Security Best Practices of Intel® Active Management Technology Q&A
January 2018

Intended Audience

This Q&A is for Intel customers who plan to deploy and activate Intel® Active Management Technology (Intel® AMT).

Content Summary:

This Q&A focuses on security practices around provisioning Intel® AMT, its security considerations, and security practices in the following areas:

- Intel AMT provisioning via Manual Configuration
- IDE-R/USB-R and Serial over LAN
- HTTP digest Authentication schema
- Remote provisioning
- Wireless Intel AMT

Key Messages

- Intel recommends following security best practices including running with the least privileged access, and keeping firmware, security software & operating systems up to date.
- Intel makes every effort to protect our platforms from attack and takes reports of issues seriously investigating each to determine merit and opportunities to further enhance system security.
- There are published best known methods and recommended security configurations that mitigate most issues raised in this Q&A.
- To exploit the potential vulnerability, a malicious user would need physical possession of the system in order to attempt manipulation of Intel AMT configurations.

Contacts: For technical assistance, please contact Intel Customer Support at https://www.intel.com/content/www/us/en/support/intel-business-support.html

Questions and Answers:

Q1. Why this Q & A?
A1. This Q & A is to articulate best practices in securing the platform and Intel AMT security capabilities and to further clarify certain misperceptions of Intel AMT security vulnerabilities, which would require the attacker to have physical access to the device and OS administrator credentials to attempt this exploit.

Q2. Are there security concerns with Intel Active Management Technology?
A2. The Intel® vPro™ platform and its included Intel Active Management Technology has supplied differentiated hardware-assisted security and manageability capabilities to over 100 million systems over the last decade. When Intel receives a report of a potential security vulnerability in our products, we begin evaluation of the report. We confirm the potential vulnerability, assesses the risk, determine the impact, and assign a processing priority. After vulnerability confirmation, the priority determines issue handling throughout the remaining steps in the process. For severe issues requiring immediate mitigation steps, communication occurs through https://www.intel.com/security.

Q3. Are there security vulnerabilities in your product(s)?
A3. Intel recognizes our role in improving the security of the computing platform. Intel actively works to identify and resolve security vulnerabilities. In the event that vulnerabilities are identified, the Product Security Incident Response Team (PSIRT) works across Intel and with the security community to understand the vulnerability and the underlying issue. The PSIRT has the responsibility to communicate with our suppliers, customers, and end users. Public communications from the PSIRT team are available at https://www.intel.com/security.

Below is a list of Security Advisories that apply to Intel Active Management Technology

Advisory Number	Advisory Title
INTEL-SA-00075	Intel Active Management Technology, Intel Small Business Technology, and Intel Standard Manageability Escalation of Privilege
INTEL-SA-00081	Intel® AMT Clickjacking Vulnerability
INTEL-SA-00082	Intel AMT® Upgradable to Vulnerable Firmware
INTEL-SA-00086	Intel Q3'17 ME 11.x, SPS 4.0, and TXE 3.0 Security Review Cumulative Update
INTEL-SA-00093	Frame replay vulnerability in Wi-Fi subsystem in Intel® Dual-Band and Tri-Band Wireless-AC Products allows remote attacker to replay frames via channel-based man-in-the-middle
INTEL-SA-00101	One or more Intel Products affected by the Wi-Fi Protected Access II (WPA2) protocol vulnerability

Q4. If Intel knew of a security issue with its products would you disclose that issue?
A4. Intel is committed to addressing security vulnerabilities affecting our customers and providing responsible guidance on the solution, impact, severity and mitigation. The latest information about product security issues is available on our portal https://security-center.intel.com/.

Q5. What prevents malicious software from using Intel AMT to exploit a PC and what authentication mechanism is used to prevent an unauthorized person from gaining access?
A5. Access and communications between Intel AMT and authorized management consoles can be fully encrypted. Even if authorized management consoles are not "encrypted", the communication with Intel AMT requires valid credential setup during configuration, either digest authentication or Kerberos authentication are supported. It is also possible to setup Intel AMT to require a client x509v3 certificate (aka TLS mutual authentication) to provide additional security. In addition, IT administrators' access can be limited to only certain remote features and full privilege can be granted only to those with Admin rights. Intel AMT also includes an Access Monitor feature that allows only an Auditor to clear out logs to help deter malicious insider attacks.

Q6. Is Intel AMT disabled by default on Intel vPro platforms? If not, can it be disabled or have any default passwords changed by end users not part of the IT-supported network?
A6. Depending on the customers' request, Intel vPro platforms can be delivered by OEMs in one of the following Intel AMT states: un-provisioned and ON in BIOS, un-provisioned and OFF in BIOS, and un-provisioned and permanently OFF in BIOS. The Intel AMT firmware does not search for a configuration server when being plugged in the network for the first time, this capability was removed in AMT 6.0 and later platforms. Intel recommends when receiving a new Intel AMT capable platform with Intel AMT turned ON in the BIOS, that the default password be changed and Intel AMT be provisioned.

Q7. What is the Intel® Management Engine BIOS Extension (Intel® MEBX)?
A7. The Intel® Management Engine BIOS Extension (Intel® MEBX) is an additional BIOS menu present only on Intel AMT systems. This menu is displayed if the local user presses a special key combination (usually Ctrl-P) during system POST. The Intel MEBX can be used to locally configure Intel AMT.

Q8. How do I change the default Intel MEBX password?
A8. Before the Intel MEBX can be used, the default password must be changed. This can be done locally by the user pressing a special key combination (usually Ctrl-P) during system POST and following the prompts. The Intel MEBX can also be changed remotely during the Intel AMT configuration process. To configure Intel AMT remotely you can leverage the Intel® Remote Configuration Server (RCS) to configure the system into Admin Control Mode. Client Control Mode does not support changing the Intel MEBX password.

Q9. Are there security vulnerabilities in Manual Configuration of Intel AMT provisioning via Intel MEBX or USB key?
A9. The Intel AMT manual configuration methods let you provision an Intel AMT system with basic settings, but they do require local access to the device in order to boot to the Intel MEBX or a configured USB key. If the Intel MEBX default password was never changed, an unauthorized person with physical access to the system could manually provision Intel AMT via the Intel MEBX or with a USB key using the default password. Once configured, Intel AMT allows remote access to the Intel AMT feature set on the local area network (LAN). If the system's manufacturer has followed Intel's recommendation to protect the Intel MEBX menu with the system BIOS password, this physical attack would be mitigated

Q10. Has Intel provided guidance to system manufacturers to reduce the potential vulnerability of unauthorized Intel AMT provisioning via Manual Configuration?
A10. Yes, Intel has provided recommendations to system manufacturers in September 2015 to protect the Intel MEBX with the system BIOS password. Intel has also recommended that system manufacturers provide a system BIOS option to disable USB provisioning and to set the value to disable by default.

Q11. Is there a method to detect if an unauthorized attacker has access to my Intel AMT system?
A11. Intel AMT provides event log and audit log capabilities that can provide detail on use of Intel AMT capabilities. However, users with the Intel AMT password have the ability to clear event logs or fill logs in an attempt to obfuscate their activity. The use of the AMT "KVM remote control" feature provides a prominent and mandatory flashing border indicating an active KVM session; however, this relies on the local user being present to observe it.

Q12. Are there security vulnerabilities in IDE-R and Serial over LAN?
A12. In legacy systems (AMT 5.x and older), passwords could be visible when performing SOL/IDER only when TLS is disabled. In AMT 6.0 and later versions, Intel has further hardened these features by supporting an additional authentication scheme.

Q13. Are there security vulnerabilities in an HTTP digest authentication scheme?
A13 HTTP digest authentication requires a username and password as forms of identification. While it is theoretically possible to uncover the Intel AMT credentials that are exchanged during HTTP digest authentication. Due to this less secure method, a majority of our customers use Kerberos-based authentication schemes

Q14. Are there security vulnerabilities in Intel AMT related to Remote Provisioning?
A14. A complex sequence of successful CA infrastructure and domain hacks would be required to purchase and install a compromised certificate. In addition to the certificate, you will need to gain access to the network by setting up a rogue DHCP server and also have administrative rights to the clients in order to perform remote provisioning tasks.

Q15. Are there security vulnerabilities in wireless Intel® AMT related to 802.11?
A15. There are generic security concerns on all 802.11 compliant products (Intel AMT and non-AMT). Intel has implemented AMT configurations preventing connections to open networks, enforcing a password policy for PSK profiles; Intel AMT configuration only allows an AMT authorized user to add a wireless profile. Additionally, 802.1x authentication and 802.11i encryption are both supported for secure WLAN connections.