# Chapter 16

# Privacy Protection in Intel® Active Management Technology

*The things most people want to know about are usually none of their business.*

—George Bernard Shaw

In today's modern society, privacy is essentially someone's right to be left alone to mind their own business. More precisely, an individual's privacy is related to his or her willingness to reveal as much information or as little information about him- or herself to another individual. Privacy also relates to anonymity. If someone is private enough so as not to be noticed in public, then that person can be called anonymous. Unauthorized invasion of privacy is unwelcome in most cultures. Every time that there are moves to encroach upon people's right to privacy, it usually is met with resistance. This makes the topic of privacy a sensitive topic. In general, people are willing to sacrifice their privacy at the airports during body and baggage searches because it helps in providing security and safety during the travel. On the other hand, people in general resist attempts by the police to tap into their telephone lines without obtaining appropriate consent from the courts. The right to privacy and its protection in the technology world is an equally important and hotly debated topic.

## Privacy in the World of Technology

Invasion of privacy has become a major problem in today's electronically dependent and highly connected world. On one hand we love the luxuries offered by our digital lifestyle and are more willing than ever to embrace digitization, thereby creating new paradigms for ourselves. On the other hand, these digital systems on which we entrust our lifestyle are not perfect. When these systems fail it bites us hard. It bites harder if these digital systems accidentally break or are purposely compromised such that an adversary is able to exploit the situation to his advantage, and against the individual.

Security and robustness of the digital systems play an important role in protecting the privacy of individuals and organizations. As an example, it would be disastrous if a major retailer's Web site database of customers' private information (such as their home address, phone number, credit card information, their shopping history, and so on) were to be accessed by a cyber-criminal. Or even worse, if a rogue insider (a disgruntled or ill-motivated employee) stole this information and misused it to even out a grudge, or make financial gains. To prevent such a disaster from ever happening, some online retailers invest a lot of resources to ensure that their systems are secure and robust, while their customers enjoy a rich online shopping experience.

In addition to building secure and robust systems, vendors of digital systems or services also need to make public claims about the privacy protections they offer to their customers. These are usually detailed in their privacy policy declarations that they adopt and commit themselves to. Another aspect that heavily influences privacy protection in digital systems is the user's (the customer or consumer of the product or service) choice and control of using various aspects of the product or service. For example, a customer may choose not to provide any credit card information to shop at Amazon.com. Instead he could send a check to Amazon.com for the purchase. The only drawback is that the order would not ship until the check is received and realized by Amazon.com. So in this case, the customer could trade the order fulfillment duration for privacy protection (of course, assuming that the check is not stolen). Therefore, privacy sensitive systems usually offer their users certain levels of choice and control regarding the nature and amount of information the user wishes to reveal. The level and quality of service the user receives varies accordingly.

**Interesting Reading on Privacy**

Here are some links to interesting privacy related Web sites

- Electronic Privacy Information Center (www.epic.org)
- Privacy.org (www.privacy.org)
- Privacy Rights Clearinghouse (www.privacyrights.org)
- TRUSTe Privacy (www.truste.org)

## Privacy in the Workplace

Workplace privacy is usually a lesser-understood area by many employers and employees. The privacy laws and policies at the workplace vary by geography, country, and culture. For example, there is quite a significant difference between the policy adopted by the European Union (EU) employers and US employers. EU employers have to comply with the EU directive on the protection of privacy for individuals. Under this directive it is illegal for firms to monitor employees' e-mail messages or Internet traffic, or scan employees' computer for files or data without their consent. US employers on the other hand enjoy a more relaxed policy environment and many US firms monitor employees' e-mail messages and/or Internet traffic.

The employer is only one of many entities that can invade privacy of an individual, albeit the employer can do so very easily and stealthily. In large firms, there is usually a department or team that manages the computers and other IT infrastructure. Any ill motivated member of this team could misuse his legitimate access rights and invade employees' privacy by stealing their data files, or spying on their Web traffic or other supposedly personal information. Moving one step further, any employee in the firm not necessarily having legitimate access rights to employees' computers can also attempt to fish for his co-workers private information. The advantages such an employee has over a remote cyber-attacker is that he has physical access to several of these computers (presumably during quiet hours), and he knows enough about the security and networking setup in the firm to enable an attempt. Finally, remote cyber-attackers are always lurking around to steal private information such as credit card data, bank account passwords, and other sensitive data by luring users into visiting some Web sites, or into opening malicious email attachments, and so on. The scenario of remote cyber-attackers applies to all users of computers regardless of whether they are using employer-provided equipment or personal home equipment.

### What Constitutes Private Information?

In the privacy policy and law terminology, PII (personally identifying information) is any piece of information that can potentially be used to uniquely identify or locate an individual. In the digital world, several such tidbits of information are available that can be exploited by cyber-criminals to steal the identity of the individual, which in turn can have significant financial consequences. Some examples of such pieces of PII are as follows.

- Name
- Date of birth
- Telephone number
- Street address
- E-mail address
- Social Security Number or National ID number (depending on country)
- Credit card information
- Bank account number

A web search on “personally identifying information” throws up a good list of Web sites that you can visit for more information.

### The Legal Aspect of Privacy

As a result of the Internet boom, technology products have been the focus and target of privacy-related scrutiny. This is because today’s technology makes it very easy to collect, store, and transmit PII. There are obvious advantages of this such as online loan applications and instant approvals (PII is transmitted over the wire), one-click shopping (the online shopping site remembers your credit card information), and so on. However, any lapse in securing the PII while it is in transit or being stored leads to PII leakage. Worse still, if word gets out of such a leak, especially to the press, it is usually very damaging to the reputation of the firm or agency, and puts the individuals (whose PII is leaked) at risk too. You may have read several such stories in the news about private information being lost or stolen from seemingly secure and protected environments. In some cases it is the negligence of IT personnel handling the information that causes the leaks. In other cases, bugs or design flaws in a product cause the leaks. The former is more often the case, but even in such scenarios, the products do come under the scrutiny of the press. And if the leak was a consequence of a flaw in the product, then such a product is bound to attract a lot of criticism from the press.

To steer away from such potentials breaches, several reputable vendors of products and services have established strong privacy policies and notices that they commit themselves to. Some examples are as follows.

- Intel Privacy Policy [1]
- Microsoft Online Privacy Notice [2]
- Amazon.com privacy notice [3]
- Privacy Policy for PayPal Services [4]

There are specific organizations (government funded and otherwise) that define guidelines and principles for organizations building technology products and services. The common theme of these guidelines is to ensure that organizations that deal with PII treat this information responsibly and respectfully. Some examples of such organizations are

- US Government's Export Portal (www.export.gov)
- Center for Democracy and Technology (www.cdt.org)
- Online Privacy Alliance (www.privacyalliance.org)

The U.S. Department of Commerce developed a "Safe Harbor" framework in consultation with the European Commission. This framework was developed to bridge the differences between privacy approaches and provide a streamlined means for U.S. organizations to comply with the European Commission's Directive on Data Protection[1]. The safe harbor Web site[2] is a rich repository of privacy related information. The overview page has a very good description of the safe harbor principles. They also maintain a good list of data privacy Web pages[3]. Intel is a participating organization of the safe harbor.

[1] http://www.cdt.org/privacy/eudirective/EU_Directive_.html

[2] http://www.export.gov/safeharbor/SH_Overview.asp

[3] http://www.export.gov/safeharbor/SH_Privacy_Links.asp

The Online Privacy Alliance also has a well written set of guidelines for online privacy policies[4]. In particular, the CDT's set of privacy principles is very succinct and precise, reproduced here.

**CDT: Privacy Basics**

- The Principle of Openness: The existence of record-keeping systems and databanks that contain personal data must be publicly known, along with a description of the main purpose and uses of the data.
- The Principle of Individual Participation: Individuals should have a right to view all information that is collected about them; they must also be able to correct or remove data that is not timely, accurate relevant, or complete.
- The Principle of Collection Limitation: There should exist limits to the collection of personal data; data should be collected by lawful and fair means and should be collected, where appropriate, with the knowledge or consent of the subject.
- The Principle of Data Quality: Personal data should be relevant to the purposes for which it is collected and used; personal data should be accurate, complete, and timely.
- The Principle of Finality: There should be limits to the use and disclosure of personal data; data should be used only for purposes specified at the time of collection; data should not be otherwise disclosed without the consent of the data subject or other legal authority.
- The Principle of Security: Personal data should be protected by reasonable security safeguards against such risks as loss, unauthorized access, destruction, use, modification or disclosure.
- The Principle of Accountability: Record keepers should be accountable for complying with fair information practices.

*Source: CDT Privacy Basics*
*(http://www.cdt.org/privacy/guide/basic/generic.html)*

[4] http://www.privacyalliance.org/resources/ppguidelines.shtml

## Importance of Privacy in Intel® AMT

Intel's products are designed to protect the end user's right to privacy, and Intel AMT is no exception. As you have read in earlier chapters, Intel AMT functionality allows IT technicians to remotely troubleshoot users' computer systems. Many of these capabilities have been available via software tools and applications that existed prior to the advent of Intel AMT. What makes Intel AMT particularly powerful is that it allows authorized IT technicians to remotely monitor and manage users' computers even if the user has turned off the computer. This makes Intel AMT a privacy-sensitive technology, especially if we consider scenarios where the privacy policies or laws prohibit the enterprise IT technicians from monitoring the user's usage of the computer. The following list recaps (from the previous chapters) some of the capabilities that Intel AMT offers to authorized IT administrators and technicians belonging to the organization, for managing the computers in a cost effective manner.

- Remotely power up and reboot the user's system for troubleshooting and repair
- Remotely access BIOS configuration screens on the user's system for fixing BIOS related problems
- Configure Intel AMT network traffic filters to protect the user's system from viruses and worms
- Verify that some of the critical applications on the user's system (such as antivirus software or personal firewall software) are properly running all the time
- Receive alerts generated by the Intel AMT firmware reporting events on the user's system that may require technical support
- Remotely troubleshoot the user's system by redirecting the boot process to a floppy disk, CD-ROM, or image located on the IT technician's system
- Allow software applications that have registered with the Intel AMT subsystem to store data on the Intel AMT nonvolatile flash memory. Authorized IT technicians can read this information remotely for purposes of software inventory collection and management.

- Store private configuration data (such as network settings, access control lists, event and audit logs, and so on) that is necessary for proper functioning of the Intel AMT subsystem. Most of this data is remotely manageable by authorized IT technicians.

In some organizations that are highly privacy sensitive (that is, protective of the privacy of their employees from their own IT departments), these capabilities may be viewed as unsuitable. Going one step further, the fear of rogue administrators (who are legitimately entrusted with authority to use Intel AMT to manage the employees' computers) that try to spy on employees' computer activities is also very real. These rogue insiders could be motivated by any number of reasons, such as bearing a grudge against another employee, retaliation against poor performance reviews or salary increases, financial motives to steal valuable organizational secrets and sell to interested parties, or just having what they may perceive as some harmless fun.

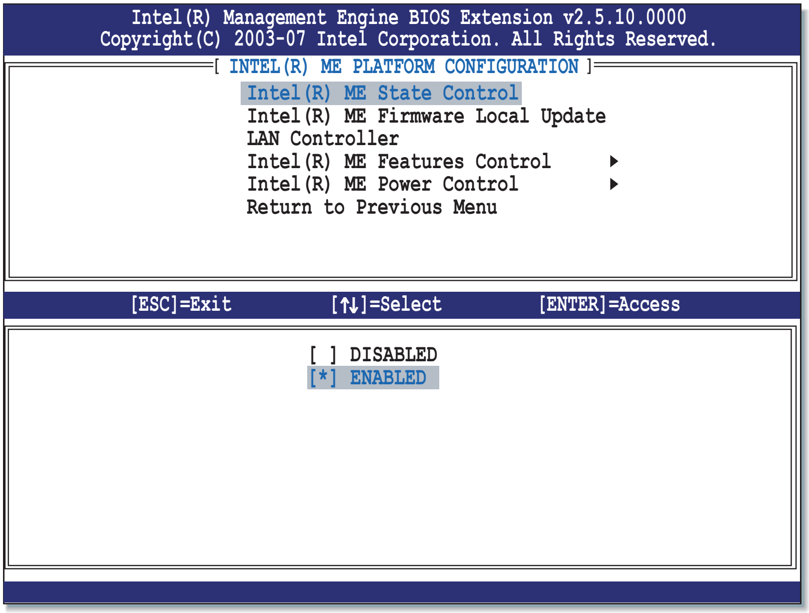
## Privacy Protection Mechanisms in Intel® AMT

In the design of Intel AMT we have taken several measures to protect the interests of end users and organizations from the privacy perspective. Intel AMT by its very nature is not a product that requires any PII for its operation. Obviously, Intel AMT does not need your date of birth, phone number, street address, or credit card information for its operation. It must also be equally obvious that Intel AMT does not store your bank account passwords, your email account passwords, and so on. Intel AMT works with information such as IP addresses, machine UUIDs, machine FQDNs, and the like. These pieces of information allow a network administrator to locate and connect to Intel AMT and perform computer management operations in a secure manner.

Intel AMT has several built in mechanisms to ensure that computer management happens securely and only by authorized IT administrators belonging to the organization's IT departments. It also provides several options that offer choices and control to IT administrators and end-users of the computers for opting in or opting out of various capabilities. It also ensures that the data stored by Intel AMT is protected from unauthorized access. Mechanisms are also available to protect against attacks by rouge administrators. Intel also collaborates with its ecosystem partners (such as OEMs and ISVs) to offer privacy protections in Intel AMT-related components that are built by them.

## Opt-in and Opt-out

Intel AMT has opt-in and opt-out settings for the whole subsystem as well as individually for several features. The IT administrator or the end-user can turn Intel Management Engine (Intel ME) and/or Intel AMT on or off from the Intel Management Engine BIOS Extensions (Intel MEBX) screen in the system BIOS. Similarly, some of the Intel AMT features can also be turned on or off such as IDE-Redirection (IDE-R), Serial over LAN (SoL) and Firmware Updates. These options are provided to offer the principle of choice and participation to users of computers with Intel vPro™ technology. Figures 16.1 through 16.6 show the Intel MEBX screens that demonstrate these options.

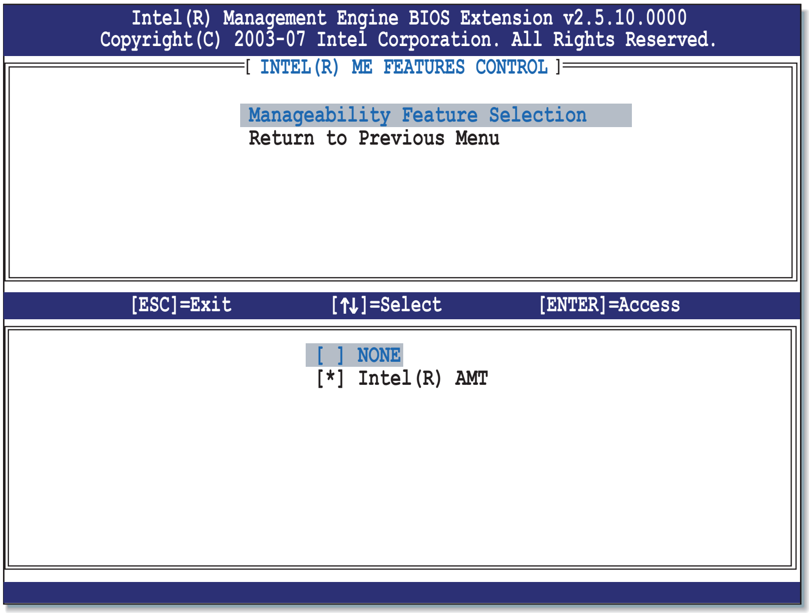


```
           Intel(R) Management Engine BIOS Extension v2.5.10.0000
         Copyright(C) 2003-07 Intel Corporation. All Rights Reserved.
                    [ INTEL(R) ME PLATFORM CONFIGURATION ]
                         Intel(R) ME State Control
                         Intel(R) ME Firmware Local Update
                         LAN Controller
                         Intel(R) ME Features Control        ►
                         Intel(R) ME Power Control           ►
                         Return to Previous Menu

        [ESC]=Exit              [↑↓]=Select            [ENTER]=Access

                               [ ] DISABLED
                               [*] ENABLED
```

**Figure 16.1** Intel® MEBX Option to Enable or Disable Intel® ME



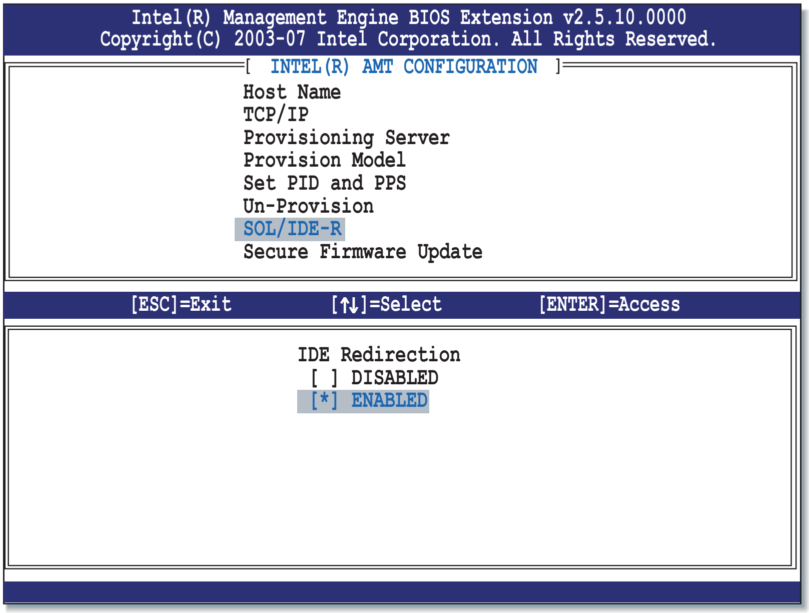
```
        Intel(R) Management Engine BIOS Extension v2.5.10.0000
     Copyright(C) 2003-07 Intel Corporation. All Rights Reserved.
[ INTEL(R) ME FEATURES CONTROL ]

                 Manageability Feature Selection
                 Return to Previous Menu

     [ESC]=Exit          [↑↓]=Select          [ENTER]=Access

                        [ ] NONE
                        [*] Intel(R) AMT
```

**Figure 16.2** Intel® MEBX Option to Enable or Disable Intel® AMT

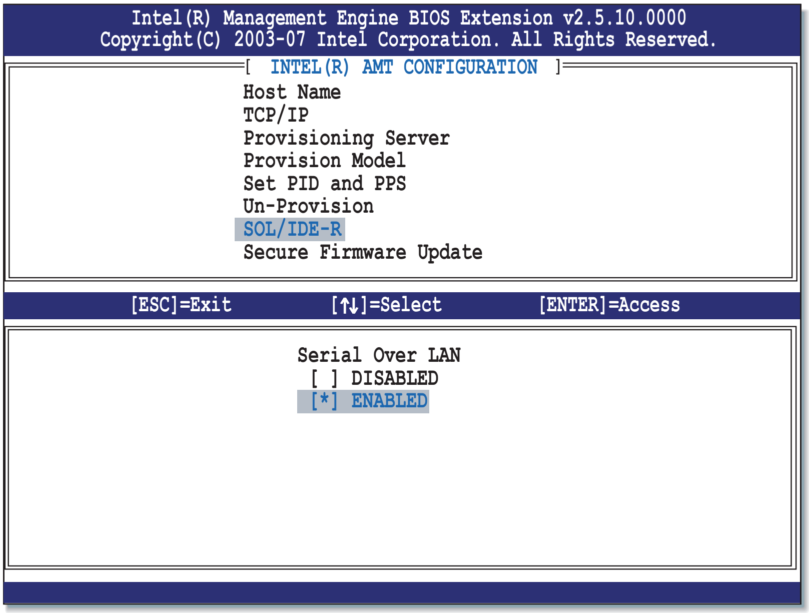


```
        Intel(R) Management Engine BIOS Extension v2.5.10.0000
     Copyright(C) 2003-07 Intel Corporation. All Rights Reserved.
[ INTEL(R) AMT CONFIGURATION ]
                 Host Name
                 TCP/IP
                 Provisioning Server
                 Provision Model
                 Set PID and PPS
                 Un-Provision
                 SOL/IDE-R
                 Secure Firmware Update

     [ESC]=Exit          [↑↓]=Select          [ENTER]=Access

                      IDE Redirection
                       [ ] DISABLED
                       [*] ENABLED
```

**Figure 16.3** Intel® MEBX Option to Enable or Disable IDE-Redirection

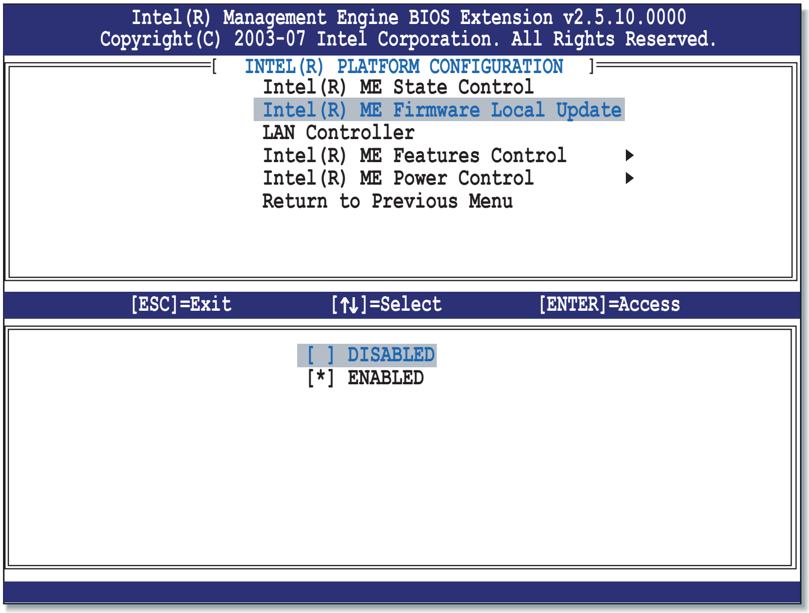


```
     Intel(R) Management Engine BIOS Extension v2.5.10.0000
   Copyright(C) 2003-07 Intel Corporation. All Rights Reserved.
                  [ INTEL(R) AMT CONFIGURATION ]
                  Host Name
                  TCP/IP
                  Provisioning Server
                  Provision Model
                  Set PID and PPS
                  Un-Provision
                  SOL/IDE-R
                  Secure Firmware Update

       [ESC]=Exit         [↑↓]=Select         [ENTER]=Access

                       Serial Over LAN
                        [ ] DISABLED
                        [*] ENABLED
```

**Figure 16.4** Intel® MEBX Option to Enable or Disable Serial over LAN

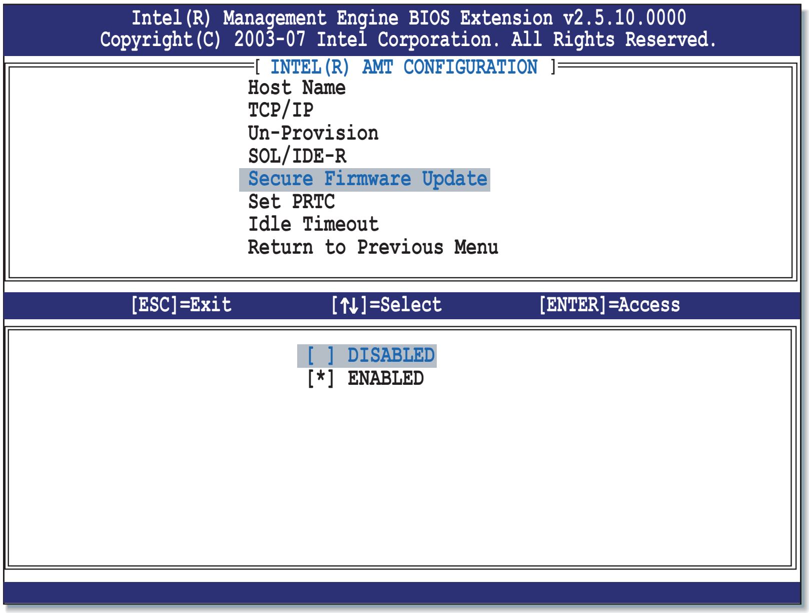


```
     Intel(R) Management Engine BIOS Extension v2.5.10.0000
   Copyright(C) 2003-07 Intel Corporation. All Rights Reserved.
               [ INTEL(R) PLATFORM CONFIGURATION ]
                  Intel(R) ME State Control
                  Intel(R) ME Firmware Local Update
                  LAN Controller
                  Intel(R) ME Features Control       ▶
                  Intel(R) ME Power Control          ▶
                  Return to Previous Menu

       [ESC]=Exit         [↑↓]=Select         [ENTER]=Access

                        [ ] DISABLED
                        [*] ENABLED
```

**Figure 16.5** Intel® MEBX Option to Enable or Disable Local Firmware Update



```
Intel(R) Management Engine BIOS Extension v2.5.10.0000
Copyright(C) 2003-07 Intel Corporation. All Rights Reserved.

[ INTEL(R) AMT CONFIGURATION ]
Host Name
TCP/IP
Un-Provision
SOL/IDE-R
Secure Firmware Update
Set PRTC
Idle Timeout
Return to Previous Menu

[ESC]=Exit          [↑↓]=Select          [ENTER]=Access

[ ] DISABLED
[*] ENABLED
```

**Figure 16.6** Intel® MEBX Option to Enable or Disable Secure Firmware Update

One particularly relevant distinction is end-user choice versus IT administrator choice. End-user in this context is the actual person using the vPro computer. As mentioned earlier, some organizations want to give their end-users the final right to their privacy (even when working on the computers belonging to the organization). In such cases the end-user may go into the Intel MEBX screen of the system BIOS and opt out of Intel AMT capability or some specific features depending upon his or her choice. In such case, the remote IT administrator cannot change the end-user preferences. The Intel MEBX configuration setting overrides the setting configured by the remote IT administrator. Of course, the remote IT administrator can change the settings in the Intel MEBX if he or she knows the end user's BIOS and Intel MEBX passwords, but we expect end-users to keep these passwords confidential.

### Secure Local Configuration

The end-user configuration of some Intel AMT settings (such as enabling or disabling Intel AMT or certain features in it) is not possible to do from the host operating system. This is because host software is susceptible to attacks from viruses and malware, and we do not want such malicious programs to modify the configuration settings. If modification of configuration settings is allowed to happen from the host operating system, then Intel AMT has no way to find out whether the configuration is being modified by a malicious program or a legitimate end-user. Malicious programs can then make configuration modifications silently without requiring any end-user input or intervention. This is a very undesirable scenario. So we need to look for another mechanism that is more secure to allow the end-user to interact with Intel AMT to modify the configuration settings. The other piece of software that executes on the computer that the end-user can interact with is the system BIOS. Viruses that attack the BIOS are far rarer than viruses that attack popular operating systems, such as Windows. Therefore Intel AMT uses the BIOS (that is, the Intel MEBX, as shown in the Figures 16.1 through 16.6) as the interface to allow the end-user to modify privacy related Intel AMT configuration settings. The Intel MEBX–based interface inherently enforces the physical presence of an end user to interact with it, and one that has knowledge of the Intel MEBX authentication password. This largely eliminates the possibility of a silent and remote exploit by a malicious program. Examples are the same as illustrated in the screens shown in Figures 16.1 through 16.6.

### End User Notification

Intel AMT's activity within the user's computer and within the communication network is largely invisible to the user. As a result, the end user has little knowledge whether his or her computer is being managed and monitored by another entity—the IT administrator. From a privacy standpoint, the impact of such a mode of operation might range from an uncomfortable feeling for the end user to something more significant. Therefore, Intel developed a host software-based notification mechanism (an application icon in the system tray) that explicitly made the end-user aware that Intel AMT is available within the platform, and some other information regarding its status.

The main functionality of the tray icon application is to give Intel AMT status to the end user of the computer with Intel vPro technology. This icon application is available for the most popular versions of Windows and Linux (Windows XP, Windows Vista, Red Hat Linux, and Novell SuSE Linux). On Windows, the system tray icon application adheres to Microsoft's guidelines for system tray icons. The system tray icon supports notifications of events via notification bubbles. Apart from the status, the system tray icon includes an option to initiate a remote connection from Intel AMT to the enterprise management console upon user's request. Figure 16.7 shows the Intel AMT system tray icon on a Windows-based computer with Intel vPro technology.

Missing

**Figure 16.7** Intel® AMT System Tray Icon Application

The tray icon application communicates with Intel AMT firmware using the host interface commands exposed by the firmware. The tray icon obtains the following pieces of information from the Intel AMT firmware and reports it to the end user:

- Whether Intel AMT was detected in the firmware or not
- If detected, the Intel AMT firmware version number
- Whether Intel AMT is enabled or disabled
- Whether Intel AMT is configured or not
- Whether Intel AMT is configured in enterprise mode or SMB mode
- Whether web-based user interface is enabled or disabled

Upon double clicking the system tray icon application, a window opens up that shows some more details including a link to an Internet site where more information can be obtained on Intel vPro technology and Intel AMT.

## Private Data Storage Protection

Intel AMT stores sensitive pieces of information such as key material, access control lists, certificates, profiles and policies, logs, and so on. This information is stored in a private region of the nonvolatile flash memory that is accessible only to the Intel AMT subsystem and not to the host operating system. Therefore any malicious program that may be running on the host cannot access this data. However, if an attacker were to gain physical access to the computer (such as by stealing it at the airport), the attacker could use a flash memory reader to access the physical flash memory device on the computer's motherboard and read all the data on it—including the data stored in the private region. To protect against such a severe class of attacks, Intel AMT encrypts the most sensitive pieces of data stored on the flash memory using a special hardware key that is embedded deep inside the chipset manufactured by Intel. It is practically impossible to get to these hardware keys. Therefore the most sensitive data stored on the flash memory by Intel AMT is protected against very severe forms of attack. Intel AMT integrity protects some pieces of data as well. Table 16.1 lists some such pieces of data (please note that this may not be a complete list, as there may be some product changes from the time of this writing).

**Table 16.1** An illustrative list of Intel® AMT data structures that is encrypted and integrity protected while being stored on the nonvolatile flash memory device

| Intel® AMT Data Structure | Encrypted | Integrity Protected |
|---|---|---|
| Usernames and hashed passwords | No | Yes |
| Permissions, Access Control Lists | No | Yes |
| Network Security Settings | No | Yes |
| Certificates | No | Yes |
| Intel® AMT Configuration settings and parameters | No | Yes |
| Admin authentication password | Yes | Yes |
| Configuration passphrases | Yes | Yes |
| Kerberos keys and attributes | Yes | Yes |
| Private portions of asymmetric key pairs | Yes | Yes |

When an Intel AMT subsystem is decommissioned (that is, when an IT administrator takes the computer out of daily use and readies it for removal from service), all the private data stored on the flash memory device is erased and the contents are restored to their original factory default values. The technical details of this storage protection are available in Chapter 15.

### Secure Communication of Information

Intel AMT uses strong authentication (Kerberos or HTTP Digest password based authentication), authorization (HTTP realm–based authorization) and session security (TLS using AES 128- or 256-bit security) mechanisms to protect the communication traffic. More details of these aspects are available in Chapter 14.

### Mitigating the Rogue Administrator

Intel AMT has the capability to log the actions of the IT administrator. Intel AMT builds in the notion of dual-person controls by separating the duties of the IT administrator and the IT auditor. The IT auditor is the person who monitors the actions of the IT administrator and ensures that the actions did not represent any purposeful malicious intent. Therefore, to be able to do harmful and malicious actions within an Intel AMT subsystem and escape undetected, the IT administrator and IT auditor must collude. This requirement of dual-person control inherently increases the security of the system and provides a sufficient level of deterrence to the IT administrator from performing intentionally malicious actions. And if the IT administrator does perform malicious actions, the IT auditor can furnish sufficient evidence (in the form of audit logs) to be able to prosecute the corrupt IT administrator. More technical details on the audit logging mechanism in Intel AMT are available in Chapter 15.

## Summary

In this chapter we learned the basics of privacy sensitivities in the technology world, some of the initiatives related to protecting online privacy and privacy guidelines and best practices. We also briefly discussed the privacy sensitive capabilities of Intel AMT, and discussed why privacy is so important to Intel AMT. Finally we covered the various mechanisms put in place within the design of Intel AMT to adhere to the online privacy guidelines and best practices, and how Intel AMT offers a high level of privacy protection to its users.