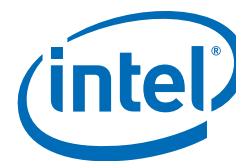


Technology Brief

Intel® Centrino® 2 Processor Technology

Intel® Anti-Theft Technology



Protect Notebooks and Data with Intel® Anti-Theft Technology

Keeping data secure in a mobile environment is not just a daunting challenge, but a critical requirement. Complying with increasingly stringent regulations in data security and privacy adds additional complexity for companies with mobile users. At the same time, loss and theft of systems and data can be costly to IT, result in financial or legal exposure, and cause significant disruptions to business.

The latest Intel® Centrino® 2 processor technology-based notebooks include innovative Intel® Anti-Theft Technology¹ (Intel® AT). Intel AT gives you the ability to disable your PC if it is lost or stolen. A local or remote poison pill can delete or block access to software-based encryption keys (or other critical cryptographic material), thereby disabling access to encrypted data stored on the hard drive. Because the technology is built into PC hardware, it provides local, tamper-resistant defense that works even if the OS is reimaged, a new hard-drive is installed, or the notebook is disconnected from the network.

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 IT policy. Because Intel AT has a flexible policy engine, you can specify which detection mechanism should be used to assert theft mode, the thresholds for time intervals, and which action(s) to take.

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

- **Excessive login attempts** — The system is disabled after an IT-determined number of login failures in the pre-OS login screen (the preboot authentication module, or PBA).
- **Timeframe rendezvous requirement** — The system can be disabled if the notebook does not periodically rendezvous with a central server within the IT-specified time interval. To help identify unauthorized access to the system, Intel AT includes three programmable, interdependent hardware-based timers: a rendezvous timer (tracks the frequency of communication with the central server), a disable timer (specifies the interval after which to lock down the system after the rendezvous is missed), and an unlock timer (specifies the interval after a lock-down, in which the user is allowed to unlock the system).
- **Notification from the central server** — After being notified of the notebook’s loss or theft, IT flags the notebook in the central server database. The next time a “user” connects the system to the Internet, the notebook contacts and synchronizes with the central server. When Intel AT receives notification from the server that the notebook has been tagged as stolen, Intel AT disables the PC and/or disables access to data, according to IT policy. (Security vendors/ service providers can host the central server on the Internet in order to allow communication with notebooks outside the corporate firewall.)

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

Intel® Anti-Theft Technology Feature ¹	How It Works	Benefit
PC disable	Local or remote poison pill renders the PC inoperable by blocking the OS from booting.	<ul style="list-style-type: none">▪ Minimizes the potential of a stolen notebook being used and sensitive data being accessed.▪ PC disable can be triggered locally or remotely.
Data access disable	Local or remote poison pill deletes or blocks access to software-based encryption keys (or other critical cryptographic material), thereby disabling access to encrypted data stored on the hard drive.	<ul style="list-style-type: none">▪ Fast, more secure way to protect encrypted data from unauthorized access.▪ Allows you to escrow software-based encryption keys or other critical cryptographic material in hardware (which is more secure), instead of on the hard disk.▪ Tamper-resistant.
Reactivation	Return notebook to full functionality via: <ul style="list-style-type: none">▪ Local passphrase that was preprovisioned by user.▪ Recovery token (one-time use) provided by IT.	<ul style="list-style-type: none">▪ Simple, inexpensive way to restore notebook to full functionality without compromising local security features for data access disable or PC disable.

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 AT is designed to be easily integrated into existing solutions. Theft-management software vendors who support Intel AT include Absolute Software Corporation and Phoenix Technologies Ltd. Additional security ISVs are planning to offer solutions in 2010.
- Intel® Centrino® 2 processor technology-based notebooks with Intel AT capabilities are now available from Lenovo and Fujitsu Computers. These systems 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). Additional OEMs, such as Panasonic and Acer, are planning to offer Intel AT-ready notebooks in late 2009.

Local and remote responses

There are several automated loss/theft responses available to IT administrators. These responses can be activated locally and automatically (based on the detection mechanism), or remotely by IT. The responses are also flexible and can be programmed to:

- **Disable access to data**, by deleting software-based encryption keys or other cryptographic credentials required to access encrypted data on the hard drive.
- **Disable the PC**, by blocking the boot process, even if the hard drive is replaced or reformatted.
- **Disable both the PC and access to data**. Erases encryption keys and disables the PC.

Excessive login attempts can trigger PC disable

Disabling a PC after excessive login attempts in the PBA module can be an effective way to prevent loss of encrypted data. For example, an engineer's notebook and wallet might be stolen in an airport. The thief might try to log in using information from the engineer's wallet, but – based on IT policy – after five login attempts, the Intel AT trigger is tripped, and the system locks down. In this case, encryption keys for encrypted data are erased from the chipset, and the PC is disabled. Even if the thief removes the hard drive and installs it

in another device, the security credentials that provide access to encrypted data on the hard drive have been erased and cannot be stolen. Until reactivated by the authorized user or IT, the PC will not boot, and the encrypted data cannot be accessed.

Local timer expiry can trigger PC disable

In another example, a research scientist's notebook might contain highly sensitive data about a new invention. In this case, IT has defined the triggers on the scientist's notebook 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 timer expiry threshold is reached, the notebook enters "theft mode," disables itself, and erases the encryption keys for encrypted data on the hard drive. Even if the notebook is removed from the lab while the user is away, the notebook has secured itself until the scientist returns and reactivates the system.

Easy reactivation and full system recovery

To speed up recovery when a notebook is being returned to service, Intel AT also includes two rapid reactivation mechanisms:

- **Local passphrase**, which is a strong password preprovisioned in the notebook by the user. To reactivate the system, the user simply enters this passphrase in a special pre-OS login screen.
- **Recovery token**, 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 recovery token is provided to the user via phone or other means, and the user enters the token in a special pre-OS login screen.

Both passphrase and recovery token return the PC to full functionality and offer simple, inexpensive methods of recovering the notebook without compromising sensitive data or the system's security features.

Intel® Anti-Theft Technology: Built-in protection and reactivation

With Intel AT, businesses now have built-in client-side intelligence to help secure sensitive data regardless of the state of the OS and 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 business risk.

¹No 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) 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 recovery 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.

*Other names and brands may be claimed as the property of others. Copyright © 2008 Intel Corporation. All rights reserved.

