

## Evaluating Intel® Anti-Theft Technology

- Available on laptop PCs with 2010 Intel® Core™ vPro™ processors.
- Disables hardware as well as stored data if lost or stolen.
- Provides multiple layers of protection including theft detection and easy restoration of platform and data to original state.

Intel IT recently completed a technology evaluation of Intel® Anti-Theft Technology (Intel® AT), available on laptop PCs with 2010 Intel® Core™ vPro™ processors.

Intel AT is a hardware-based technology that can help detect theft and disable a laptop if it is lost or stolen, as shown in Figure 1. This protects valuable enterprise data and intellectual property as well as the hardware itself. Additionally, Intel AT adds value to full-disk encryption by protecting data even if the encryption keys are compromised. We worked with our encryption supplier during the development of Intel AT to help define the features required for enterprise use.

In our evaluation, we worked with the Intel AT product group and our encryption supplier to test features over our wireless LAN (wLAN), LAN, and virtual private network (VPN), based on a possible enterprise use case in which a Service Desk technician disables a stolen laptop.

The results of our evaluation indicate that Intel AT will improve our ability to protect company-owned laptops as well as data and intellectual property. We plan to test the same features over a mobile 3G network in the near future.

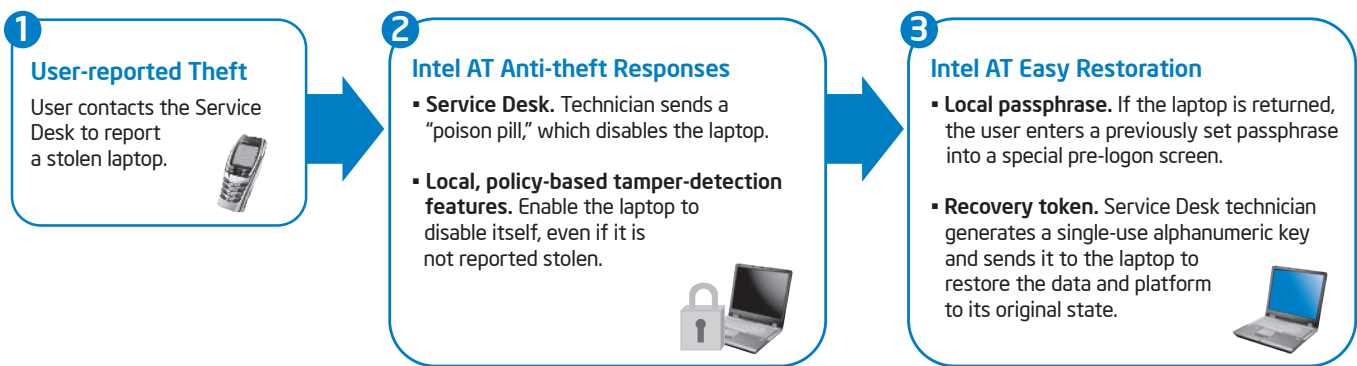


Figure 1. Intel® Anti-Theft Technology (Intel® AT) can help detect theft and disable a laptop if it is lost or stolen.

## Business Challenge

Each year, 2 million laptop PCs are stolen, and 97 percent of these are never recovered.<sup>1</sup> This represents a huge risk to enterprises in terms of lost hardware and, more importantly, lost data and intellectual property.

Intel IT is responsible for investigating potential impacts on the enterprise of all lost and stolen company-owned PCs. We investigate tools and practices that help avoid these risks, and we are interested in assessing Intel AT toward this end.

## Defining Intel AT Requirements and Features

In December 2008, we began working with the Intel AT product group to help define and evaluate Intel AT. In 2009, the product group asked us to work with our encryption supplier to help define an architecture that might make Intel AT more valuable in an enterprise environment.

We worked with the supplier in a series of face-to-face planning meetings to define enterprise-level requirements and features. These meetings focused on topics such as:

- How and where an Intel AT console would fit in the enterprise network.
- Security requirements associated with access controls and event logging.
- Enterprise requirements, including scalability, so that Intel AT meets the needs of as many clients as possible.
- A hierarchical management interface for establishing policy and for reporting.

The combined team also discussed how companies that do not outsource or host an anti-theft service through an outside supplier would use Intel AT.

## Technology Overview

Intel AT can mitigate laptop theft and loss scenarios by providing multiple layers of protection to the hardware and stored data.

### THEFT DETECTION

When users report that a laptop has been stolen, Service Desk technicians can send a remote theft alert to the laptop that disables it. Intel AT can also use programmable triggers to detect suspicious behavior and disable a laptop locally. Intel AT works in three ways:

- **User-reported theft.** If the laptop owner contacts the Service Desk, a technician can send a “poison pill” to disable the laptop. The poison pill, served in the form of an encrypted Short Message Service (SMS) text message, can be delivered over a LAN, WLAN, or 3G network.
- **Tamper detection using the local grace timer.** In the event of suspicious activity, such as excessive attempts to log on to the network or a longer-than-usual amount of elapsed time before credentials are entered, the laptop disables itself using its programmable grace timer.
- **Tamper detection using the local rendezvous timer.** If the laptop does not log on to the network within a period of time set by policy, such as daily, it disables itself using the programmable local rendezvous timer.

Intel AT can block the OS from loading, even if the hard drive is replaced or reformatted. Intel AT can also be used to disable access to data encryption keys and block access to valuable data on the hard drive, even if the drive is moved to a different system.

### EASY RESTORATION

A disabled laptop can display a customizable recovery message with contact information to help return the laptop to its rightful owner. Once the laptop is back in its owner’s hands, it can be restored without damage to the hardware or data by using one of two techniques:

- **Local passphrase.** Users set a strong passphrase in advance, to be used in a special pre-logout screen.
- **Recovery token.** A Service Desk technician generates a single-use alphanumeric key and provides it to the user.

### TAMPER RESISTANCE

Intel AT provides several features that thwart attempts to circumvent its anti-theft capabilities. Once Intel AT has been enabled in the BIOS, had the correct firmware installed on the platform, and has enrolled with a central console, the capability will continue to work even if the BIOS is flashed or the complementary metal-oxide-semiconductor (CMOS) battery is removed. Tamper-resistant capabilities make it more difficult for thieves to circumvent platform and data protections.

### SYSTEM REQUIREMENTS

Intel AT is available on laptop PCs with 2010 Intel Core vPro processors.

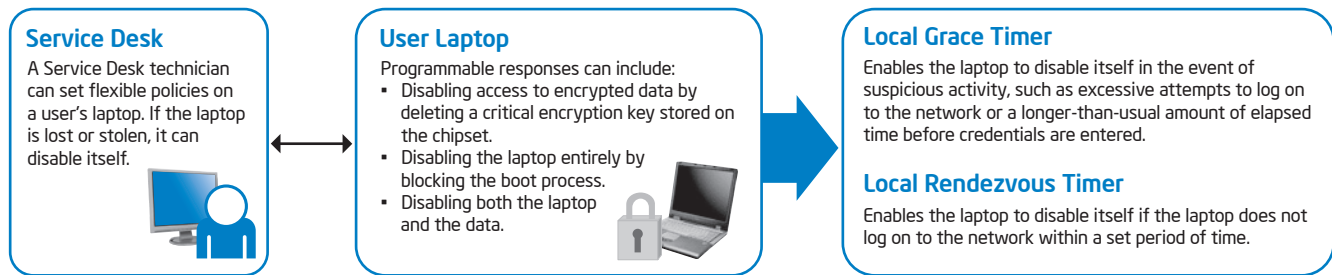


Figure 2. Intel® Anti-Theft Technology allows Service Desk technicians to set flexible, policy-based responses to laptop theft.

## Technology Evaluation

Working with the product group and our encryption supplier, we tested various features of Intel AT on our WLAN, LAN, and VPN. We also brainstormed additional use cases, such as investigations support, and discussed the potential integration of Intel AT with other enterprise security capabilities.

Our evaluation was based on a theoretical use case in which a user calls the Service Desk and reports the laptop stolen. In response, the Service Desk technician sends a poison pill from the IT management console. The poison pill disables access to the encryption keys by deleting a critical encryption key stored on the chipset. We also tested reactivating a disabled laptop using both a local passphrase and a remote recovery token to restore access to the encryption keys.

### TEST SETUP AND CONFIGURATION

We successfully activated, configured, and enrolled Intel AT on multiple systems.

- **Activation.** We first made sure that each test laptop had the appropriate level of BIOS. Then we enabled Intel AT in the BIOS using a couple of configuration switches.

- **Configuration.** We verified that the correct level of firmware was included on each test laptop. We then installed the Intel AT test agent across several versions of the client OS and on laptops from several OEMs.
- **Enrollment.** We were able to obtain a license key for each installation by using our supplier's console and connecting to Intel's Capability Licensing Service. This happened seamlessly; we also tested de-enrolling and re-enrolling a laptop.

This process enabled us to determine the level of complexity involved in using Intel AT and to map out a possible process our PC build team could use as they receive new laptops.

### FEATURE EVALUATION SUMMARY

We successfully tested the key features of Intel AT.

- **Poison pill.** We simulated a stolen laptop in order to trigger various Intel AT behaviors. We sent an encrypted SMS message to the "stolen" laptop to disable it.
- **Local grace timer.** We simulated a user taking too long to enter credentials, after which time the laptop disabled itself as expected.

- **Local rendezvous timer.** We simulated a user not logging on within a specified period of time, which disabled the laptop.
- **Local passphrase.** We used a local passphrase for self-recovery after an expired grace timer and a missed rendezvous timer.
- **Recovery token.** We simulated finding a lost or stolen laptop and sending the recovery token to the laptop to restore the data and platform to its original state.

We also tested the ability to set flexible anti-theft policies from the test console by switching policy settings for the grace and rendezvous timers, as shown in Figure 2. For example, once a laptop is marked "stolen," responses can include:

- Disable access to encrypted data by deleting a critical encryption key stored on the chipset.
- Disable the laptop entirely by blocking the boot process.
- Disable both the laptop and the data.

We plan to test these same features and policy settings over a 3G network in the near future.

## Conclusion

Intel IT's collaboration with the Intel AT product team and encryption supplier was important in defining Intel AT. This product has the potential to improve our ability to protect Intel data and intellectual property.

While hard-drive encryption is a valuable approach to data security, the ability of Intel AT to further make the encryption keys inaccessible extends the value of encryption. With Intel AT, encryption keys can be deleted remotely—and

automatically. Without the encryption keys, there is no way an unauthorized user can access the data. Even more importantly, unlike software-based anti-theft solutions, Intel AT is hardware-based and enables the encryption keys to be restored in the event that the platform is recovered.

## For More Information

To learn more and watch an Intel AT demo, visit [www.intel.com/technology/anti-theft](http://www.intel.com/technology/anti-theft).

For more straight talk on current topics from Intel's IT leaders, visit [www.intel.com/it](http://www.intel.com/it).

## AUTHORS

**Dennis Morgan**  
Security Strategist, Intel IT

**Alan Ross**  
Senior Principal Engineer, Intel IT

**Tarun Viswanathan**  
Security Architect, Intel IT

## ACRONYMS

**CMOS** complementary metal-oxide-semiconductor

**Intel® AT** Intel® Anti-Theft Technology

**SMS** Short Message Service

**VPN** virtual private network

**WLAN** wireless LAN

<sup>1</sup> Evers, Joris. "Getting over laptop loss." CNET News. June 30, 2006. [http://news.cnet.com/Getting-over-laptop-loss/2100-1044\\_3-6089921.html](http://news.cnet.com/Getting-over-laptop-loss/2100-1044_3-6089921.html)

No computer system can provide absolute security under all conditions. Intel® Anti-Theft Technology 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. The detection (triggers), response (actions), and recovery mechanisms only work after the Intel® AT functionality has been activated and configured. Certain functionality may not be offered by some ISVs or service providers and 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.

This paper is for informational purposes only. THIS DOCUMENT IS PROVIDED "AS IS" WITH NO WARRANTIES WHATSOEVER, INCLUDING ANY


WARRANTY OF MERCHANTABILITY, NONINFRINGEMENT, FITNESS FOR ANY PARTICULAR PURPOSE, OR ANY WARRANTY OTHERWISE ARISING OUT OF ANY PROPOSAL, SPECIFICATION OR SAMPLE. Intel disclaims all liability, including liability for infringement of any proprietary rights, relating to use of information in this specification. No license, express or implied, by estoppel or otherwise, to any intellectual property rights is granted herein.

Intel, the Intel logo, Intel Core, and Intel vPro are trademarks of Intel Corporation in the U.S. and other countries.

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

Copyright © 2010 Intel Corporation. All rights reserved.

Printed in USA  
0710/JLG/KC/PDF

 Please Recycle  
323947-001US

