Black Box Inside

A study about Computer Trust and Freedom

Parafestas Nikos

Xanthi, 7 January, 2024

Abstract

The dominant trend concerning cybersecurity, at a scientific as well as an executive level, is the a priori acceptance that manufacturers of technology products are trustworthy. So, security measures are designed, focusing exclusively on the higher levels of a computer system, excluding highly important parts, such as the operating system and firmware. Furthermore, there are other parts that are fundamentally more crucial in operation and, thus, in security. Inside almost all computing systems, such as laptops and mobile phones, resides an independent microcontroller that has administrator access to all its subsystems. This special type of hardware has unlimited access to the contents of the hard disk and memory, to the network devices, even to what the user views on the screen. The above mentioned are feasible, regardless of the operating system, even remotely, while the system is in shutdown mode. These "black boxes" are advertised as features that protect users from cybercriminals. In this paper, this argument is examined by exploring the relationship between trust and freedom in technology.

Keywords: Intel Management Engine, Free Software, Free Hardware, Free Bios, Privacy, Surveillance, Trust

N. Parafestas, Xanthi 2024.

Acknowledgments

This paper was finished with my partner's help, Vasileiadou Alexandra, who tried her best to proofread and correct my grammar and spelling mistakes, while being at the passenger seat in a 800 km journey with our kids.

I would, also, like to express my gratitude to the free software community, especially the Trisquel and FSF member forum for their responses and, of course, to the developers of coreboot, libreboot and gnuboot who are giving users freedom respecting alternative.

Contents

List of Figures

List of Tables

Chapter 1

Trust, Surveillance and Freedom in Technology

1.1 Technology under Surveillance

In the past years, it has become evident that technology influences our lives daily in unforeseen ways.

Edward Snowden's revelations in June 2013 [McCarthy, 2013] confirmed what was previously only suspected: that governments and private software companies are working closely to spy on their citizens and foreign countries. The authenticity of Snowden's leaks was acknowledged even by the US government [BBC, 2020].

In the European Union there are reports [Mildebrath, 2022] that citizens, journalists and rival politicians are currently monitored by governments, sometimes following orders given by the head of state .

Communication privacy is in question with "EARN IT" in the US [McKinney, 2023], "Chat Control"[1] in the E.U. [Breyer, 2023] and the "Online Safety Bill" in Great Britain [Clark, 2023]. All three bills propose the effective abolition of encryption through the mandatory introduction of backdoors in chat software. Other countries like China and Russia, have great privacy issues [Dixon, 2021] too.

The above mentioned, reasonably raises the question [Stallman, 2023c]:

> How Much Surveillance Can Democracy Withstand?

1.2 Layers of Trust

In the age of surveillance capitalism [Zuboff, 2023], people deserve a technological environment, in which they will feel that they are safe . In order to define what one can trust, we need to understand and describe this environment so that we can analyze the reliability of its components.

In order to ensure security, the various layers of a computer system are isolated from each other, like the circular, hierarchically distributed structure in Figure 1.1 [Hertzsprung, 2020]. Starting from the one with the greater administrator privileges in the center, these layers are [Wiley, 2011]:

[1] Chat Control bill is currently on hold.

- Ring 0: Trusted level - Operating system kernel
- Ring 1: Trusted layer - Components of the operating system that are not in the kernel
- Ring 2: Hardware Abstraction Layer (HAL) - I/O driver and utilities
- Ring 3: User level - Applications and programs

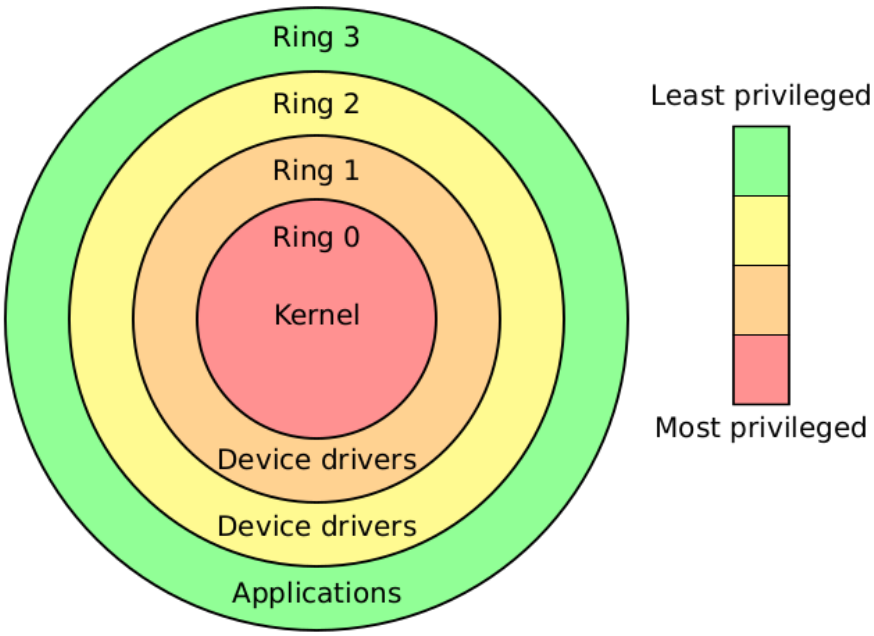

Figure 1.1: Privilege rings for the x86 architecture in protected mode.

A user can be confident that a computing system is a trustworthy if every single one of these layers is trustworthy.

1.3 Trust in Software

> Trust may not be the sort of attitude that one can will oneself to have without any evidence of a person's trustworthiness.[2]

There are various incidents [GNU, 2023b] that justify loosing trust in proprietary software, usually shipped in consumer devices. Since most commercial platforms don't provide a way to access the software source code, acquiring tangible proof of its reliability is extremely limited.

Free Software on the other hand, gives users full control over the software they use by providing the following [GNU, 2023c]:

- The freedom to run the program as you wish, for any purpose (freedom 0).

[2] «Trust». Stanford Encyclopedia of Philosophy Archive [McLeod, 2023]

- The freedom to study how the program works, and change it so it does your computing as you wish (freedom 1). Access to the source code is a precondition for this.
- The freedom to redistribute copies so you can help others (freedom 2).
- The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes. Access to the source code is a precondition for this.

All of these conditions must be met in order for the software to be free.

Being able to run, modify, copy, and share software is a precondition to privacy. Having the freedom to audit the software, can provide evidence to trust it. An example of software that respects the above mentioned four freedoms and provides trust to its users is GNU/Linux operating system, which emerged from the GNU Software Suite Project [Stallman, 2023a] and the Linux kernel. Free Software Foundation maintains a free software directory at https://directory.fsf.org.

1.4 Trust in Hardware

Hardware is often considered as being immune to attack. But, being in the center of a computing system, its potential lack of security has a much greater impact than the operating system and software. [Bhunia and Tehranipoor, 2019].

As we saw in Section 1.3 for software and operating systems, there is a reliable alternative. By using free software like GNU/Linux, one can have a high degree of trust in the digital part of a device. Ensuring a trustworthy hardware is a more complicated task.

A common term in cybersecurity is "Roots of Trust", referring to computer elements trusted to perform critical security functions. The US National Institute of Standards and Technology proposes the following definition [NIST, 2020]:

> Roots of trust are highly reliable hardware, firmware, and software components that perform specific, critical security functions. Because roots of trust are inherently trusted, they must be secure by design. As such, many roots of trust are implemented in hardware so that malware cannot tamper with the functions they provide. Roots of trust provide a firm foundation from which to build security and trust.

Having physical access to hardware, users can open up a computer and analyze its parts, so that they can be confident that it is composed of what the manufacturer claims.

On the other hand, hardware includes a special type of software; firmware. It's role is to act like a bridge between software and hardware. It is a series of instructions that allow an electronic device (such as a chip) to communicate with the rest of a computer's electronic parts and/or with its

operating system. Firmware that can be modified, should be considered software [Stallman, 2023b], therefore it must be treated, in terms of trust, as well as freedom, in the same way as software, which means, we can either trust it (if it is free firmware) or not (if it is non-free firmware).

1.5 Trust in cybersecurity

If we assume that we can trust something we have no clear knowledge of its actual operation, consequently, all other security measures are based on assumptions. This is, unfortunately, something that, both academically and professionally, is frequent in the field of cybersecurity. A security plan, for example, that doesn't take into account both software and hardware in every layer is incomplete: opting out crucial parts possibly results in trusting something that we should not trust.

Non-free software, whether in firmware or in the upper layers, is only the tip of the iceberg. There is another usually overlooked piece of hardware that lies at the core of modern devices, a computer inside the computer.

Chapter 2

Intel ME - A computer inside the computer

2.1 Introduction to Intel ME

The prioritization of the levels mentioned in Section 1.2 reflects their importance in security. The lower it is, the more (and higher) segments it affects.

A device independent of these layers, which has powerful administration rights to interact with, and control every other component of a computing system is the Intel Management Engine (IME).

This is an integrated microcomputer found inside all Intel-based computers from 2006 onward, which runs in parallel to the main unit, even when it is turned off [DG and M, 2018]. Alternative trade names for IME are Manageability Engine, Converged Security and Management Engine (CSME), and Intel vPro technology. On mobile devices such as phones and tablets IME is called the Trusted Execution Engine.

2.2 Historical overview

IME's first appearance was in 2005 as a typical Ethernet controller control system. The name IME introduced in 2007 as an implementation of AMT (see subsection 2.5.1) and not as a complete system [Ruan, 2014][1]. Since 2008, IME has been found as a standalone system on all Intel-based computers [Erica and Peter, 2017].

2.3 Literature Review

Bibliographic reference to IME is limited, considering its critical role in the security of a computer system. In this section, an attempt is made to categorize and present these sources.

[1] page 27

2.3.1 Books

The first book on IME was published by Intel in 2009, entitled "Active Platform Management Demystified: Unleashing the Power of Intel VPro Technology" [Kumar et al., 2009]. Later, in 2014, the book "Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management" was published [Ruan, 2014]. Like the first publication from Intel, this book also does not consider the ethical parameters and risks concerining this specific technology. Also, despite the author's [2] negative attitude towards non proprietary software [3], it is an important textbook describing IME. Given the minor changes in its overall operation over the years, the book is still relevant.

2.3.2 Scientific articles

The search for scientific articles revealed a distinct lack of valid published research on IME. A notable exemption is [Ogolyuk et al., 2017].

2.3.3 Conferences - Presentations - Audiovisual Material - Technical Manuals

Fortunately, there is plenty of material and multiple references to IME on a number of websites and conferences. In Table 2.1 there is a list of useful resources.

2.3.4 Free Software Foundation Campaign

Free Software Foundation has been particularly critical of Intel IME. FSF launched a campaign against Intel AMT [Vandewege et al., 2014] (more on AMT in Subsection 2.5.1) and later the campaign continued targeting IME [Gay, 2016], [DG and M, 2018]. To the FSF's view, removing IME from computing systems is essential to achieving user freedom.

2.4 Accessibility

IME cannot be restricted even by the security measures of the operating system, regardless if its Windows, Linux or Android; it has access to the entire RAM and hard drive and it communicates with the main unit to perform special processes. In terms of power management, IME has the ability to turn off the device at any time [Ruan, 2014][4]. It has remote access to both wired and wireless networks by directly accessing the network devices, without interfering with the operating system or other systems [Ruan, 2014][5]. It also has the ability to lock the operating system if the

[2] The author is an employee at Intel

[3] X. Ruan uses the term open source rather than free software. Despite many similarities, there are also important differences [Stallman, 2023d].

[4] page 90

[5] page 36

Title	Type	Description	Year
Intel's Management Engine is a security hazard, and users need a way to disable it	Online article by Electronic Frontier Foundation	Registration of privacy issues	2017
Intel ME: Myths and reality	Presentation at the 34th Chaos Communication Congress	Mentions the difficulties of inspecting and disabling IME.	2017
Behind the Scenes of Intel Security and Manageability Engine	Presentation at "Black Hat" conference	Operation description of IME version 12. Contains operation diagram, boot flow, upgrade process, etc.	2019
Intel Converged Security and Management Engine	Technical Manual	Reference to operating parameters for IME versions 14.0, 15 and 16.0.	2022

Table 2.1: Other IME related resources

firmware is modified, remotely control the display, and prevent playback of audiovisual material by applying Digital Restriction Management (DRM) [Ruan, 2014][6].

2.5 IME Modules

2.5.1 Intel Active Management Technology

There is a common confusion between IME and Active Management Technology (AMT). AMT, though, is just an IME application. It is only one of IME's components.

Platforms using AMT can be remotely controlled, regardless of their power status independently of the operating system [Intel, 2021a].

Some of the features it provides are [Vandewege et al., 2014]:

- Power control
- BIOS configuration and upgrade
- Disk clean up
- System reinstall
- Console access (VNC)

These are powerful features that make AMT, and therefore IME, powerful components in computer security.

[6] page 49

2.5.2 Booting Limitations

In 2011, Microsoft announced that the Windows 8 operating system would only run on Windows 8 certified computers with Secure Boot preinstalled.

Microsoft claims that the system is designed to protect a computer from malware by preventing unauthorized programs from running at computer startup.

More specifically, if Secure Boot is enabled while starting the computer, there is an ongoing check to see whether the digital signature of the bootloader software has been modified. The computer will only boot if the bootloader was signed using a trusted certificate from Microsoft or if the user manually approves the digital signature [Pamnani et al., 2023].

When Secure Boot is activated, it is impossible to install an alternative bootloader (see chapter 4).

Redhat and Canonical have issued a joint technical manual where they criticize this option, noting that [Kerr et al., 2011]:

> Windows 8's Secure Boot requirement will push manufacturers to implement Secure Boot.
>
> We believe that restrictions that prevent users from exercising full control over their devices are not in the best interest of those users.

Despite the initial announcement, these companies eventually succumbed to market pressure to use Secure Boot [Debian, 2023].

Another campaign, this time against Secure Boot continues to be waged by the FSF, calling the module as "Restricted Boot" [Gay, 2011]. The main claim is that although it can be disabled, it is a significant barrier to novice users using an alternative, non-Microsoft-approved operating system, thus strengthening the latter's monopoly in the PC market.

As to security, it is worth mentioning that on March 1, 2023, researchers from ESET Cybersecurity Firm reported "The first widely available UEFI bootkit to bypass UEFI Secure Boot", named "BlackLotus" [Smolar, 2023].

2.5.3 Other Applications

Other IME add-ons are (i) "Quiet System Technology" (QST) that regulates the speed of the computer's internal fan by controlling operations like temperature, voltage, and current and (ii) "Protected Audio Video Path", that is used to enforce digital rights management (or DRM) protections on content.

2.5.4 A Lost Opportunity

Applications provided by the IME could provide significant assistance in managing and securing a computer. Unfortunately, as described in Section 3.2.3, Intel doesn't provide enough evidence that is is a secure, thus a trustworthy, system. Furthermore, by making IME is hard coded in all consumer devices, Intel is depriving users even from having the choice not to use it.

Chapter 3

Security overview

3.1 Trust levels below 0

Figure 1.1 in Section 1.2 is now considered obsolete. It should be supplemented with added highly privileged layers that are below the lowest level of the core (ring 0) (see Figure 3.1 [Parafestas, 2023]). These layers are the Hypervisor, (Ring -1), the UEFI/Bios (Ring -2) and finally the IME (Ring -3) [1].

This representation highlights that IME is at the heart of modern computing systems, with unlimited control and privileges over all other subsystems. Because of its importance, until IME is completely trusted, any protection plan built on top of it can potentially be compromised.

3.2 IME Security

3.2.1 Marketing in Technology

The IME technical manual states that "no computer system can be completely secure" [Gehler et al., 2022][2]. This is a valid observation. Computing systems are used in various environments, with new threats and challenges in the field of cybersecurity constantly emerging.

At the same time, as big tech board's main goal is to increase their profits, they have upgraded marketing departments in decision making, downgrading technical and operational department's participation. This often leads to releasing unfinished and insecure products to the market. just to have a commercial edge against the competitors. This inevitably has an impact on security.

3.2.2 Security Vulnerabilities

3.2.2.1 Common Vulnerabilities and Exposures (CVE)

The USA's National Institute of Standards and Technology (NIST), gives the following definition for vulnerability [NIST, 2022]:

[1] AMD systems have PSP instead of IME (see Section 4.1)

[2] page 2

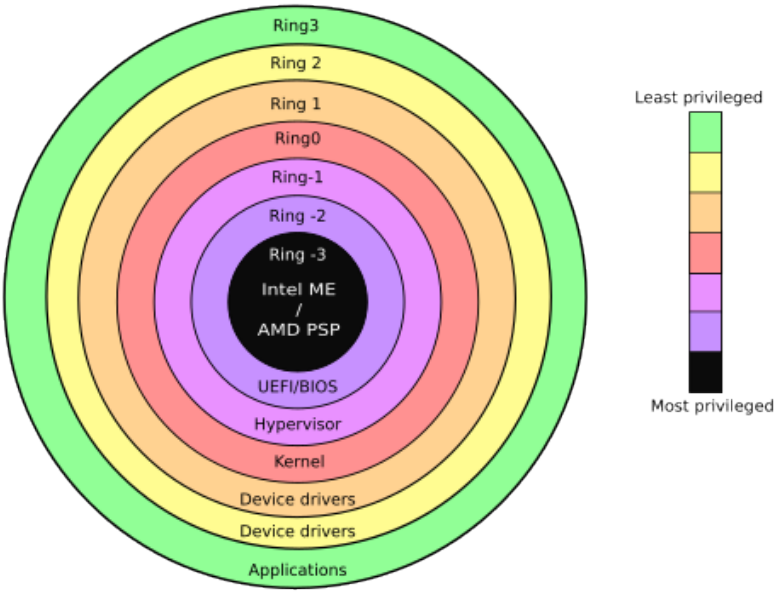

Figure 3.1: Privilege rings for the x86 architecture with additional rings

> "A weakness in the computational logic (e.g., code) found in software and hardware components that, when exploited, results in a negative impact to confidentiality, integrity, or availability. Mitigation of the vulnerabilities in this context typically involves coding changes, but could also include specification changes or even specification deprecations (e.g., removal of affected protocols or functionality in their entirety)."

Common Vulnerabilities and Exposures (CVE) have been established for standardization and consensus among IT and cybersecurity professionals. It is a list of computer security vulnerabilities. A reference to a CVE, means a security flaw, to which has been assigned a specific CVE ID number [RedHat, 2021]. The CVE program is supervised by MITER and funded by the US Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

The Common Vulnerability Scoring System (CVSS) is complement to the CVE. Its main characteristics of vulnerability are recorded on a scale that reflects its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high and critical) to help organizations properly assess and prioritize their vulnerability management responses [FIRST, 2023].

3.2.2.2 Vulnerabilities of AMT and IME

Table 3.2 lists the NIST vulnerability database entries related to Intel AMT, while Table 3.3 lists the vulnerabilities related to the rest of the IME implementations.

As this is a non-free system (see Section 1.3), any security gaps in AMT and IME can be recorded by third parties through behavior observation. If, on the other hand, the software were free, then the source code would be accessible, and security tests could be performed, not only dynamically by simulating attacks (black-boxing), but also statically by studying the code (white-boxing) or even combined (grey-boxing control) [Felderer et al., 2016].

Critical CVEs recorded in Table 3.2 and Table 3.3 are analyzed in depth in Table 3.4

3.2.2.3 Silent Bob is Silent

To better understand the operation and risks of IME on a computing system, the CVE-2017-5689 vulnerability will be further analyzed. This is a critical vulnerability (see Table 3.4), with a score of 9.8 on the CVSS V3.1 scale according to NIST.

The research team that disclosed it to Intel noted that it affects home computers, laptops and servers since 2010 made by Dell, Fujitsu, HP, Intel, Lenovo and other companies, and that IME systems that do not have AMT may also be at risk [EMBEDI, 2017]. The vulnerability was nicknamed "Silent Bob is Silent".

Using a few lines of code, [Ylonen, 2018], an unprivileged malicious user could gain administrative access not only to the compromised computer itself, but also to any other computer that is on the same internal network.

Intel finally reported the vulnerability on May 1, 2017 [Intel, 2017]. The security flaw was active for seven years until it was patched by Intel. All this time, anyone could have spotted it, as the research team that noticed the flaw used information that was already available.

3.2.3 A potential security hole that remains permanently active

Given the critical role of IME and the extremely high security vulnerabilities that exist or will occur in the future, it is understandable that one would try to disable or remove it at will. Up until nowadays, however, there is no official method for such an operation [McKinney, 2023] as Intel replies that removing IME creates security issues [Erica and Peter, 2017]. After IME version 6.0, all systems with Intel Core i3/i5/i7 processors and PCH (Platform Controller Hubs) include "ME Ignition" firmware that performs some sort of hardware initialization and power management. If the IME boot ROM does not find a valid Intel-signed ME firmware manifest in the SPI flash, the entire computer will shut down after 30 minutes [GNU, 2023a] making its removal impossible.

Ranking according to CVSS rating (v.3.1)	Number of Registered Vulnerabilities	CVE
Low CVSS ∈ [0.1-3.9]	0	
Medium CVSS ∈ [4.0-6.9]	22	CVE-2022-30944 CVE-2022-28697 CVE-2021-33159 CVE-2021-33107 CVE-2021-33068 CVE-2020-8757 CVE-2020-8746 CVE-2020-12356 CVE-2020-8674 CVE-2020-0537 CVE-2020-0535 CVE-2020-0531 CVE-2019-11100 CVE-2019-11086 CVE-2019-0097 CVE-2019-0094 CVE-2019-0092 CVE-2018-3657 CVE-2018-3658 CVE-2018-12196 CVE-2018-12185 CVE-2017-5698
High CVSS ∈ [7.0-8.9]	25	CVE-2022-36392 CVE-2022-29893 CVE-2022-27497 CVE-2022-26341 CVE-2020-8760 CVE-2020-8754 CVE-2020-8753 CVE-2020-8749 CVE-2020-8353 CVE-2020-12354 CVE-2020-0597 CVE-2020-0596 CVE-2020-0540 CVE-2020-0538 CVE-2020-0532 CVE-2019-11132 CVE-2019-11088 CVE-2019-0166 CVE-2019-0131 CVE-2019-0096 CVE-2018-19434 CVE-2018-12187 CVE-2017-5697 CVE-2017-5711 CVE-2017-5712
Critical CVSS ∈ [9.0-10.0]	10	CVE-2022-26845 CVE-2022-30601 CVE-2020-8752 CVE-2020-8747 CVE-2020-8758 CVE-2020-0595 CVE-2020-0594 CVE-2019-11131 CVE-2019-11107 CVE-2017-5689

Table 3.2: IME vulnerabilities involving AMT

Ranking according to CVSS rating (v.3.1)	Number of Registered Vulnerabilities	CVE
Low CVSS ∈ [0.1-3.9]	0	
Medium CVSS ∈ [4.0-6.9]	39	CVE-2022-26047 CVE-2021-3786 CVE-2020-8703 CVE-2020-24516 CVE-2020-24507 CVE-2020-24506 CVE-2020-8761 CVE-2020-8756 CVE-2020-8755 CVE-2020-8751 CVE-2020-8745 CVE-2020-8705 CVE-2020-0545 CVE-2020-0541 CVE-2020-0539 CVE-2020-0533 CVE-2020-8336 CVE-2019-14598 CVE-2019-11110 CVE-2019-11108 CVE-2019-11106 CVE-2019-11105 CVE-2019-11102 CVE-2019-11101 CVE-2019-11087 CVE-2019-0168 CVE-2019-0165 CVE-2019-0098 CVE-2019-0093 CVE-2018-12199 CVE-2018-12192 CVE-2018-12190 CVE-2018-12189 CVE-2018-12188 CVE-2018-12147 CVE-2018-3659 CVE-2018-3632 CVE-2018-3629 CVE-2016-8224
High CVSS ∈ [7.0-8.9]	20	CVE-2022-29871 CVE-2020-8744 CVE-2020-12303 CVE-2020-12297 CVE-2020-0542 CVE-2020-0536 CVE-2020-0534 CVE-2019-11147 CVE-2019-11104 CVE-2019-11103 CVE-2019-0169 CVE-2019-0091 CVE-2019-0090 CVE-2019-0086 CVE-2018-12208 CVE-2018-12191 CVE-2018-3655 CVE-2018-3628 CVE-2017-5708 CVE-2017-5705
Critical CVSS ∈ [9.0-10.0]	1	CVE-2019-0153

Table 3.3: Non-AMT related IME vulnerabilities

CVE	Affected Products	Description
CVE-2022-26845	AMT	Improper authentication in firmware may allow an unauthenticated user to potentially enable escalation of privilege via network access.
CVE-2022-30601	AMT and SM	Insufficiently protected credentials may allow an unauthenticated user to potentially enable information disclosure and escalation of privilege via network access.
CVE-2020-8752	AMT and SM	Out-of-bounds write in IPv6 subsystem may allow an unauthenticated user to potentially enable escalation of privileges via network access.
CVE-2020-8747	AMT	Description Out-of-bounds read in subsystem may allow an unauthenticated user to potentially enable information disclosure and/or denial of service via network access.
CVE-2020-8758	AMT and ISM	Improper buffer restrictions in network subsystem in provisioned Intel AMT and Intel ISM may allow an unauthenticated user to potentially enable escalation of privilege via network access. On un-provisioned systems, an authenticated user may potentially enable escalation of privilege via local access.
CVE-2020-0595	AMT and ISM	Use after free in IPv6 subsystem may allow an unauthenticated user to potentially enable escalation of privilege via network access.
CVE-2020-0594	AMT and ISM	Out-of-bounds read in IPv6 subsystem may allow an unauthenticated user to potentially enable escalation of privilege via network access.
CVE-2019-11131	AMT	Logic issue in subsystem may allow an unauthenticated user to potentially enable escalation of privilege via network access.
CVE-2019-11107	AMT	Insufficient input validation in the subsystem may allow an unauthenticated user to potentially enable escalation of privilege via network access.
CVE-2019-0153	CSME	Buffer overflow in subsystem may allow an unauthenticated user to potentially enable escalation of privilege via network access.
CVE-2017-5689	AMT and ISM	An unprivileged network attacker could gain system privileges to provisioned Intel manageability An unprivileged local attacker could provision manageability features gaining unprivileged network or local system privileges on Intel manageability

Table 3.4: Critical IME vulnerabilities

Regarding AMT, Intel has published procedures for disabling it [Intel, 2021b]. However, as it is a non-free software, it is impossible to verify this claim with absolute certainty.

3.2.4 IME as a deliberate back door

In Section 1.3, it was mentioned that big tech companies are known to deliberately introduce security backdoor. In the case of IME, plenty of organizations and researchers express whether it is really a back door [Gay, 2016] [Erica and Peter, 2017].

Coming from NIST, the definition of a back door is [Stouffer et al., 2023]:

> An undocumented way of gaining access to a computer system.
> A potential security risk.

To the author's view, this is a clear description of IME.

Deliberate backdoor scenarios have been rekindled by a US National Security Agency (NSA) document that called for $250 million a year to introduce backdoors to weaken the security of encryption on devices [The New York Times, 2013].

Chapter 4

Countermeasures

4.1 Is AMD a "Smarter Choice"?

Although AMD[1] has a smaller share of the processor market than Intel [Hachman, 2021], is essentially the only competing processor manufacturer. Unfortunately, the restrictions on freedom that are defined in Section 1.3 continue to apply to AMD processors as well. Since 2013, it carries an IME-like mechanism called AMD Platform Security Processor (PSP) [Williams, 2017] which has similar security and privacy concerns.

4.2 Reducing the attack surface

Introducing unnecessary features into a computing system increases complexity and security risks. According to Mandata and Wing, [2010], the attack surface is defined as:

> the subset of system resources that an attacker can use to attack the system. An attacker can use a system's entry and exit points, channels, and untrusted data elements to send (receive) data to (from) the system to attack the system.

The simplicity of a computing system means fewer exposed parts that a malicious user can exploit [Heydarchi, 2023]. It would therefore be safer from a security point of view, to seek methods to remove IME.

4.3 Free Computing Systems

Although there is no official method from Intel for the removal of IME, independent groups have suggested a procedure that either completely remove or disable parts of IME. The method has to do with the structure and functions of IME and how they have evolved over time.

In models released before 2008, which carried the ancestor of IME (such as the Lenovo ThinkPad X60, X60s, X60 Tablet, T60, etc), IME is disabled by default and can be removed [DG and M, 2018]. Removal is done using

[1] "The smart choice" became AMD's advertising campaign slogan

GNU Boot[2], a free software project that aims to replace non-free boot firmware with free boot software.

On computers built in 2008/09, IME can be disabled by transferring specific values to the SPI flash memory and then removing it entirely, as in previous versions [GNU, 2023a]. For example, this can happen on computers like the Lenovo ThinkPad R400, T400, T400s, T500, W500, X200, X200s, and X200T.

An external flasher like the one in Figure 4.1[3], can be used for the process [Parafestas, 2021].

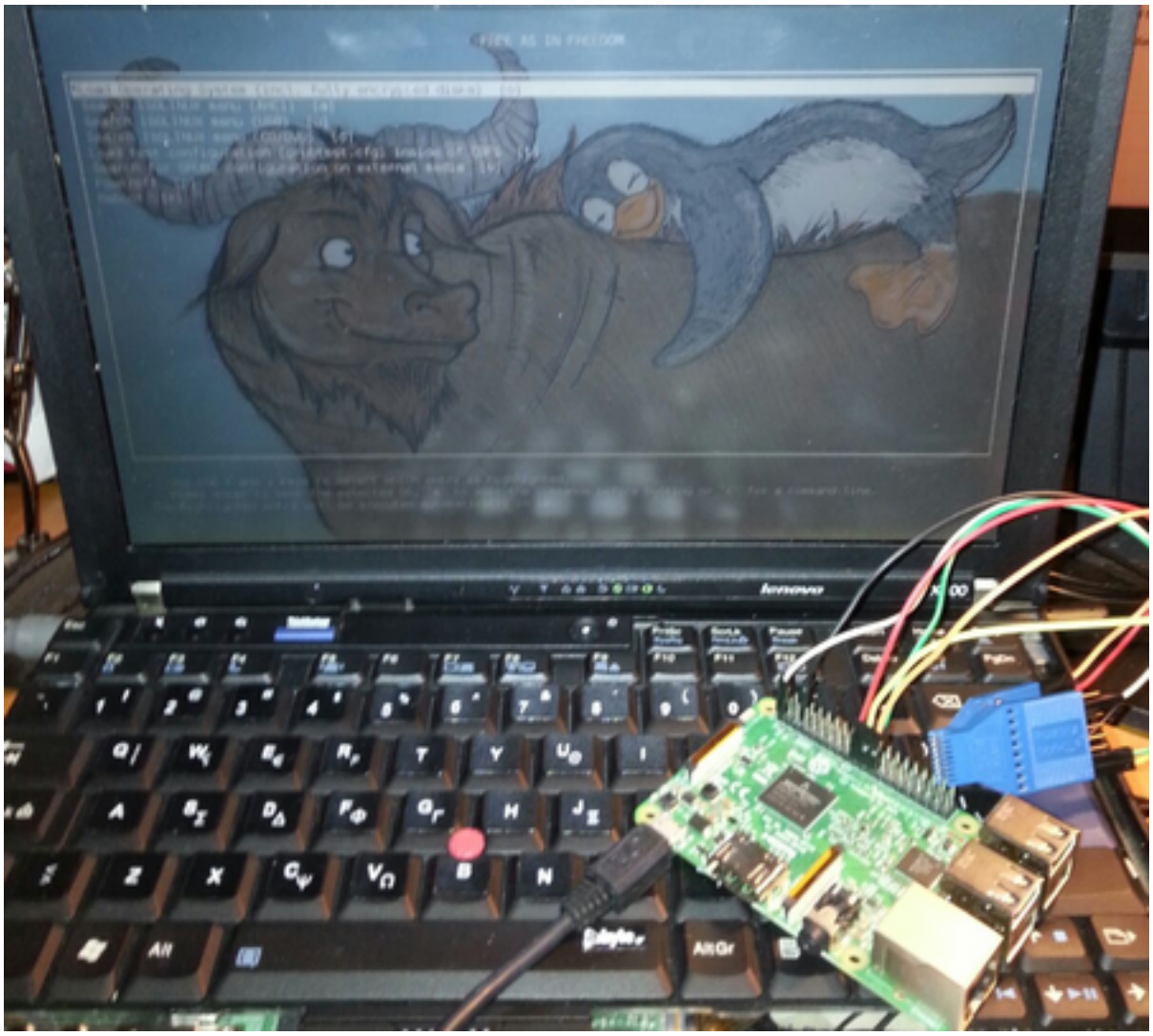

Figure 4.1: IME removal process on Lenovo ThinkPad x200

As already mentioned, from 2009 on, IME gained a more central role in the operation of the system. So, in case it is removed, the computer

[2]GNU Boot is a fork of Libreboot after the latter changed its policy to include non-free firmware

[3]The flasher in the photo is a Raspberry Pi 2. An alternative flasher with both free software and firmware is available at https://www.zerocat.org/chipflasher-board-edition-1.html

shuts down after 30 minutes (see Section 3.2.3). This makes its complete removal practically impossible.

In 2017, a group of researchers introduced me_cleaner, a script that can remove most parts of the IME without affecting the functionality of the computer [Skochinsky and Corna, 2017]. With this method, only a small piece of IME code remains, but its functionality remains unknown.

Without a similar corresponding IME mechanism, computers with OpenPOWER architecture are released by Raptor CS with free firmware [RaptorCS, 2022]. Finally, without significant freedom and privacy concerns low-power systems with ARM architecture are listed by the Free Software Foundation [FSF, 2021].

Chapter 5

Conclusion

As users of technology or researchers of cybersecurity, we need to claim fore more freedom in our technology and communications. At a time when humanity's trust in technology is drying up, free software and free firmware can remove any doubt or suspicion. By eliminating black boxes in computer science, we can reduce the technological alienation created by labyrinthine, complex systems.

The author's personal attitude towards cybersecurity includes a social approach as well. One can protect oneself by protecting others. A real-life analogy by observing the nature is[TBI, 2023]:

> One reason why birds swarm is for safety in numbers. Predators like hawks, falcons, and eagles have a harder time singling out one bird from a large group than they do picking off solitary prey. The more birds that are present, the less likely any s c ingle individual will be attacked.

That is why it is important to protect ourselves while also helping others. This way, we are creating a swarm that protects those who need protection the most, like whistleblowers or activists. Having freedom and trust in technology is crucial in the pursue of social liberation in the modern world.

Bibliography

[BBC, 2020] BBC (2020). NSA surveillance exposed by Snowden ruled unlawful. *BBC News*. https://www.bbc.com/news/technology-54013527.

[Bhunia and Tehranipoor, 2019] Bhunia, S. and Tehranipoor, M. (2019). *Hardware Security*. Morgan Kaufmann.

[Breyer, 2023] Breyer, P. (2023). Chat Control: The EU's CSEM scanner proposal. https://www.patrick-breyer.de/en/posts/chat-control.

[Clark, 2023] Clark, L. (2023). Proposed UK moves to break encryption draw anger of IT world. The Register. https://www.theregister.com/2023/04/18/wrong$_t$*ime*$_t$*o*$_w$*eaken*$_e$*ncryption*/.

[Debian, 2023] Debian (2023). Secureboot. Debian Wiki. https://wiki.debian.org/SecureBoot.

[DG and M, 2018] DG, C. and M, B. (2018). The intel management engine: An attack on computer usersÂÂ freedom. *Free Software Foundation*.

[Dixon, 2021] Dixon, R. (2021). Russiaâs surveillance state still doesn't match China. But Putin is racing to catch up. *Washington Post*. https://www.washingtonpost.com/world/europe/russia-facial-recognition-surveillance-navalny/2021/04/16/4b97dc80-8c0a-11eb-a33e-da28941cb9ac$_s$*tory.html*.

[EMBEDI, 2017] EMBEDI (2017). MythBusters: CVE-2017-5689. Embedi Research Team. https://web.archive.org/web/20180320053922if/*https* : *//embedi.com/news/mythbusters* − *cve* − 2017 − 5689.

[Erica and Peter, 2017] Erica, P. and Peter, E. (2017). Intel's management engine is a security hazard, and users need a way to disable it.

[Felderer et al., 2016] Felderer, M., BÃŒchler, M., Johns, M., Brucker, A. D., Breu, R., and Pretschner, A. (2016). Chapter one - security testing: A survey. In Memon, A., editor, *Advances in Computers*, volume 101 of *Advances in Computers*, pages 1–51. Elsevier.

[FIRST, 2023] FIRST (2023). Common Vulnerability Scoring System SIG. Forum of Incident Response and Security Teams. https://www.first.org/cvss.

[FSF, 2021] FSF (2021). Single-board computers. Online. Free Software Foundation. https://www.fsf.org/resources/hw/single-board-computers.

[Gay, 2011] Gay, J. (2011). Will your computer's "secure boot" turn out to be "restricted boot"? Free Software Foundation. https://www.fsf.org/campaigns/campaigns/secure-boot-vs-restricted-boot.

[Gay, 2016] Gay, J. (2016). Intel & me, and why we should get rid of me. Free Software Foundation. https://www.fsf.org/blogs/licensing/intel-me-and-why-we-should-get-rid-of-me.

[Gehler et al., 2022] Gehler, R., Hasarfaty, S., Moyal, Y., and Siam, Y. (2022). Intel converged security and management engine (intel csme) security.

[GNU, 2023a] GNU (2023a). GNU Boot – Frequently Asked Questions. GNU. https://www.gnu.org/software/gnuboot/web/faq.htmlintelme.

[GNU, 2023b] GNU (2023b). Proprietary back doors. GNU. https://www.gnu.org/proprietary/proprietary-back-doors.en.html.

[GNU, 2023c] GNU (2023c). What is Free Software? GNU. https://www.gnu.org/proprietary/proprietary-back-doors.en.html.

[Hachman, 2021] Hachman, M. (2021). PC CPU market rebounds into 'meh' territory. PCWorld. https://www.pcworld.com/article/2029526/pc-cpu-market-rebounds-into-meh-territory.html.

[Hasarfaty and Moyal, 2019] Hasarfaty, S. and Moyal, Y. (2019). Behind the scenes of intel security and manageability engine.

[Hertzsprung, 2020] Hertzsprung (2020). Privilege rings for the x86 architecture[image]. Online. Wikipedia. https://wikipedia.org/wiki/File:Priv$_r ings.svg$.

[Heydarchi, 2023] Heydarchi, M. H. (2023). The Principle of Least Complexity in Security (KISS).

[Intel, 2017] Intel (2017). INTEL-SA-00075. Intel. https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00075.html.

[Intel, 2021a] Intel (2021a). Getting started with intel active management technology. Intel.https://www.intel.com/content/www/us/en/developer/articles/guide/getting-started-with-active-management-technology.html.

[Intel, 2021b] Intel (2021b). How to deactivate Intel® AMT on an HP Laptop? https://www.intel.com/content/www/us/en/support/articles/000039084/technologies/intel-active-management-technology-intel-amt.html.

[Kerr et al., 2011] Kerr, J., Garrett, M., and Bottomley, J. (2011). Uefi secure boot impact on linux. techreport, RedHat & Canonical.

[Kumar et al., 2009] Kumar, A., Goel, P., Saint-Hilare, Y., and Books24x7, I. (2009). *Active Platform Management Demystified: Unleashing the Power of Intel VPro Technology*. IT Pro. Intel Press.

[Manadhata and Wing, 2010] Manadhata, P. K. and Wing, J. M. (2010). An attack surface metric. *IEEE Transactions on Software Engineering*, 37(3):371–386.

[McCarthy, 2013] McCarthy, T. (2013). Edward Snowden identifies himself as source of NSA leaks - as it happened. *the Guardian*. http://www.theguardian.com/world/2013/jun/09/nsa-secret-surveillance-lawmakers-live.

[McKinney, 2023] McKinney, I. (2023). EFF to Congress: Oppose the EARN IT Act and the STOP CSAM Act. https://www.eff.org/deeplinks/2023/05/eff-letter-congress-oppose-earn-it-act-and-stop-csam-act.

[McLeod, 2023] McLeod, C. (2023). Trust. In Zalta, E. N. and Nodelman, U., editors, *The Stanford Encyclopedia of Philosophy*. Metaphysics Research Lab, Stanford University, Fall 2023 edition. https://plato.stanford.edu/archives/fall2023/entries/trust/.

[Mildebrath, 2022] Mildebrath, H. (2022). Greece's Predatorgate: The latest chapter in Europe's spyware scandal? | Think Tank | European Parliament.

[NIST, 2020] NIST (2020). Roots of trust. National Institute of Standards and Technology. https://csrc.nist.gov/Projects/Hardware-Roots-of-Trust.

[NIST, 2022] NIST (2022). Vulnerabilities. https://nvd.nist.gov/vuln.

[Ogolyuk et al., 2017] Ogolyuk, A., Sheglov, A., and Sheglov, K. (2017). UEFI BIOS and Intel Management Engine Attack Vectors and Vulnerabilities. *PROCEEDING OF THE 20TH CONFERENCE OF FRUCT ASSOCIATION*.

[Pamnani et al., 2023] Pamnani, V., Matarazzo, P., and Duffey, C. (2023). Secure the Windows boot process - Windows Security. Microsoft.

[Parafestas, 2021] Parafestas, N. (2021). Process of removing ime on a lenovo thinkpad x200 using gnuboot [image]. Online. https://totsipaki.net/bepasty/zynYWsh2GnuBootingX200.

[Parafestas, 2023] Parafestas, N. (2023). Privilege rings for the x86 architecture [image]. Online. https://totsipaki.net/bepasty/ce7NQ9CEPrivRingsIntelME.

[RaptorCS, 2022] RaptorCS (2022). OpenPOWER - RCS Wiki. Raptor Computing Systems. https://wiki.raptorcs.com/wiki/OpenPOWER.

[RedHat, 2021] RedHat (2021). What is a CVE? RedHat. https://www.redhat.com/en/topics/security/what-is-cve.

[Ruan, 2014] Ruan, X. (2014). *Platform Embedded Security Technology Revealed: Safeguarding the Future of Computing with Intel Embedded Security and Management Engine*. Expert's voice in computer security. Apress.

[Skochinsky and Corna, 2017] Skochinsky, I. and Corna, N. (2017). Intel me: Myths and reality.

[Smolar, 2023] Smolar, M. (2023). BlackLotus UEFI bootkit: Myth confirmed. ESET. https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/.

[Stallman, 2023a] Stallman, R. (2023a). About the GNU Project. https://www.gnu.org/gnu/thegnuproject.html.

[Stallman, 2023b] Stallman, R. (2023b). Free Hardware and Free Hardware Designs - GNU Project - Free Software Foundation. https://www.gnu.org/philosophy/free-hardware-designs.en.htmltop.

[Stallman, 2023c] Stallman, R. (2023c). How Much Surveillance Can Democracy Withstand? - GNU Project - Free Software Foundation. https://www.gnu.org/philosophy/surveillance-vs-democracy.en.html.

[Stallman, 2023d] Stallman, R. (2023d). Why Open Source Misses the Point of Free Software. https://www.gnu.org/philosophy/open-source-misses-the-point.en.html.

[Stouffer et al., 2023] Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., and Lightman, S. (2023). Guide to operational technology (ot) security. *National Institute of Standards and Technology: Gaithersburg, MD, USA*.

[TBI, 2023] TBI (2023). What Does It Mean When Birds Swarm -. The Bird Identifier. https://www.wwt.org.uk/news-and-stories/blog/marvellous-murmurations-why-do-birds-flock-together/.

[The New York Times, 2013] The New York Times (2013). Documents Reveal N.S.A. Campaign Against Encryption. https://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html.

[Vandewege et al., 2014] Vandewege, W., Garrett, M., and Stallman, R. M. (2014). "active management technology": The obscure remote control in some intel hardware. *FSF*.

[Wiley, 2011] Wiley, J. J. (2011). *ProtectionÂ Rings*, pages 988–990. Springer US, Boston, MA.

[Williams, 2017] Williams, R. (2017). AMD Confirms It Won't Opensource EPYC's Platform Security Processor Code. https://web.archive.org/web/20231027005550if/*https* : *//hothardware.com/news/amd − confirms − it − will − not − be − opensourcing − epycs − platform − security − processor − code*.

[Ylonen, 2018] Ylonen, T. (2018). Intel AMT Vulnerability CVE-2017-5689 in Firmware | SSH.COM. https://web.archive.org/web/20180305001456if/*https* : *//www.ssh.com/vulnerability/intel − amt*.

[Zuboff, 2023] Zuboff, S. (2023). *The age of surveillance capitalism*. Routledge.