based reactivation gives IT the flexibility to establish a robust reactivation process in a pre-OS environment the user is already familiar with (this is the user's typical pre-OS screen for authenticating access to the main OS).

Reactivation returns the PC to full functionality and offers IT several simple, inexpensive methods of returning the laptop to normal operation without compromising sensitive data or the system's security features.

Intel® Anti-Theft Technology: Intelligent protection and simple, rapid reactivation

Encryption provides strong protection of data – as long as the encryption keys and/or passwords themselves are not compromised. Intel AT takes security one step further and gives IT the ability to rapidly and automatically – as well as locally or remotely – disable and reactivate the PC itself. After a data disable command is executed, even if an encryption password is known, encrypted data remains protected. After a PC-disable, the system is locked down until the user is reauthenticated. Businesses now have built-in client-side intelligence to help secure sensitive data regardless of the state of the OS, hard drive, boot order, or network connectivity. This hardware-based technology provides compelling tamper-resistance and increased protection to extend your security capabilities anywhere, anytime, on or off the network, and minimize your business risk.

[1] No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology (Intel® AT) for PC protection requires the computer system to have an Intel® AT-enabled chipset, BIOS, firmware release, software and an Intel AT-capable Service Provider/ISV application and service subscription. Intel AT performs the encrypted data access disable by preventing access to or deleting cryptographic material (e.g., encryption keys or user credentials) required to access previously encrypted data. ISV-provided Intel-AT-capable encryption software may store this cryptographic material in the PC's chipset. In order to restore access to data when the system is recovered, this cryptographic material must be escrowed/backed up in advance in a separate device or server provided by the security ISV/service provider. The detection (triggers), response (actions), and reactivation mechanisms only work after the Intel AT functionality has been activated and configured. The activation process requires an enrollment procedure in order to obtain a license from an authorized security vendor/service provider for each PC or batch of PCs. Activation also requires setup and configuration by the purchaser or service provider and may require scripting with the console. Certain functionality may not be offered by some ISVs or service providers. Certain functionality may not be available in all countries. Intel assumes no liability for lost or stolen data and/or systems or any other damages resulting thereof.

[2] Essential cryptographic material includes anything that is essential to access the encrypted drive, including part of the encryption key, user credentials, biometric information, or other cryptographic material.

[3] Intel® Active Management Technology (Intel® AMT) requires the computer system to have an Intel® AMT-enabled chipset, network hardware and software, as well as connection with a power source and a corporate network connection. Setup requires configuration by the purchaser and may require scripting with the management console or further integration into existing security frameworks to enable certain functionality. It may also require modifications of implementation of new business processes. For more information, see www.intel.com/technology/platform-technology/intel-amt/.

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

Printed in USA 0210/MC/OCG/XX/PDF ♻ Please Recycle 323358-001US