

Virtual Conference Series: Securing Your Environment with Intel(R) Anti-Theft Technology

Securing Your Environment with Intel® Anti-Theft Technology

Aired live June 23, 2009 9:00 am PDT

Recording now available! [Click to watch the recorded webinar.](#)

Today's business environment is extremely difficult. All types of organizations are being asked to do more with less. And with the cost and impact of PC theft, security has become even more important to corporations and IT leaders. Join us to hear how IT professionals can take advantage of new technologies to protect their business.

Impact of Data Breaches

Dr. Larry Ponemon, Chairman and Founder of the Ponemon Institute, will share information from his annual study on the cost of data breaches; the associated financial impacts to business, the threat of customer turnover as well as preventative solutions. The Ponemon institutue is a research "think tank" dedicated to advancing privacy and data protection practices. [Click here to read the study.](#)

Intel Anti-Theft Technology

Intel Solution Architect, Mike Schulien, will discuss how Intel's latest security innovation, Intel® Anti-Theft Technology, can combat security breaches by strengthening PC hardware and security solutions. This new hardware-level

technology will shut down a PC and/or its data if it is lost or stolen with the ability to reactivate it if it is recovered.

Computrace Software from Absolute

Geoff Glave, Absolute Software Product Manager, will talk about how IT administrators can use Computrace, Absolute's leading IT asset-management

and security solution, to secure their assets remotely, automatically locking down a system quickly in case of theft or suspicious circumstances. Computrace technology is the leading security service now using Intel® Anti-Theft Technology. [Click here to read the white paper.](#)

Question & Answer Section

Ponemon Institute Q&A:

Did any of these lost laptops include units with the onboard anti-theft tracking hardware?

Of the 138 lost or stolen laptop cases investigated by Ponemon Institute, two had anti-theft solutions. In both cases, the cost of lost laptops was simply replacement value.

Have you done any studies of BitLocker vs other hard drive encryption software?

No. We have not done any study concern BitLocker. We have completed numerous students on encryption, including whole disk encryption solutions such as PGP.

Was the cost of a lost laptop higher than you expected?

Yes. We did, however, expect the total cost to be much higher than the computer's replacement value. An average cost of approximately \$50k was about three-times what we anticipated before launching the study.

If the number of benchmark companies is 29 with 138 laptop cases, is this enough to draw valid conclusions?

The unit of analysis in this study is each lost or stolen laptop (and not each company). Our research design required benchmark sampling methods rather than a scientific sample. So, we need to be cautious about broad generalizations from this work. We discuss these caveats in our final report.

Were you able to determine if certain IP is more costly when on a lost laptop than other types?

We found certain types of IP, specifically software source code, product design documents, and strategic planning materials were enormously expensive to companies – but only when the laptops containing these documents were determined to be stolen rather than lost. As expected, technology and service organizations experienced the highest IP losses.

Why is the cost of a lost manager's/director's laptop higher than a senior executive's lost laptop?

Our analysis shows that C-level executives are more likely to have whole disk encryption installed on their laptops than individuals at lower organizational levels. In addition, executives are less likely to have detailed data such as customer or employee level information.

Why do you think the anti-deterrent label was so successful in discouraging laptop theft?

I think that most people are honest and, hence, unlikely to steal a laptop with or without a conspicuous anti-theft label. However, the small group of people motivated to steal are likely to “think twice” when they believe the laptop computer is fully secure and unavailable to them.

Intel Q&A:

AT Technology is present only in v-PRO machines, or non-vPRO can also have it ?

Today only Intel® vPro™ technology- based notebooks offer the Intel® Anti-Theft Technology (Intel® AT), going forward with our next generation Processor both the desktop and notebook will offer Intel® AT and there will be a non-vPro (consumer) SKU as well.

What inherent protections are provided to ensure the hardware elements of the AT-p technology are not maliciously activated by a threat agent?

The Intel AT can only be activated by an Intel signed application – Absolute's Computrace applications gets its security certificate from an Intel Backend signing server. Going forward as more ISV's come on board the same Security Certificate (Intel Signing Authority server) will be required.

What does poison pill do to the laptop? Is it physically useless? Can it be reset if recovered and reused?

The poison pill sends a secure lock code to the PC that causes the Intel Management Engine to disable the Intel Chipset, the PC becomes physically "bricked" or useless. Once the PC is recovered a recovery code from the ISV will unlock the PC and usage would return as normal.

Will AT be offered in other platforms beside vPro (like Classmate PC)?

While this is being discussed for most Intel based Platforms and there will be a consumer based solution in the near term, no actual commitment has been made for the Classmate.

How does the encryption key escrow methodology interact with disk encryption methodologies utilizing Trusted Platform Modules?

While there may be some interaction the main thrust of the encryption key escrowing will not directly affect TPM. The idea here is to be able to store the encryption key in the actual Management Engine (ME) and when the system is “Bricked” the Encryption Keys will be inaccessible to the hard drive thereby rendering it useless. This is a simplified overview, the exact method is still being worked out.

What happens if you use the one time password? What happens if you need it again?

A new onetime Password would be required; once an OTP is used it is useless. A new OTP would be generated for another unlock – each OTP is unique to the PC that it was generated for , this is accomplished based on the code the PC itself generates when it is in a “Bricked” state.

When will the encryption functionality and key storage capability undergo FIPS 140-2 (or 140-3) validation in order to meet minimum requirements for use by US government agencies?

No time frame is available at this time.

Would AT technology prevent bypassing by booting from a live Linux disc or USB drive?

Yes, Intel AT disables the Chipset from within the chipset, any boot device internal or external would be disabled at the chip level.

Absolute Software Q&A:

Why has the Computrace option activation been taken out of the T8 BIOS?

This question needs to be directed to the OEM (i.e. the computer manufacturer), as we don't have any control over this. Some of the OEMs put it in, some don't

Since you can fairly easily disable computrace in the bios, doesn't this negate the use of the poison pill?

You cannot easily disable Computrace in the BIOS. Once persistence has been turned ON, it cannot be turned off, so no, this does not negate the poison pill.

Please describe what protections are in place to ensure a DNS redirection attack could not be used to force agent reports to a malicious location resulting in an unauthorized 'poison pill' being sent to the enterprise computing base, causing a widely distributed denial of service.

There are many components in both Absolute and Intel's architecture that prevent this.

For example, the Computrace Application Agent will not accept communications from another server unless you know our protocol, and break our encryption. In addition, the rogue server won't have Absolute's private keys or the keys to talk to the Intel server which are also encrypted. If you're able to do all that, come see us. We have a job waiting for you.

Once disabled, if a new hd is put in, is the laptop usable?

No - the AT-lock is a pre-boot lock so the new hard disk is not accessed.

What is the main difference between existing solutions that for example Dell provides together with Absolute and this one with Lenovo?

All of the other solutions that Absolute Software provides depend on disabling the operating system and/or the hard drive. The Intel AT solution "bricks" the device at the pre-boot hardware level. Absolute will support other OEMs as they implement their integrations with the Intel AT chipset.