Black Box Inside

A study about Trust and Computer Freedom

Parafestas Nikos

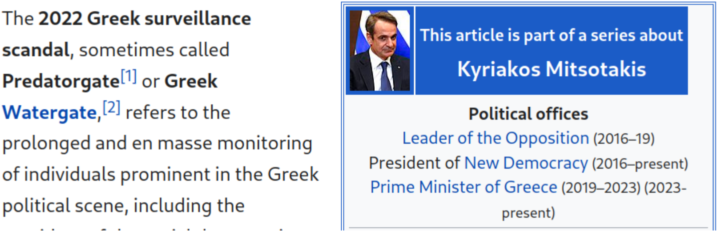
26 January 2024

Section 1: Trust, Surveillance and Freedom in Technology

Technology under Surveillance

Source: https://emailselfdefense.fsf.org/en/infographic.html

Who will protect us from the patrons?[1]



The **2022 Greek surveillance scandal**, sometimes called **Predatorgate**[1] or **Greek Watergate**,[2] refers to the prolonged and en masse monitoring of individuals prominent in the Greek political scene, including the

This article is part of a series about

Kyriakos Mitsotakis

Political offices

Leader of the Opposition (2016–19)

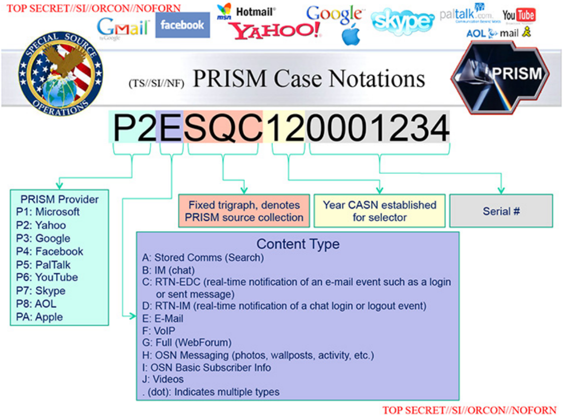
President of New Democracy (2016–present)

Prime Minister of Greece (2019–2023) (2023-present)

Source: https://wikipedia.org/wiki/2022_Greek_surveillance_scandal

[1] Lyrics of Greek labour song “Laos Prostatis” from Thomas Mpakalakos

Surveillance Capitalism



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) PRISM Case Notations

P2ESQC120001234

PRISM Provider
P1: Microsoft
P2: Yahoo
P3: Google
P4: Facebook
P5: PalTalk
P6: YouTube
P7: Skype
P8: AOL
PA: Apple

Fixed trigraph, denotes PRISM source collection

Year CASN established for selector

Serial #

Content Type
A: Stored Comms (Search)
B: IM (chat)
C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
D: RTN-IM (real-time notification of a chat login or logout event)
E: E-Mail
F: VoIP
G: Full (WebForum)
H: OSN Messaging (photos, wallposts, activity, etc.)
I: OSN Basic Subscriber Info
J: Videos
. (dot): Indicates multiple types

TOP SECRET//SI//ORCON//NOFORN

Source: https://wikipedia.org/wiki/Edward_Snowden
Licence: public domain

Trust

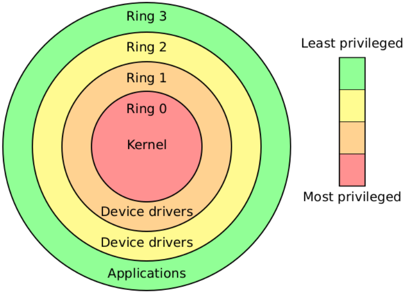
Trust may not be the sort of attitude that one can will oneself to have without any evidence of a person’s trustworthiness.

«Trust». Stanford Encyclopedia of Philosophy Archive

Roots of Trust

> Roots of trust are highly reliable hardware, firmware and software components that perform specific, critical security functions. ... (they) provide a firm foundation from which to build security and trust.
>
> NIST, "Roots of Trust"

Software Layers of Trust



Privilege rings for the x86 architecture

Source: https://wikipedia.org/wiki/File:Priv_rings.svg
Author: Hertzsprung
Licence: GNU Free Documentation License, Version 1.2 or any later | CC BY-SA 3.0 Deed

- 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

Free Software

Source: http://fsfla.org/svnwiki/selibre/linux-libre/index.en.html#artwork
Licence: GNU Free Documentation License, Version 1.2 or any later

Hardware

Source: https://commons.wikimedia.org/wiki/File:Computer_from_inside_018.jpg
Licence: public domain

Firmare

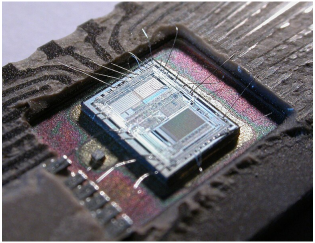
Raimond Spekking / CC BY-SA 4.0 (via Wikimedia Commons)

Let's dive really inside

Down the Rabbit Hole
Source:https://www.flickr.com/photos/valkyrieh116/311526846/
Licence: CC BY-SA 2.0 Deed

Section 2: Intel Management Engine

A computer inside the computer



Source:https://www.flickr.com/photos/biwook/153056995//
Author: Ioan Sameli
Licence: CC BY-SA 2.0 Deed

Intel Management Engine[2] 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

[2] 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.

Accessibility

- Cannot be restricted even by the security measures of the operating system
- Independent of all other layers, which has powerful administration rights to interact with, and control every other component of a computing system.
- Access to the entire RAM and hard drive and it communicates with the main unit to perform special processes
- Ability to turn off the device at any time
- Remote access to both wired and wireless networks by directly accessing the network devices,without interfering with the operating system or other systems
- Ability to lock the operating system if the firmware is modified
- Remotely control the display
- Prevent playback of audiovisual material by applying DRM[3]

[3] Digital Restriction Management

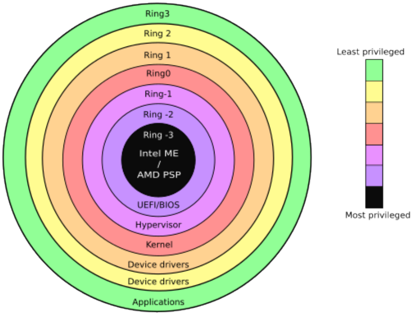
Main IME Modules

- **Intel Active Management Technology (AMT)**
  - Power control
  - BIOS configuration and upgrade
  - Disk clean up
  - System reinstall
  - Console access (VNC)
- **Secure Boot**[4]
  - 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
- **Quiet System Technology**

[4] Also called "restricted boot"

Section 3: Security Overview

Trust levels below 0



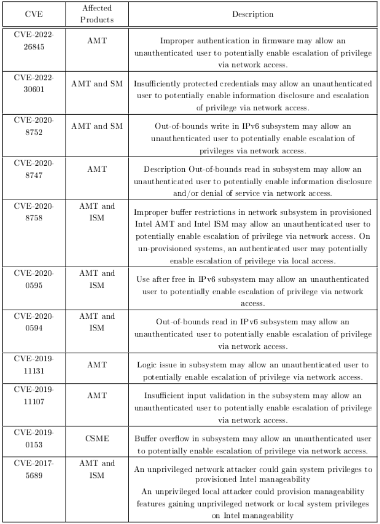
Privilege rings for the x86 architecture with aditional rings

Source: https://libreplanet.org/wiki/File:Priv_rings_ME

Author: Parafestas Nikos

Licence: GNU Free Documentation License, Version 1.2 or any later | CC BY-SA 3.0 Deed

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

IME Critical CVE's (CVSS $\geq$ 7.0)

Silent Bob is Silent (CVE-2017-5689)

- Score of 9.8 on the CVSS V3.1 scale according to NIST
- Affects home computers, laptops and servers since 2010 made by Dell, Fujitsu, HP, Intel, Lenovo and others

Using a few lines of code, 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
- 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.

Silent Bob is Silent (programming error)

The remote user authorization process included a programmer error: it compared the user-given authorization token hash (`user_response`) to the true value of the hash (`computed_response`) using this code:

```
strncmp(computed_response, user_response,
response_length)
```

Silent Bob is Silent (exploit)

```
strncmp(computed_response, user_response,
response_length)
```

- `response_length` was the length of the user-given token and not of the true token.
- if it is less than the length of `computed_response`, only a part of the string will be tested for equality.
- if `user_response` is the empty string (with length 0), this "comparison" will always return true, and thus validate the user.

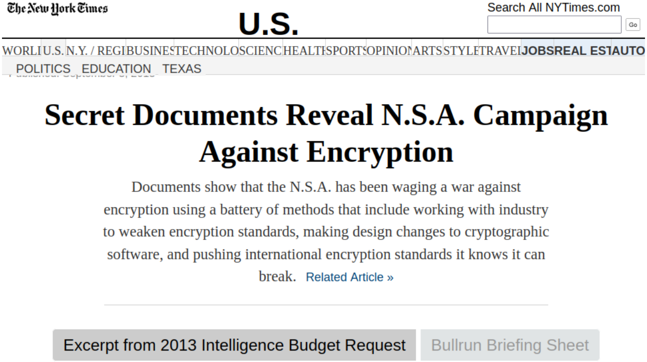
Is IME a deliberate back door?

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

NIST Definition of Back Door[5]

[5] Keith Stouffer, Michael Pease, C Tang, Timothy Zimmerman, Victoria Pillitteri, and Suzanne Lightman, "Guide to operational technology (ot) security", National Institute of Standards and Technology: Gaithersburg, MD, USA (2023).

Back Door by the NSA?


The New York Times
U.S.
Search All NYTimes.com
Go
WORLI U.S. N.Y. / REGI BUSINES TECHNOLO SCIENC HEALTI SPORTS OPINIOI ARTS STYLE TRAVEI JOBS REAL ESI AUTO
POLITICS EDUCATION TEXAS
Related Article »
Excerpt from 2013 Intelligence Budget Request
Bullrun Briefing Sheet

Secret Documents Reveal N.S.A. Campaign Against Encryption

Documents show that the N.S.A. has been waging a war against encryption using a battery of methods that include working with industry to weaken encryption standards, making design changes to cryptographic software, and pushing international encryption standards it knows it can break.

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[6]

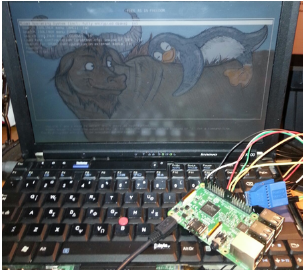
[6] https://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html

Section 4: Countermeasures

Countermeasures Targets

- Reduce the attack surface
- Use code that gives freedom to study
- **Do whaterver we want with our devices**

Liberate a Computer System



IME removal process on Lenovo ThinkPad x200

- In models released before 2008/09, (such as the Lenovo ThinkPad X60, X60s, X60 Tablet, T60, etc), IME is or can be disabled by default so it can be removed (GNU BOOT)
- Models from 2009 on, in case IME is removed, the computer shuts down after 30 minutes. This makes its complete removal practically impossible.
  - There is me_cleaner, a script that can remove most parts of the IME without affecting the functionality of the computer.
  - Only a small piece of IME code remains, but its functionality remains unknown
  - Coreboot (similar to Gnu Boot but with some non-free blobs can be installed)

The end