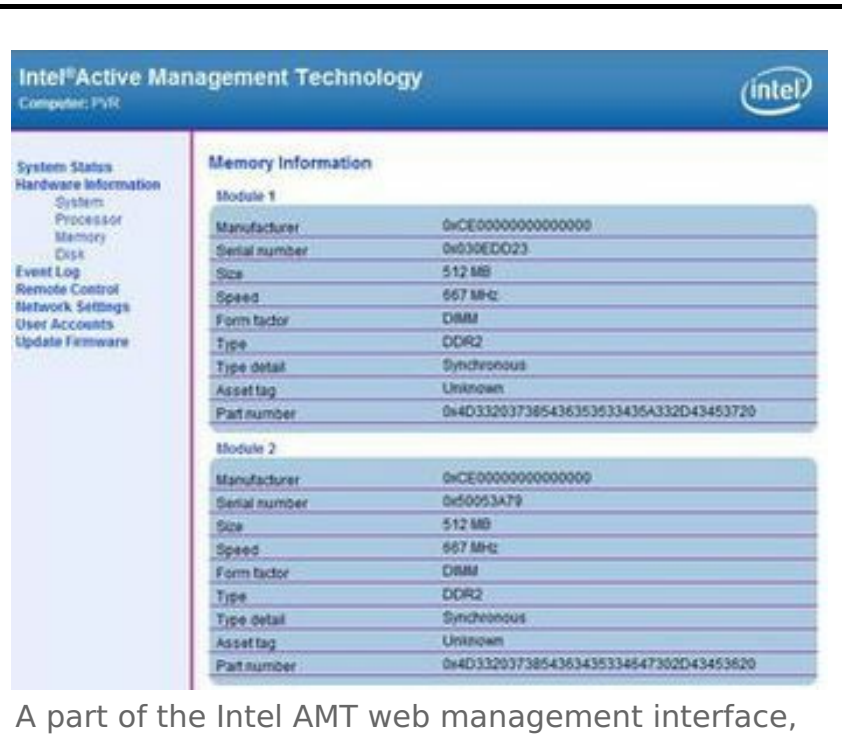
Intel Active Management Technology



Intel®Active Management Technology
Computer: PVR

Memory Information

Module 1

Manufacturer	0xCE00000000000000
Serial number	0x030EDD23
Size	512 MB
Speed	667 MHz
Form factor	DIMM
Type	DDR2
Type detail	Synchronous
Asset tag	Unknown
Part number	0x4D3320373854363535333435A332D43453720

Module 2

Manufacturer	0xCE00000000000000
Serial number	0x50053A79
Size	512 MB
Speed	667 MHz
Form factor	DIMM
Type	DDR2
Type detail	Synchronous
Asset tag	Unknown
Part number	0x4D33203738543634353334647302D43453620

A part of the Intel AMT web management interface, accessible even when the computer is sleeping

Intel Active Management Technology (**AMT**) is hardware and firmware technology for remote out-of-band management of personal computers,[1][2][3][4][5] in order to monitor, maintain, update, upgrade, and repair them.[1] Out-of-band (OOB) or hardware-based management is different from software-based (or in-band) management and software management agents.[1][2]

Hardware-based management works at a different level from software applications, and uses a communication channel (through the TCP/IP stack) that is different from software-based communication (which is through the software stack in the operating system). Hardware-based management does not depend on the presence of an OS or locally installed management agent. Hardware-based management has been available on Intel/AMD based computers in the past, but it has largely been limited to auto-configuration using DHCP or BOOTP for dynamic IP address allocation and diskless workstations, as well as wake-on-LAN (WOL) for remotely powering on systems.[6] AMT is not intended to be used by itself; it is intended to be used with a software management application.[1] It gives a management application (and thus, the system administrator who uses it) access to the PC down the wire, in order to remotely do tasks that are difficult or sometimes impossible when working on a PC that does not have remote functionalities built into it.[1][3][7]

AMT is designed into a secondary (service) processor located on the motherboard,[8] and uses TLS-secured communication and strong encryption to provide additional security.[2] AMT is part of the Intel Management Engine (ME), which is built into PCs with Intel vPro technology.[2] AMT has moved towards increasing support for DMTF Desktop and mobile Architecture for System Hardware (DASH) standards and AMT Release 5.1 and later releases are an implementation of DASH version 1.0/1.1 standards for out-of-band management.[9] AMT provides similar functionality to IPMI, although AMT is designed for client computing systems as compared with the typically server-based IPMI.

Currently, AMT is available in desktops, servers, ultrabooks, tablets, and laptops with Intel Core vPro processor family, including Intel Core i5, i7, and Intel Xeon processor E3-1200 product family.[1][10][11]

Intel has confirmed a Remote Elevation of Privilege bug (CVE-2017-5689) in its Management Technology, on 1 May 2017.[12] Every Intel platform with either Intel Standard Manageability, Active Management Technology, or Small Business Technology, from Nehalem in 2008 to Kaby Lake in 2017 has a remotely exploitable security hole in the IME (Intel Management Engine).[13][14] Some manufacturers, like Purism are already selling hardware with Intel Management Engine disabled to prevent the remote exploit.[15]

Contents

Non-free service access

Although iAMT may be included for free in devices sold to the public and to small businesses, the full capabilities of iAMT, including encrypted remote access via a public key certificate and automatic remote device provisioning of unconfigured iAMT clients, are not accessible for free to the general public or to the direct owners of iAMT equipped devices. iAMT cannot be fully utilized to its maximum potential without purchasing additional software or management services from Intel or another 3rd party independent software vendor (ISV) or value added reseller (VAR).

Intel itself provides a *developer's toolkit* software package which allows basic access to iAMT, but is not intended to be normally used to access the technology.[16] Only basic modes of access are supported, without full access to the encrypted communications of the complete purchased management system.[17]

Features

Intel AMT includes hardware-based remote management, security, power management, and remote configuration features that enable independent remote access to AMT-enabled PCs.[1][7][18] Intel AMT is security and management technology that is built into PCs with Intel vPro technology.[1][6] PCs with Intel vPro include many other "platform" (general PC) technologies and features.

Intel AMT uses a hardware-based out-of-band (OOB) communication channel[1] that operates regardless of the presence of a working operating system. The communication channel is independent of the PC's power state, the presence of a management agent, and the state of many hardware components such as hard disk drives and memory.

Most AMT features are available OOB, regardless of PC power state.[1] Other features require the PC to be powered up (such as console redirection via serial over LAN (SOL), agent presence checking, and network traffic filtering).[1] Intel AMT has remote power-up capability.

Hardware-based features can be combined with scripting to automate maintenance and service.[1]

Hardware-based AMT features on laptop and desktop PCs include:

- Encrypted, remote communication channel for network traffic between the IT console and Intel AMT.[1][2]
- Ability for a wired PC (physically connected to the network) outside the company's firewall on an open LAN to establish a secure communication tunnel (via AMT) back to the IT console.[1][2] Examples of an open LAN include a wired laptop at home or at an SMB site that does not have a proxy server.
- Remote power up / power down / power cycle through encrypted WOL.[1][2]
- Remote boot, via integrated device electronics redirect (IDE-R).[1][2]
- Console redirection, via serial over LAN (SOL).[1]
- Keyboard, video, mouse (KVM) over network.
- Hardware-based filters for monitoring packet headers in inbound and outbound network traffic for known threats (based on programmable timers), and for monitoring known / unknown threats based on time-based heuristics. Laptops and desktop PCs have filters to monitor packet headers. Desktop PCs have packet-header filters and time-based filters.[1][2][19]
- Isolation circuitry (previously and unofficially called "circuit breaker" by Intel) to port-block, rate-limit, or fully isolate a PC that might be compromised or infected.[1][2][19]
- Agent presence checking, via hardware-based, policy-based programmable timers. A "miss" generates an event; you can specify that the event generate an alert.[1][2][19]
- OOB alerting.[1][2]
- Persistent event log, stored in protected memory (not on the hard drive).[1][2]
- Access (preboot) the PC's universal unique identifier (UUID).[1][2]
- Access (preboot) hardware asset information, such as a component's manufacturer and model, which is updated every time the system goes through power-on self-test (POST).[1][2]
- Access (preboot) to third-party data store (TPDS), a protected memory area that software vendors can use, in which to version information, .DAT files, and other information.[1][2]
- Remote configuration options, including certificate-based zero-touch remote configuration, USB key configuration (light-touch), and manual configuration.[1][2][20]
- Protected Audio/Video Pathway for playback protection of DRM-protected media.

Laptops with AMT also include wireless technologies:

- Support for IEEE 802.11 a/g/n wireless protocols[1][10][21][22]
- Cisco-compatible extensions for Voice over WLAN[1][10][21][22]

History

Software updates provide upgrades to the next minor version of Intel AMT. New major releases of Intel AMT are built into a new chipset, and are updated through new hardware.[2]

Applications

Almost all AMT features are available even if the PC is in a powered-off state but with its power cord attached, if the operating system has crashed, if the software agent is missing, or if hardware (such as a hard drive or memory) has failed.[1][2] The console-redirection feature (SOL), agent presence checking, and network traffic filters are available after the PC is powered up.[1][2]

Intel AMT supports these management tasks:

- Remotely power up, power down, power cycle, and power reset the computer.[1]
- Remote boot the PC by remotely redirecting the PC's boot process, causing it to boot from a different image, such as a network share, bootable CD-ROM or DVD, remediation drive, or other boot device.[1][7] This feature supports remote booting a PC that has a corrupted or missing OS.
- Remotely redirect the system's I/O via console redirection through serial over LAN (SOL).[1] This feature supports remote troubleshooting, remote repair, software upgrades, and similar processes.
- Access and change BIOS settings remotely.[1] This feature is available even if PC power is off, the OS is down, or hardware has failed. This feature is designed to allow remote updates and corrections of configuration settings. This feature supports full BIOS updates, not just changes to specific settings.
- Detect suspicious network traffic.[1][19] In laptop and desktop PCs, this feature allows a sys-admin to define the events that might indicate an inbound or outbound threat in a network packet header. In desktop PCs, this feature also supports detection of known and/or unknown threats (including slow- and fast-moving computer worms) in network traffic via time-based, heuristics-based filters. Network traffic is checked before it reaches the OS, so it is also checked before the OS and software applications load, and after they shut down (a traditionally vulnerable period for PCs).
- Block or rate-limit network traffic to and from systems suspected of being infected or compromised by computer viruses, computer worms, or other threats.[1][19] This feature uses Intel AMT hardware-based isolation circuitry that can be triggered manually (remotely, by the sys-admin) or automatically, based on IT policy (a specific event).
- Manage hardware packet filters in the on-board network adapter.[1][19]
- Automatically send OOB communication to the IT console when a critical software agent misses its assigned check in with the programmable, policy-based hardware-based timer.[1][19] A "miss" indicates a potential problem. This feature can be combined with OOB alerting so that the IT console is notified only when a potential problem occurs (helps keep the network from being flooded by unnecessary "positive" event notifications).
- Receive Platform Event Trap (PET) events out-of-band from the AMT subsystem (for example, events indicating that the OS is hung or crashed, or that a password attack has been attempted).[1] You can alert on an event (such as falling out of compliance, in combination with agent presence checking) or on a threshold (such as reaching a particular fan speed).
- Access a persistent event log, stored in protected memory.[1] The event log is available OOB, even if the OS is down or the hardware has already failed.
- Discover an AMT system independently of the PC's power state or OS state.[1] Discovery (preboot access to the UUID) is available if the system is powered down, its OS is compromised or down, hardware (such as a hard drive or memory) has failed, or management agents are missing.
- Perform a software inventory or access information about software on the PC.[1] This feature allows a third-party software vendor to store software asset or version information for local applications in the Intel AMT protected memory. (This is the protected third party data store, which is different from the protected AMT memory for hardware component information and other system information). The third-party data store can be accessed OOB by the sys-admin. For example, an antivirus program could store version information in the protected memory that is available for third-party data. A computer script could use this feature to identify PCs that need to be updated.
- Perform a hardware inventory by uploading the remote PC's hardware asset list (platform, baseboard management controller, BIOS, processor, memory, disks, portable batteries, field replaceable units, and other information).[1] Hardware asset information is updated every time the system runs through power-on self-test (POST).

From major version 6, Intel AMT embeds a proprietary VNC server, for out-of-band access using dedicated VNC-compatible viewer technology, and have full KVM (keyboard, video, mouse) capability throughout the power cycle – including uninterrupted control of the desktop when an operating system loads. Clients such as VNC Viewer Plus from RealVNC also provide additional functionality that might make it easier to perform (and watch) certain Intel AMT operations, such as powering the computer off and on, configuring the BIOS, and mounting a remote image (IDER).

Provisioning and integration

AMT supports certificate-based or PSK-based remote provisioning (full remote deployment), USB key-based provisioning ("one-touch" provisioning), manual provisioning[1] and provisioning using an agent on the local host ("Host Based Provisioning"). An OEM can also pre-provision AMT.[20]

The current version of AMT supports remote deployment on both laptop and desktop PCs. (Remote deployment was one of the key features missing from earlier versions of AMT and which delayed acceptance of AMT in the market.)[7] Remote deployment, until recently, was only possible within a corporate network.[23] Remote deployment lets a sys-admin deploy PCs without "touching" the systems physically.[1] It also allows a sys-admin to delay deployments and put PCs into use for a period of time before making AMT features available to the IT console.[24] As delivery and deployment models evolve, AMT can now be deployed over the Internet, using both "Zero-Touch" and Host-Based methods.[25]

PCs can be sold with AMT enabled or disabled. The OEM determines whether to ship AMT with the capabilities ready for setup (enabled) or disabled. Your setup and configuration process will vary, depending on the OEM build.[20]

AMT includes a Privacy Icon application, called IMSS,[26] that notifies the system's user if AMT is enabled. It is up to the OEM to decide whether they want to display the icon or not.

AMT supports different methods for disabling the management and security technology, as well as different methods for reenabling the technology.[1][24][27][28]

AMT can be partially unprovisioned using the Configuration Settings, or fully unprovisioned by erasing all configuration settings, security credentials, and operational and networking settings.[29] A partial unprovisioning leaves the PC in the setup state. In this state, the PC can self-initiate its automated, remote configuration process. A full unprovisioning erases the configuration profile as well as the security credentials and operational / networking settings required to communicate with the Intel Management Engine. A full unprovisioning returns Intel AMT to its factory default state.

Once AMT is disabled, in order to enable AMT again, an authorized sys-admin can reestablish the security credentials required to perform remote configuration by either:

- Using the remote configuration process (full automated, remote config via certificates and keys).[1]
- Physically accessing the PC to restore security credentials, either by USB key or by entering the credentials and MEBx parameters manually.[1]

There is a way to totally reset AMT and return in to factory defaults. This can be done in two ways:

- Setting the appropriate value in the BIOS.
- Clearing the CMOS memory and / or NVRAM.

Setup and integration of AMT is supported by a setup and configuration service (for automated setup), an AMT Webserver tool (included with Intel AMT), and AMT Commander, an unsupported and free, proprietary application available from the Intel website.

Communication

All access to the Intel AMT features is through the Intel Management Engine in the PC's hardware and firmware.[1] AMT communication depends on the state of the Management Engine, not the state of the PC's OS.

As part of the Intel Management Engine, the AMT OOB communication channel is based on the TCP/IP firmware stack designed into system hardware.[1] Because it is based on the TCP/IP stack, remote communication with AMT occurs via the network data path before communication is passed to the OS.

Intel AMT supports wired and wireless networks.[1][10][21][30] For wireless notebooks on battery power, OOB communication is available when the system is awake and connected to the corporate network, even if the OS is down. OOB communication is also available for wireless or wired notebooks connected to the corporate network over a host OS-based virtual private network (VPN) when notebooks are awake and working properly.

AMT version 4.0 and higher can establish a secure communication tunnel between a wired PC and an IT console outside the corporate firewall.[1][31] In this scheme, a management presence server (Intel calls this a "vPro-enabled gateway") authenticates the PC, opens a secure TLS tunnel between the IT console and the PC, and mediates communication.[1][32] The scheme is intended to help the user or PC itself request maintenance or service when at satellite offices or similar places where there is no on-site proxy server or management appliance.

Technology that secures communications outside a corporate firewall is relatively new. It also requires that an infrastructure be in place, including support from IT consoles and firewalls.

An AMT PC stores system configuration information in protected memory. For PCs version 4.0 and higher, this information can include the name(s) of appropriate "whitelist" management servers for the company. When a user tries to initiate a remote session between the wired PC and a company server from an open LAN, AMT sends the stored information to a management presence server (MPS) in the "demilitarized zone" ("DMZ") that exists between the corporate firewall and client (the user PC's) firewalls. The MPS uses that information to help authenticate the PC. The MPS then mediates communication between the laptop and the company's management servers.[1]

Because communication is authenticated, a secure communication tunnel can then be opened using TLS encryption. Once secure communications are established between the IT console and Intel AMT on the user's PC, a sys-admin can use the typical AMT features to remotely diagnose, repair, maintain, or update the PC.[1]

Design

Hardware

The *Management Engine* (ME) is an isolated and protected coprocessor, embedded as a non-optional[33] part in all current (as of 2015) Intel chipsets.[34]

Starting with ME 11, it is based on the Intel Quark x86-based 32-bit CPU and runs the MINIX 3 operating system.[35] The ME state is stored in a partition of the SPI flash, using the Embedded Flash File System (EFFS).[36] Previous versions were based on an ARC core, with the Management Engine running the ThreadX RTOS from Express Logic. Versions 1.x to 5.x of the ME used the ARCTangent-A4 (32-bit only instructions) whereas versions 6.x to 8.x used the newer ARCompact (mixed 32- and 16-bit instruction set architecture). Starting with ME 7.1, the ARC processor could also execute signed Java applets.

The ME has its own MAC and IP address for the out-of-band interface, with direct access to the Ethernet controller; one portion of the Ethernet traffic is diverted to the ME even before reaching the host's operating system, for what support exists in various Ethernet controllers, exported and made configurable via Management Component Transport Protocol (MCTP).[37][38] The ME also communicates with the host via PCI interface.[36] Under Linux, communication between the host and the ME is done via `/dev/mei`.[34]

Until the release of Nehalem processors, the ME was usually embedded into the motherboard's northbridge, following the Memory Controller Hub (MCH) layout.[39] With the newer Intel architectures (Intel 5 Series onwards), ME is included into the Platform Controller Hub (PCH).[40][41]

Software

Firmware modules:

- Active Management Technology (AMT)
- Alert Standard Format (ASF)
- *Quiet System Technology* (QST), formerly known as *Advanced Fan Speed Control* (AFSC), which provides support for acoustically-optimized fan speed control, and monitoring of temperature, voltage, current and fan speed sensors that are provided in the chipset, CPU and other devices present on the motherboard. Communication with the QST firmware subsystem is documented and available through the official software development kit (SDK).[42]
- Trusted Platform Module (TPM)

Security

Because AMT allows access to the PC below the OS level, security for the AMT features is a key concern.

Security for communications between Intel AMT and the provisioning service and/or management console can be established in different ways depending on the network environment. Security can be established via certificates and keys (TLS public key infrastructure, or TLS-PKI), pre-shared keys (TLS-PSK), or administrator password.[1][2]

Security technologies that protect access to the AMT features are built into the hardware and firmware. As with other hardware-based features of AMT, the security technologies are active even if the PC is powered off, the OS is crashed, software agents are missing, or hardware (such as a hard drive or memory) has failed.[1][2][43]

Because the software that implements AMT exists outside of the operating system, it is not kept up-to-date by the operating system's normal update mechanism. Security defects in the AMT software can therefore be particularly severe, as they will remain long after they have been discovered and become known to potential attackers.

On May 15th, 2017, Intel announced a critical vulnerability in AMT. According to the update "The vulnerability could enable a network attacker to remotely gain access to business PCs or devices that use these technologies".[44] Intel announced partial availability of a firmware update to patch the vulnerability for some of the affected devices.

Networking

While some protocols for in-band remote management use a secured network communication channel (for example Secure Shell), some other protocols are not secured. Thus some businesses have had to choose between having a secure network or allowing IT to use remote management applications without secure communications to maintain and service PCs.[1]

Modern security technologies and hardware designs allow remote management even in more secure environments. For example, Intel AMT supports IEEE 802.1x, Preboot Execution Environment (PXE), Cisco SDN, and Microsoft NAP.[1]

All AMT features are available in a secure network environment. With Intel AMT in the secure network environment:

- The network can verify the security posture of an AMT-enabled PC and authenticate the PC before the OS loads and before the PC is allowed access to the network.
- PXE boot can be used while maintaining network security. In other words, an IT administrator can use an existing PXE infrastructure in an IEEE 802.1x, Cisco SDN, or Microsoft NAP network.

Intel AMT can embed network security credentials in the hardware, via the Intel AMT Embedded Trust Agent and an AMT posture plug-in.[1][2] The plug-in collects security posture information, such as firmware configuration and security parameters from third-party software (such as antivirus software and antispyware), BIOS, and protected memory. The plug-in and trust agent can store the security profile(s) in AMT's protected, nonvolatile memory, which is not on the hard disk drive.

Because AMT has an out-of-band communication channel, AMT can present the PC's security posture to the network even if the PC's OS or security software is compromised. Since AMT presents the posture out-of-band, the network can also authenticate the PC out-of-band, before the OS or applications load and before they try to access the network. If the security posture is not correct, a system administrator can push an update OOB (via Intel AMT) or reinstall critical security software before letting the PC access the network.

Support for different security postures depends on the AMT release:

- Support for IEEE 802.1x and Cisco SDN requires AMT version 2.6 or higher for laptops, and AMT version 3.0 or higher for desktop PCs.[1][45][46]
- Support for Microsoft NAP requires AMT version 4.0 or higher.[1]
- Support for PXE boot with full network security requires AMT version 3.2 or higher for desktop PCs.[1]

Technology

AMT includes several security schemes, technologies, and methodologies to secure access to the AMT features during deployment and during remote management.[1][2][43] AMT security technologies and methodologies include:

- Transport Layer Security, including pre-shared key TLS (TLS-PSK)
- HTTP authentication
- Single sign-on to Intel AMT with Microsoft Windows domain authentication, based on Microsoft Active Directory and Kerberos
- Digitally signed firmware
- Pseudo-random number generator (PRNG) which generates session keys
- Protected memory (not on the hard disk drive) for critical system data, such as the UUID, hardware asset information, and BIOS configuration settings
- Access control lists (ACL)

As with other aspects of Intel AMT, the security technologies and methodologies are built into the chipset.

Known vulnerabilities and exploits

Ring −3 rootkit

A ring −3 rootkit was demonstrated by Invisible Things Lab for the Q35 chipset; it does not work for the later Q45 chipset as Intel implemented additional protections.[47] The exploit worked by remapping the normally protected memory region (top 16 MB of RAM) reserved for the ME. The ME rootkit could be installed regardless of whether the AMT is present or enabled on the system, as the chipset always contains the ARC ME coprocessor. (The "−3" designation was chosen because the ME coprocessor works even when the system is in the S3 state, thus it was considered a layer below the System Management Mode rootkits.[39]) For the vulnerable Q35 chipset, a keystroke logger ME-based rootkit was demonstrated by Patrick Stewin.[48][49]

Zero-touch provisioning

Another security evaluation by Vassilios Ververis showed serious weaknesses in the GM45 chipset implementation. In particular, it criticized AMT for transmitting unencrypted passwords in the SMB provisioning mode when the IDE redirection and Serial over LAN features are used. It also found that the "zero touch" provisioning mode (ZTC) is still enabled even when the AMT appears to be disabled in BIOS. For about 60 euros, Ververis purchased from Go Daddy a certificate that is accepted by the ME firmware and allows remote "zero touch" provisioning of (possibly unsuspecting) machines, which broadcast their HELLO packets to would-be configuration servers.[50]

Silent Bob is Silent

In May 2017, Intel confirmed that many computers with AMT have had an unpatched critical privilege escalation vulnerability (CVE-2017-5689).[14][51][12][52][53] The vulnerability, which was nicknamed "Silent Bob is Silent" by the researchers who had reported it to Intel,[54] affects numerous laptops, desktops and servers sold by Dell, Fujitsu, Hewlett-Packard (later Hewlett Packard Enterprise and HP Inc.), Intel, Lenovo, and possibly others.[54][55][56][57][58][59][60] Those researchers claimed that the bug affects systems made in 2010 or later.[61] Other reports claimed the bug also affects systems made as long ago as 2008.[62][14] The vulnerability was described as giving remote attackers:

> "full control of affected machines, including the ability to read and modify everything. It can be used to install persistent malware (possibly in firmware), and read and modify any data."
>
> — Tatu Ylönen, *ssh.com*[54]

PLATINUM

In June 2017, the PLATINUM cybercrime group became notable for exploiting the serial over LAN (SOL) capabilities of AMT to perform data exfiltration of stolen documents.[63][64][65][66][67][68][69][70]

Avoidance and mitigation

PCs with AMT typically provide an option in the BIOS menu to switch off AMT, though OEMs implement BIOS features differently[71] and therefore the BIOS is not a reliable method to switch off AMT. Intel-based PCs that shipped without AMT are supposed not to be able to have AMT later installed. However, as long as the PC's hardware is potentially capable of running the AMT, it is unclear how effective these protections are.[72][73][74] Presently, there are mitigation guides[75] and tools[76] to disable AMT on Windows, but Linux has only received a tool to check whether AMT is enabled and provisioned on Linux systems.[77] The only way to actually fix this vulnerability is to install a firmware update. Intel has made a list of updates available.[78]

In 2015, a small number of competing vendors began to offer Intel-based PCs designed or modified specifically to address potential AMT vulnerabilities, and related concerns.[79][80][81][82][83][84][85]

See also

- Backdoor (computing)
- Host Embedded Controller Interface
- HP Integrated Lights-Out
- Intel CIRA
- Intel Core 2
- Internet kill switch
- I/O Controller Hub
- Lights out management
- Southbridge (computing)
- System Service Processor
- Intel AMT versions
- Intel Management Engine

References

1. "Intel Centrino 2 with vPro Technology and Intel Core2 Processor with vPro Technology" (https://web.archive.org/web/20081206123107/http://download.intel.com/products/vpro/whitepaper/crossclient.pdf) (PDF). Intel. 2008. Archived from the original (ftp://download.intel.com/products/vpro/whitepaper/crossclient.pdf) (PDF) on 2008-12-06. Retrieved 2008-08-07.
2. "Architecture Guide: Intel Active Management Technology" (https://www.webcitation.org/68FLdCH2k?url=http://software.intel.com/en-us/articles/architecture-guide-intel-active-management-technology/). Intel. 2008-06-26. Archived from the original (http://softwarecommunity.intel.com/articles/eng/1032.htm) on 2012-06-07. Retrieved 2008-08-12.
3. "Remote Pc Management with Intel's vPro" (http://www.tomshardware.com/reviews/command-conquer,1591.html). Tom's Hardware Guide. Retrieved 2007-11-21.
4. "Intel vPro Chipset Lures MSPs, System Builders" (http://www.crn.com/white-box/201802550). ChannelWeb. Retrieved 1 August 2007.
5. "Intel Mostly Launches Centrino 2 Notebook Platform" (http://www.crn.com/hardware/209100230?queryText=vPro). ChannelWeb. Retrieved 1 July 2008.
6. "A new dawn for remote management? A first glimpse at Intel's vPro platform" (https://arstechnica.com/articles/paedia/hardware/vpro.ars/1). ars technica. Retrieved 2007-11-07.
7. "Revisiting vPro for Corporate Purchases" (http://mediaproducts.gartner.com/reprints/intel/153886.html). Gartner. Retrieved 2008-08-07.
8. "Answers to Frequently Asked Questions about libreboot" (http://libreboot.org/faq/#intel). *libreboot.org*. Retrieved 2015-09-25.
9. "Archived copy" (https://web.archive.org/web/20120414141100/http://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/DOCS/Implementation%20and%20Reference%20Guide/default.htm). Archived from the original (http://software.intel.com/sites/manageability/AMT_Implementation_and_Reference_Guide/DOCS/Implementation%20and%20Reference%20Guide/default.htm) on 2012-04-14. Retrieved 2012-04-30.
10. "Intel Centrino 2 with vPro Technology" (https://web.archive.org/web/20080315093244/http://download.intel.com/products/centrino/pro/316888.pdf) (PDF). Intel. Archived from the original (http://download.intel.com/products/centrino/pro/316888.pdf) (PDF) on 2008-03-15. Retrieved 2008-07-15.
11. "Intel MSP" (https://msp.intel.com/find-a-vpro-system). Msp.intel.com. Retrieved 2016-05-25.
12. "Intel® Product Security Center" (https://security-center.intel.com/advisory.aspx?intelid=INTEL-SA-00075&languageid=en-fr). *Security-center.intel.com*. Retrieved 2017-05-07.
13. Charlie Demerjian (2017-05-01). "Remote security exploit in all 2008+ Intel platforms" (https://semiaccurate.com/2017/05/01/remote-security-exploit-2008-intel-platforms/). SemiAccurate. Retrieved 2017-05-07.
14. "Red alert! Intel patches remote execution hole that's been hidden in chips since 2010" (https://www.theregister.co.uk/2017/05/01/intel_amt_me_vulnerability/). *Theregister.co.uk*. Retrieved 2017-05-07.
15. HardOCP: Purism Is Offering Laptops with Intel's Management Engine Disabled (https://www.hardocp.com/news/2017/10/22/purism_offering_laptops_intelrsquos_management_engine_disabled)
16. Garrison, Justin (2011-03-28). "How to Remotely Control Your PC (Even When it Crashes)" (http://www.howtogeek.com/56538/how-to-remotely-control-your-pc-even-when-it-crashes/). *Howtogeek.com*. Retrieved 2017-05-07.
17. "Open Manageability Developer Tool Kit | Intel® Software" (https://software.intel.com/en-us/articles/download-the-latest-version-of-manageability-developer-tool-kit/). *Software.intel.com*. Retrieved 2017-05-07.
18. "Intel vPro Technology" (http://www.intel.com/technology/vpro/). Intel. Retrieved 2008-07-14.
19. "Intel Active Management Technology System Defense and Agent Presence Overview" (https://software.intel.com/sites/default/files/82/9f/41003) (PDF). Intel. February 2007. Retrieved 2008-08-16.
20. "Intel Centrino 2 with vPro Technology" (https://web.archive.org/web/20080315145234/http://softwarecommunity.intel.com/articles/eng/1477.htm). Intel. Archived from the original (http://softwarecommunity.intel.com/articles/eng/1477.htm) on 2008-03-15. Retrieved 2008-06-30.
21. "New Intel-Based Laptops Advance All Facets of Notebook PCs" (https://web.archive.org/web/20080717125337/http://www.intel.com/pressroom/archive/releases/20080715comp_sm.htm). Intel. Archived from the original (http://www.intel.com/pressroom/archive/releases/20080715comp_sm.htm#story) on 2008-07-17. Retrieved 2008-07-15.
22. "Understanding Intel AMT over wired vs. wireless (video)" (https://web.archive.org/web/20080326134854/http://communities.intel.com/docs/DOC-1129). Intel. Archived from the original (http://communities.intel.com/docs/DOC-1129) on March 26, 2008. Retrieved 2008-08-14.
23. "Intel® vPro™ Technology" (http://www.intel.com/content/www/us/en/architecture-and-technology/vpro/vpro-technology-general.html). *Intel*.
24. "Part 3: Post Deployment of Intel vPro in an Altiris Environment: Enabling and Configuring Delayed Provisioning" (http://communities.intel.com/docs/DOC-1920). Intel (forum). Retrieved 2008-09-12.
25. "Archived copy" (https://web.archive.org/web/20140103152316/https://safefrontier.com/sites/default/files/pdf/ACTIVE%20MANAGEMENT%20CLOUD%20OVERVIEW.pdf) (PDF). Archived from the original (https://safefrontier.com/sites/default/files/pdf/ACTIVE%20MANAGEMENT%20CLOUD%20OVERVIEW.pdf) (PDF) on January 3, 2014. Retrieved July 20, 2013.
26. "Archived copy" (https://web.archive.org/web/20110220204348/http://software.intel.com/en-us/blogs/2009/07/17/intel-management-and-security-status-imss-advanced-configurations-part-9/). Archived from the original (http://software.intel.com/en-us/blogs/2009/07/17/intel-management-and-security-status-imss-advanced-configurations-part-9/) on February 20, 2011. Retrieved December 26, 2010.
27. "Intel vPro Provisioning" (http://www.planet-lab.org/files/AMT.pdf) (PDF). HP (Hewlett Packard). Retrieved 2008-06-02.
28. "vPro Setup and Configuration for the dc7700 Business PC with Intel vPro Technology" (http://www.icare.hp.com.cn/TechCenter_StaticArticle/37022/44474.pdf) (PDF). HP (Hewlett Packard). Retrieved 2008-06-02.
29. "Part 4: Post Deployment of Intel vPro in an Altiris Environment Intel: Partial UnProvDefault" (http://communities.intel.com/docs/DOC-1921). Intel (forum). Retrieved 2008-09-12.
30. "Technical Considerations for Intel AMT in a Wireless Environment" (https://software.intel.com/en-us/articles/technical-considerations-for-intel-amt-in-a-wireless-environment/). Intel. 2007-09-27. Retrieved 2008-08-16.
31. "Intel Active Management Technology Setup and Configuration Service, Version 5.0" (http://softwarecommunity.intel.com/isn/downloads/Manageability/Intel_AMT_SCS_Console_Guide_5.0.pdf) (PDF). Intel. Retrieved 2008-08-04.
32. "Intel AMT - Fast Call for Help" (http://softwareblogs.intel.com/2008/08/18/intel-amt-fast-call-for-help/). Intel. 2008-08-15. Retrieved 2008-08-17.(Intel developer's blog)
33. "Archived copy" (https://web.archive.org/web/20160103020058/http://blog.invisiblethings.org/2015/10/27/x86_harmful.html). Archived from the original (http://blog.invisiblethings.org/2015/10/27/x86_harmful.html) on 2016-01-03. Retrieved 2016-01-16.
34. "Archived copy" (https://web.archive.org/web/20141101045709/https://www.kernel.org/doc/Documentation/misc-devices/mei/mei.txt). Archived from the original (https://www.kernel.org/doc/Documentation/misc-devices/mei/mei.txt) on November 1, 2014. Retrieved February 25, 2014.
35. "Positive Technologies Blog: Disabling Intel ME 11 via undocumented mode" (http://blog.ptsecurity.com/2017/08/disabling-intel-me.html). Retrieved 2017-08-30.
36. Igor Skochinsky (Hex-Rays) Rootkit in your laptop (http://2012.ruxconbreakpoint.com/assets/Uploads/bpx/Breakpoint%202012%20Skochinsky.pdf), Ruxcon Breakpoint 2012
37. "Intel Ethernet Controller I210 Datasheet" (http://www.intel.com/content/dam/www/public/us/en/documents/datasheets/i210-ethernet-controller-datasheet.pdf) (PDF). Intel. 2013. pp. 1, 15, 52, 621–776. Retrieved 2013-11-09.
38. "Intel Ethernet Controller X540 Product Brief" (http://www.intel.com/content/dam/www/public/us/en/documents/product-briefs/ethernet-x540-brief.pdf) (PDF). Intel. 2012. Retrieved 2014-02-26.
39. Joanna Rutkowska. "A Quest to the Core" (http://invisiblethingslab.com/resources/misc09/Quest%20To%20The%20Core%20%28public%29.pdf) (PDF). *Invisiblethingslab.com*. Retrieved 2016-05-25.
40. "Archived copy" (https://web.archive.org/web/20140211075753/http://www.intel.com/content/dam/www/public/us/en/documents/datasheets/celeron-mobile-p4000-u3000-datasheet.pdf) (PDF). Archived from the original (http://www.intel.com/content/dam/www/public/us/en/documents/datasheets/celeron-mobile-p4000-u3000-datasheet.pdf) (PDF) on February 11, 2014. Retrieved February 26, 2014.
41. "Platforms II" (http://users.nik.uni-obuda.hu/sima/letoltes/magyar/SZA2011_osz/nappali/Platforms-3_E_2011_12_14.ppt) (PDF). *Users.nik.uni-obuda.hu*. Retrieved 2016-05-25.
42. "Intel Quiet System Technology 2.0: Programmer's Reference Manual" (https://software.intel.com/sites/default/files/af/73/Intel_QST_Programmers_Reference_Manual.pdf) (PDF). Intel. February 2010. Retrieved 2014-08-25.
43. "New Intel vPro Processor Technology Fortifies Security for Business PCs (news release)" (https://web.archive.org/web/20070912110718/http://www.intel.com/pressroom/archive/releases/20070827comp.htm). Intel. 2007-08-27. Archived from the original (http://www.intel.com/pressroom/archive/releases/20070827comp.htm) on 2007-09-12. Retrieved 2007-08-07.
44. "Intel® AMT Critical Firmware Vulnerability" (http://www.intel.com/content/www/us/en/architecture-and-technology/intel-amt-vulnerability-announcement.html?cid=sem43700020664978070&intel_term=intel+amt&gclid=CjwKEAjw6e_IBRDvorfv2Ku79jMSJAAuiv9YxWLVPO0LpmcztbPctTbUFHqfpKONqvJQnI4XEwwJiRoC8d7w_wcB&gclsrc=aw.ds). *Intel*. Retrieved 10 June 2017.
45. "Intel Software Network, engineer / developers forum" (http://softwarecommunity.intel.com/isn/Community/en-US/forums/thread/30235057.aspx). Intel. Retrieved 2008-08-09.
46. "Cisco Security Solutions with Intel Centrino Pro and Intel vPro Processor Technology" (http://www.intel.com/business/casestudies/cisco.pdf) (PDF). Intel. 2007.
47. "Invisible Things Lab to present two new technical presentations disclosing system-level vulnerabilities affecting modern PC hardware at its core" (http://invisiblethingslab.com/press/itl-press-2009-03.pdf) (PDF). *Invisiblethingslab.com*. Retrieved 2016-05-25.
48. "Berlin Institute of Technology : FG Security in telecommunications : Evaluating "Ring-3" Rootkits" (http://www.stewin.org/slides/pstewin-SPRING6-EvaluatingRing-3Rootkits.pdf) (PDF). *Stewin.org*. Retrieved 2016-05-25.
49. "Persistent, Stealthy Remote-controlled Dedicated Hardware Malware" (http://stewin.org/slides/44con_2013-dedicated_hw_malware-stewin_bystrov.pdf) (PDF). *Stewin.org*. Retrieved 2016-05-25.
50. "Security Evaluation of Intel's Active Management Technology" (http://web.it.kth.se/~maguire/DEGREE-PROJECT-REPORTS/100402-Vassilios_Ververis-with-cover.pdf) (PDF). *Web.it.kth.se*. Retrieved 2016-05-25.
51. "CVE - CVE-2017-5689" (https://www.cve.mitre.org/cgi-bin/cvename.cgi?name=2017-5689). *Cve.mitre.org*. Retrieved 2017-05-07.
52. "Intel Hidden Management Engine - x86 Security Risk?" (https://www.darknet.org.uk/2016/06/intel-hidden-management-engine-x86-security-risk/). Darknet. 2016-06-16. Retrieved 2017-05-07.
53. Garrett, Matthew (2017-05-01). "Intel's remote AMT vulnerablity" (https://mjg59.dreamwidth.org/48429.html). *mjg59.dreamwidth.org*. Retrieved 2017-05-07.
54. "2017-05-05 ALERT! Intel AMT EXPLOIT OUT! IT'S BAD! DISABLE AMT NOW!" (https://www.ssh.com/vulnerability/intel-amt/). *Ssh.com\Accessdate=2017-05-07*.
55. Dan Goodin (2017-05-06). "The hijacking flaw that lurked in Intel chips is worse than anyone thought" (https://arstechnica.com/security/2017/05/the-hijacking-flaw-that-lurked-in-intel-chips-is-worse-than-anyone-thought/). Ars Technica. Retrieved 2017-05-08.
56. "General: BIOS updates due to Intel AMT IME vulnerability - General Hardware - Laptop - Dell Community" (http://en.community.dell.com/support-forums/laptop/f/3518/t/20011662). *En.community.dell.com*. Retrieved 2017-05-07.
57. "Advisory note: Intel Firmware vulnerability – Fujitsu Technical Support pages from Fujitsu Fujitsu Continental Europe, Middle East, Africa & India" (http://support.ts.fujitsu.com/content/Intel_Firmware.asp). Support.ts.fujitsu.com. 2017-05-01. Retrieved 2017-05-08.
58. "HPE | HPE CS700 2.0 for VMware" (http://h22208.www2.hpe.com/eginfolib/securityalerts/CVE-2017-5689-Intel/CVE-2017-5689.html). *H22208.www2.hpe.com*. 2017-05-01. Retrieved 2017-05-07.
59. "Intel® Security Advisory regarding escalation o... |Intel Communities" (https://communities.intel.com/thread/114071). *Communities.intel.com*. Retrieved 2017-05-07.
60. "Intel Active Management Technology, Intel Small Business Technology, and Intel Standard Manageability Remote Privilege Escalation" (https://support.lenovo.com/us/en/product_security/LEN-14963). *Support.lenovo.com*. Retrieved 2017-05-07.
61. "MythBusters: CVE-2017-5689" (https://www.embedi.com/news/mythbusters-cve-2017-5689). *Embedi.com*. Retrieved 2017-05-07.
62. Charlie Demerjian (2017-05-01). "Remote security exploit in all 2008+ Intel platforms" (https://semiaccurate.com/2017/05/01/remote-security-exploit-2008-intel-platforms/). *SemiAccurate.com*. Retrieved 2017-05-07.
63. "Sneaky hackers use Intel management tools to bypass Windows firewall" (https://arstechnica.com/security/2017/06/sneaky-hackers-use-intel-management-tools-to-bypass-windows-firewall/). Retrieved 10 June 2017.
64. Tung, Liam. "Windows firewall dodged by 'hot-patching' spies using Intel AMT, says Microsoft - ZDNet" (http://www.zdnet.com/article/windows-firewall-dodged-by-hot-patching-spies-using-intel-amt-says-microsoft/). Retrieved 10 June 2017.
65. "PLATINUM continues to evolve, find ways to maintain invisibility" (https://blogs.technet.microsoft.com/mmpc/2017/06/07/platinum-continues-to-evolve-find-ways-to-maintain-invisibility/). Retrieved 10 June 2017.
66. "Malware Uses Obscure Intel CPU Feature to Steal Data and Avoid Firewalls" (https://www.bleepingcomputer.com/news/security/malware-uses-obscure-intel-cpu-feature-to-steal-data-and-avoid-firewalls/). Retrieved 10 June 2017.
67. "Hackers abuse low-level management feature for invisible backdoor" (https://www.itnews.com.au/news/hackers-abuse-low-level-management-feature-for-invisible-backdoor-464499). *iTnews*. Retrieved 10 June 2017.
68. "Vxers exploit Intel's Active Management for malware-over-LAN • The Register" (https://www.theregister.co.uk/AMP/2017/06/08/vxers_exploit_intels_amt_for_malwareoverlan/). *www.theregister.co.uk*. Retrieved 10 June 2017.
69. Security, heise. "Intel-Fernwartung AMT bei Angriffen auf PCs genutzt" (https://www.heise.de/security/meldung/Intel-Fernwartung-AMT-bei-Angriffen-auf-PCs-genutzt-3739441.html). *Security*. Retrieved 10 June 2017.
70. "PLATINUM activity group file-transfer method using Intel AMT SOL" (https://channel9.msdn.com/Shows/Windows-Security-Blog/PLATINUM-activity-group-file-transfer-method-using-Intel-AMT-SOL). *Channel 9*. Retrieved 10 June 2017.
71. "Disabling AMT in BIOS" (https://software.intel.com/en-us/forums/intel-business-client-software-development/topic/285926#comment-1503750). *software.intel.com*. Retrieved 2017-05-17.
72. "Are consumer PCs safe from the Intel ME/AMT exploit? - SemiAccurate" (https://semiaccurate.com/2017/05/03/consumer-pcs-safe-intel-meamt-exploit/). *semiaccurate.com*.
73. "Intel x86s hide another CPU that can take over your machine (you can't audit it)" (http://boingboing.net/2016/06/15/intel-x86-processors-ship-with.html). *Boing Boing*. 2016-06-15. Retrieved 2017-05-11.
74. "[coreboot] : AMT bug" (https://mail.coreboot.org/pipermail/coreboot/2017-May/084250.html). *Mail.coreboot.org*. 2017-05-11. Retrieved 2017-06-13.
75. "Disabling Intel AMT on Windows (and a simpler CVE-2017-5689 Mitigation Guide)" (https://mattermedia.com/blog/disabling-intel-amt/). *Social Media Marketing | Digital Marketing | Electronic Commerce*. 2017-05-03. Retrieved 2017-05-17.
76. "bartblaze/Disable-Intel-AMT" (https://github.com/bartblaze/Disable-Intel-AMT). *GitHub*. Retrieved 2017-05-17.
77. "mjg59/mei-amt-check" (https://github.com/mjg59/mei-amt-check). *GitHub*. Retrieved 2017-05-17.
78. "Intel® AMT Critical Firmware Vulnerability" (https://www.intel.com/content/www/us/en/architecture-and-technology/intel-amt-vulnerability-announcement.html#usefulresources). *Intel*. Retrieved 2017-05-17.
79. Vaughan-Nichols, Steven J. "Taurinus X200: Now the most 'Free Software' laptop on the planet - ZDNet" (http://www.zdnet.com/article/a-new-free-software-laptop-arrives/).
80. Kißling, Kristian. "Libreboot: Thinkpad X220 ohne Management Engine » Linux-Magazin" (http://www.linux-magazin.de/NEWS/Libreboot-Thinkpad-X220-ohne-Management-Engine). *Linux-Magazin*.
81. online, heise. "Libiquity Taurinus X200: Linux-Notebook ohne Intels Management Engine" (https://www.heise.de/newsticker/meldung/Libiquity-Taurinus-X200-Linux-Notebook-ohne-Intels-Management-Engine-2835910.html). *heise online*.
82. "Intel AMT Vulnerability Shows Intel's Management Engine Can Be Dangerous" (http://www.tomshardware.co.uk/intel-amt-vulnerability-me-dangerous,news-55499.html). 2 May 2017.
83. "Purism Explains Why It Avoids Intel's AMT And Networking Cards For Its Privacy-Focused 'Librem' Notebooks" (http://www.tomshardware.com/news/purism-notebooks-avoid-intel-amt,32576.html). *Tom's Hardware*. 2016-08-29. Retrieved 2017-05-10.
84. "The Free Software Foundation loves this laptop, but you won't" (http://www.pcworld.com/article/2879086/the-free-software-foundation-loves-this-laptop-but-you-wont.html).
85. "FSF Endorses Yet Another (Outdated) Laptop - Phoronix" (https://phoronix.com/scan.php?page=news_item&px=FSF-RYF-Another-X200). *phoronix.com*.

External links

- Intel Active Management Technology (http://www.intel.com/technology/platform-technology/intel-amt/)
- Intel Manageability Developer Community (https://web.archive.org/web/20080126234743/http://softwarecommunity.intel.com/isn/home/manageability.aspx)
- Intel vPro Expert Center (http://www.intel.com/go/vproexpert)
- Intel AMT Open Source Drivers and Tools (http://www.openamt.org/)
- Intel 82573E Gigabit Ethernet Controller (Tekoa) (http://www.intel.com/design/network/products/lan/controllers/82573.htm)
- ARC4 Processor (http://www.arc.com/upload/download/F1010.5_ARC%20A4_4-9-03_FINAL.pdf)
- AMT videos (select the desktop channel) (http://video.intel.com/)
- Intel AMT Client - Radmin Viewer 3.3 (https://web.archive.org/web/20090130050515/http://www.radmin.com/products/radmin/intel_amt_features.php)
- Intel vPro/AMT as a hardware antivirus (http://www.foxnetwork.ru/index.php/en/component/content/article/105-intel-amt.html)
- AMT Over the Internet Provisioning (OOB Manager) (https://web.archive.org/web/20130802104832/http://demoamt.tsges.com/demo_amt/index.php?r=site%2Findex)
- Intel ME Secrets: Hidden code in your chipset and how to discover what exactly it does (http://www.slideshare.net/codeblue_jp/igor-skochinsky-enpub) by Igor Skochinsky, talk at Code Blue 2014
- Using Intel AMT and the Intel NUC with Ubuntu (http://blog.dustinkirkland.com/2013/12/everything-you-need-to-know-about-intel.html)

Retrieved from "https://en.wikipedia.org/w/index.php?title=Intel_Active_Management_Technology&oldid=810652351"

This page was last edited on 16 November 2017, at 16:17.