Security in Windows 10

Research Proposal · April 2019

DOI: 10.13140/RG.2.2.18410.75208

3 authors, including:

Kiran Ramasamy
Carleton University
2 PUBLICATIONS **4** CITATIONS
SEE PROFILE

Vinoth Kumar Baskaran
Carleton University
2 PUBLICATIONS **1** CITATION
SEE PROFILE

Security in Windows 10

Kiran Ramasamy
Department of Systems and Computer Engineering
Carleton University
Ottawa, Canada
kiranramasamy@cmail.carleton.ca

Shubham Thakur
Department of Systems and Computer Engineering
Carleton University
Ottawa, Canada
shubhamthakur@cmail.carleton.ca

Vinoth Kumar Baskaran
Department of Systems and Computer Engineering
Carleton University
Ottawa, Canada
vinothkumarbaskaran@cmail.carleton.ca

***Abstract*—Security of the system does not only depend on the characteristics of security models and design but also on how these security models and designs are being implemented. According to an analytics report, as of September 2018, Windows 10 is running on more than 700 million devices and has an estimated usage share of 45% on traditional PCs. This paper is intended to discuss software security with attention on attacks and defences, and on their formal aspects. It will focus on vulnerabilities and threats to various system resources. It will also emphasize on security challenges and common methods or approaches that Windows 10 uses to secure itself.**

I. Introduction

The software is a set of instructions or programs that instruct the computer to do specific tasks. The software is often divided into System software, Programming software, and Application software. System software generally includes operating systems and any other programs that support application software. An operating system is an important component of the software system which handles the computer hardware and software resources and provides common functionality for computer programs.

Windows 10 is the most recent version of the Microsoft Operating System that was released on July 29, 2015, as a successor to Windows 8. It is probably the most secure version of Windows, ever [1]. Windows 10 is the closest Microsoft has come to a virus-proof operating system so far [1]. When compared to other versions of Windows, Microsoft has included many in-built defence mechanisms in Windows 10 which will ensure the Confidentiality, Integrity, and Availability of the system and these features will be discussed in detail in section VII.

II. Boot Process

Booting a computer refers to the process of powering on the computer and starting the operating system. The boot process loads the operating system into main memory or the random-access memory (RAM) installed on your computer.

A. Windows 10 Boot Process

Windows 10 boots in four stages,

1. Pre-Boot:

- POST (Power-On Self-Test) is initiated and loads firmware settings.
- Checks whether hardware devices are working correctly [2].

2. Windows Boot Manager:

- Finds and starts the Windows Loader on the Windows Boot Partition [2].

3. Windows OS Loader:

- Essential drivers are loaded to start the Windows Kernel [2].

4. Windows NT OS Kernel:

- Registry settings and additional drivers are loaded into the memory.
- Control is passed to the Session Manager Process which loads up the UI and greeted with Login Screen [2].

B. Importance of Protecting the Boot Process

Windows 10 rely heavily on firmware security. If the firmware security is compromised, all the next levels of boot process can be broken. Boot process security should be assured so as to run the device securely [2].

Windows 10 secure the boot process by employing the following countermeasures.

- Secure Boot
- Trusted Boot
- Early Launch Anti-Malware (ELAM)
- Measured Boot

III. Data Storage

There are two types of data storage,

- Primary storage - Random Access Memory.
- Secondary storage - Hard Disk Drive (HDD) or Solid State Drive (SSD).

A. RAM

It is a computing device where the data in current use are kept so they can be quickly reached by the device's processor. RAM is volatile.

B. HDD/SSD

These are the main and largest storage devices. Every file that is put on the computer is stored here; it includes all software and system files and the user files like photos, documents and the files we download [3].

C. Importance of Data Protection

In today's world, Data is recognized as an important asset that needs to be safeguarded. Loss of information can lead to direct financial losses for big corporations and individuals [4]. Importance of data protection increases as the amount of data created and stored is growing at an alarming rate.

IV. CIA Requirements

When talking about Window 10 security, it becomes important to gather security requirements to preserve the confidentiality, integrity, and availability of the system, so that the system will be adequately secure and trustworthy. Also,

the security requirements would help Microsoft to protect the critical assets of the system.

The following security properties should be satisfied for maintaining the CIA of the system.

A. Cryptographic Support

Windows provides cryptographic functions that support encryption/decryption, cryptographic signatures and hashings. It additionally provides support for public keys, credential management and certificate validation.Windows offers access to the cryptographic support functions for user-mode and kernel-mode programs. Public key certificates generated and used by Windows, authenticate users and machines as well as protect both user and system data in transit [24].

B. User Data Protection

Windows 10 take strong measures to help protect customer data from inappropriate access by unauthorized persons, either external or internal, and to prevent customers from gaining access to one another's data. It also provides virtual private networking capabilities and other security mechanisms to ensure the protection of the user data [24].

C. Identification and Authentication

Each Windows user must be identified and authenticated based on administrator-defined policy. Windows maintains databases of accounts including user identities, authentication information, group associations, and privilege and logon rights associations [24].

D. Trusted Path for Communication

Windows 10 uses HTTPS, DTLS and TLS to provide a trusted communication path.

V. Cyber Threats

Windows 10 is the most widely used operating system in the world, which makes it the most common target for cybercriminals to carry out attacks. Most of the attacks take place through the Internet. A cyber-criminal carries out these attacks with the sole intention of making personal gain. Some of the most common types of cyber threats on Windows 10 are discussed below.

A. Malware

Malware is a term that is widely used to describe malicious or untrusted software and applications. It usually causes damage to the system and also obstructs with the normal functioning of computing devices. By infecting a system with malware, cybercriminals can get unauthorized access and use of system resources, steal passwords, lockout a computer, ask for ransom, and many more [5]. They are often motivated by money and will steal confidential information that can be sold or used to extort money from victims.

There are many types of malware available, but we will discuss about the most common ones that had an impact on Windows 10 security in the past. Some of the most common types of malware attacks are Rootkits, Phishing, and Ransomware.

1) Rootkits: Rootkits are a sophisticated and dangerous type of malware that runs in the kernel mode using the same privileges as the operating system [5]. Rootkits can remain in a system undetected for as long as possible. After a rootkit attack, the information that a device reports about itself cannot be trusted. Four types of rootkits are listed below.

a) Firmware Rootkits: They basically overwrite the PC's firmware so that these rootkits can kick start before Windows wakes up.

b) Bootkits: These are an advanced form of rootkits that has the basic functionality of a rootkit along with the ability to infect the Master Boot Record (MBR). Bootkits are designed to not only load from the master boot record but also remain active throughout the working of the system.

c) Kernel Rootkits: By getting access to the Kernel, attacker get the complete control over the operating system. These rootkits replace a portion of the operating system kernel so that these rootkits can start automatically when system loads.

d) Driver Rootkits: As most of the drivers run in the kernel mode and have access to all of the important kernel files. They pretend to be one of the trusted drivers that Windows use to communicate with the PC hardware.

2) Phishing: An attacker who is conducting a phishing attack tries to steal private information via emails, websites, text messages or other forms of electronic communication that often looks to be from legitimate companies or individuals [5]. An attacker then uses the stolen information to conduct activities such as hacking, identity theft, stealing money from the bank account or credit cards, and many more. Some of the most common phishing techniques are listed below.

a) Invoice Phishing: An attacker attempts to lure the users with an email stating that you have an outstanding invoice from a known vendor or company and provides a link for you to access and pay your invoice.

b) Payment/ Delivery Scam: Users are asked to provide a credit card or other personal information so that their payment information can be updated with a commonly known vendor or supplier.

c) Tax Phishing: A common IRS phishing scams is one in which an urgent email letter is sent indicating that you owe money to the IRS.

d) Downloads: Another frequently-used phishing scam is one in which an attacker sends a fraudulent email requesting the user to open or download a document, often one requiring them to sign in.

3) Ransomware: Ransomware is a type of malware that encrypts files and folders, thus preventing access to important files [5]. It aims to extort money from victims, usually in the form of cryptocurrencies, in exchange for the decryption key. Ransomware is known for increasingly sophisticated malware behaviour, highlighted by the use of exploits and other attack vectors which makes older platforms especially vulnerable to ransomware attacks.

Most of the Ransomware infections start with either email messages with attached files that attempt to install ransomware or by websites that try to exploit vulnerabilities in web browsers and other software to install ransomware. Once a device is infected with ransomware, its data will be

encrypted automatically using encryption algorithms likes RSA or RC4. Some of the popular ransomware are Spora, WannaCry, and Petya.

B. *Countermeasures to Cyber Threats*

Below listed are countermeasures provided by Windows 10 to avoid above discussed cyber threats [5].

1) UEFI Secure Boot: It checks the integrity of every component of the start-up process before loading the operating system. Computers with UEFI firmware and a Trusted Platform Module (TPM) can be configured to load only trusted operating system bootloaders.

2) Microsoft Exchange Online Protection: It uses various layers of filtering and provides different controls for spam filtering, such as bulk mail controls and international spam [5]. It helps to protect the email, files, and online storage against malware.

3) Controlled Folder Access: It stops ransomware from encrypting files and holding the files for ransom by giving only limited access to files and folders.

4) Awareness.

5) Apply the latest updates to the operating system.

VI. Recent Vulnerabilities

Like any other operating system, Windows 10 has been subjected to many vulnerabilities in the past. Right after its launch it became the most popular choice to conduct attacks among cybercriminals.

Figure 1 [6] shows number of vulnerabilities encountered by Windows 10 each year from 2015 to 2019. Figure 2 [6] denotes number of times a particular type of vulnerability that has happened in the past.

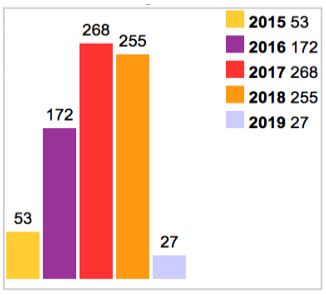

Figure 1. Vulnerabilities by Year

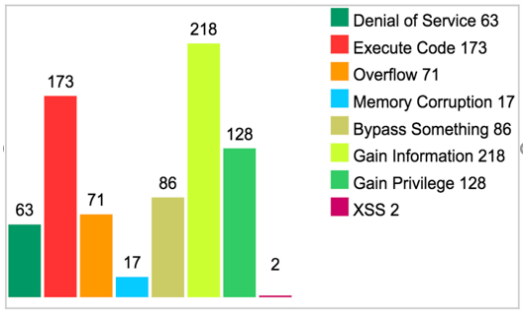

Figure 2. Vulnerabilities by Type

Below is the list of some of the recent vulnerabilities that Windows 10 has encountered in the past.

A. *Remote Code Eecution*

This vulnerability is the most recent one which came into attention in January 2019. By exploiting this vulnerability, an attacker can get access to someone else's computing device and make changes, no matter where the device is geographically located. This vulnerability existed due to improper input validation by Microsoft .NET framework [6].

CVSS Impact - 9.3 (Very High)	Integrity Impact - Complete
Confidentiality Impact - Complete	Availability Impact - Complete

Table 1. Remote Code Execution Impact [6]

B. *Elevation of Privilege*

This vulnerability existed when Windows improperly handles authentication requests. This vulnerability may occur when the Windows kernel fails to properly handle objects in memory [6]. An attacker who successfully exploited the vulnerability could run arbitrary code in the kernel mode. By exploiting this vulnerability an attacker can install programs; view, change, or delete data; or create new accounts with full user rights. This vulnerability happened in December 2018.

CVSS Impact - 7.2 (Medium)	Integrity Impact - Partial
Confidentiality Impact - Partial	Availability Impact - Partial

Table 2. Elevation of Privilege Impact [6]

C. *Information Disclosure*

It happened in December 2018 due to the improper memory operations that are performed by the affected software, some of the memory contents were disclosed. To exploit the vulnerability an attacker would have to trick a user into browsing to a malicious website [7]. By exploiting this vulnerability an attacker could attempt a brute-force attack to disclose user password.

CVSS Impact - 4.3 (Low)	Integrity Impact - None
Confidentiality Impact - Partial	Availability Impact - None

Table 3. Information Disclosure Impact [6]

D. *Coold Boot Attack*

Cold boot attack occurs when an attacker forces a computer to reboot and then steals any data left over in the RAM [7]. A cold boot attack requires physical access to the computer and special hardware tools to perform. It is a serious threat for the individuals who store highly-sensitive information in their pc, or for high-value individuals such as government officials or businessmen. New cold boot attacks unlock disk encryption in almost all modern PCs [7].

E. *Countermeasure to Recent Vulnerabilities*

Microsoft addressed the above mentioned vulnerabilities in Windows 10 by providing the following countermeasures [7].

1) Windows uses User Access Control (UAC) [5] to provide automatic, granular control of privileges. It

temporarily restricts privileges and prompts the active user every time an application attempts to make potentially consequential changes to the system.

2) Microsoft provides regular security updates and patches which addresses most of the vulnerabilities that are listed in the system.

3) To identify any unknown vulnerability, administrators may use the Microsoft Baseline Security Analyser (MBSA) scan tool to identify common security misconfigurations and missing security updates on system endpoints.

VII. Security Features In Windows 10

A. *Virtualization-based Security (VBS)*

Virtualization-based security, or VBS, uses hardware virtualization features to create and isolate a secure region of memory from the normal operating system [8]. Windows use this "secure mode" to employ various security solutions, giving the system increased protection from vulnerabilities. Therefore, it prevents the use of malicious software which attempts to defeat protection mechanisms.

VBS uses the Windows hypervisor to create this virtual secure mode and to enforce restrictions which protect the vital system and operating system resources or to protect security assets such as authenticated user credentials [8]. Even if malware obtains access to operating system kernel, the VBS can greatly contain and limit the possible exploits, because the hypervisor can prevent the malware from executing code or accessing platform secrets.

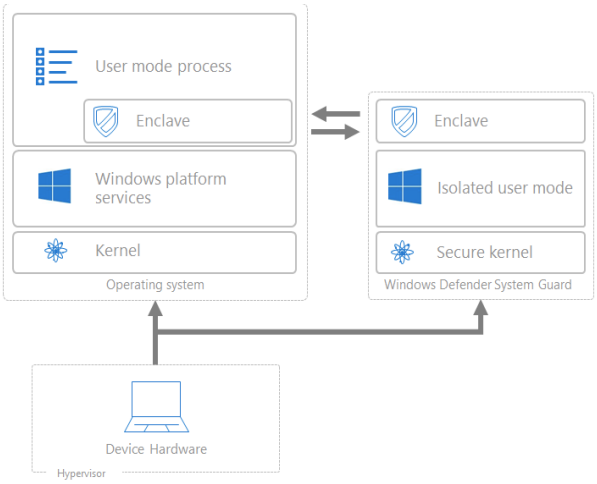

Figure 3. Virtualization Based Security Mechanism

B. *UEFI Secure Boot*

A PC starts by finding the operating system bootloader and loading it to the memory. Without Secure Boot, PCs will simply run whatever bootloader is stored in the computer without even verifying it. It is very difficult to ensure that bootloader is from a trusted party and not a rootkit.

Whereas as the computer UEFI firmware and TPM (Trusted Platform Module) first verifies that the firmware is digitally signed, hence reduces the risk of firmware rootkits. If the Secure Boot is enabled, the firmware examines the digital signature of the bootloader to make sure that the bootloader files have not been compromised. The firmware will then start the bootloader only if one of the below-mentioned conditions are true:

- The bootloader was signed using a trusted certificate (Microsoft® certificate signed) [9].
- The user has manually approved the bootloader's digital signature which will allow the user to load non-Microsoft operating systems [9].

After secure boot comes the trusted boot [9]. Trusted boot checks the integrity of every component of the start-up process which includes boot drives, start-up files, and ELAM before loading it into the memory. If the integrity of even one of the components is compromised, then bootloader refuses to load the corrupted component.

Secure Boot has protected the Bootloader and Trusted Boot has protected the Windows kernel, but an attacker can still infect the system with malware by injecting a non-Microsoft boot driver. This is where ELAM (Early Launch Anti-Malware) comes to play a crucial role by loading a Microsoft or non-Microsoft anti-malware driver before all non-Microsoft boot drivers and applications, therefore continues the trust established by Secure Boot and Trusted Boot.

Measured Boot maintains the logs of boot process which is sent by the Windows to a trusted server that can objectively assess the PC's health [9]. As anti-malware applications do not identify the presence of rootkits, as a result infected PCs appears to be healthy. Measured boot helps to identify those hidden rootkits in the system.

C. *Device Guard*

Device guard is a combination of hardware and software security features which will lock a device down and can only run trusted applications. By using a feature called configurable code integrity device guard provides better security against Advanced Persistent Threats (APT) and unknown malware by blocking all apps that are not considered to be trusted i.e. allowing only the apps that are signed by specific software vendors or from the Windows Store [10].

Device guard uses virtualization-based security and segregates the process that determines whether apps are trusted so that it will make sure that the compromised Windows system is not used to launch the untrusted applications [10]. It will isolate the Microsoft Windows kernel from Code Integrity service so that the Code Integrity service runs alongside the kernel in a Windows hypervisor-protected container.

So, device guard uses Configurable code integrity policies and virtualization-based protection of code integrity and presents a very strong protection capability for Windows 10 devices [11].

D. *Credential Guard*

Windows defender credential Guard allows only privileged system software to access the confidential credentials. It will isolate the credentials from the rest of the operating system by using virtualization-based security [12].

The credential guard is introduced in Windows 10 Enterprise edition. It protects the NT LAN Manager (NTLM) password hashes and Kerberos Ticket granting tickets, so it is more effective to pass the hash attacks [13]. Credential guard

provides protection against trial and error threats such as brute force attacks by storing the randomized full-length hashes.

Credential guard separates the credentials from OS and stores it in protected containers by using Virtualization based security [12]. So even if a malicious attack occurs the files that are protected by credential guard are safe and are not exposed to the attacker.

When users login in Windows 10, the Local Security Authority (LSA) will validate the users. The Credential guard stores the credentials in an isolated LSA which will contain only the certified and virtualization-based security trusted binaries [13]. Before launching a file inside the protected area, the isolated LSA validate each binary by communicating with regular LSA through remote procedure calls.

E. *Windows Defender Advanced Threat Protection (ATP)*

Windows Defender Advanced Threat Protection is a platform designed to help prevent, detect, investigate, and respond to advanced threats [14]. Windows Defender ATP protects endpoints from cyber threats, detects advanced attacks and data breaches. It also automates reporting of security incidents. Advanced Threat Protection uses following methods:

1) Attack Surface Reduction: This is the first line of defence in the stack. By making sure that configuration settings are proper and exploit mitigation techniques are there, these set of techniques resist potential attacks and exploitations [14].

2) Next Generation Protection: Windows Defender ATP uses next generation protection which is particularly designed to catch emerging threats [14].

3) Endpoint Detection and Response: This capability is put in place to detect, investigate, and respond to advanced threats that may have breached the first two security mechanisms [14].

4) Automatic Investigation and Remidiation: In addition to respond to advanced threats, Advanced Threat Protection also provides automatic investigation and remediation capabilities which will help reduce the volume of attacks [14].

5) Secure Score: Windows Defender ATP makes use of secure score to help the user dynamically assess the security state of the network, identify unprotected systems, and take appropriate actions to improve the overall security of the system [14].

6) Microsoft Threat Experts: This service provides proactive hunting, prioritization, and additional context and insights that helps to identify and respond to threats quickly and accurately [14].

VIII. Security Challenges

Windows 10 faces numerous security challenges when deployed in different environments. It may include technical challenges as well as non-technical challenges.

A. *Psychological Challenges*

Security engineers must understand human behavior. Humans have limitations in mental capacity and also error-prone.

Traditional passwords are unsafe as they are hard to remember, and therefore people either choose easy-to-guess passwords or write down their passwords. Also, people use the same password for all applications which is not advisable.

To address this challenge Windows 10 came up with a new feature, Windows Hello.

Windows Hello is a biometrics-based technology that enables Windows 10 users to authenticate secure access to their devices with just a fingerprint or facial recognition. Windows hello Facial recognition works by bouncing infrared (IR) light off our face and picking it up with a camera. With this feature, we can log in into the windows device three times faster than the traditional password and it allows us to keep pin as a backup.

B. *Usability Challenge*

Usability is one of the most important and hardest problems in many secure systems. When an OS with all security features is implemented in an environment, many of its features will not be used by all the users. An unused security feature becomes a useless one. Windows addressed this challenge by providing 4 different editions with varying security features in each edition. Proper incentives are essential for ensuring that users will abide by security policies. The table shows the different editions of windows and their respective security features.

Features	Home	Pro	Enterprise	Education
Microsoft Passport	✓	✓	✓	✓
Enterprise Data Protection		✓	✓	✓
Credential Guard			✓	✓
Device Guard			✓	✓
Device Encryption	✓	✓	✓	✓
BitLocker		✓	✓	✓

Table 4. Windows 10 Editions

C. *Privacy Challenge*

Windows 10 gathers some performance, diagnostic and usage information such as location, installed apps, peripherals, performance data, and web browsing and online searches. But most of the users are not comfortable with their private information being used by Windows. Microsoft states that Windows uses this information to enhance the user experience and to identify problems and fix them [15].

In order to address this challenge, Windows 10 came up with better control in data collection level. It allows the users to switch between basic and full levels of data collection i.e. if the users don't want windows to gather their personal data, they can actually turn off the information gathering in the Privacy settings.

IX. Compliance

Windows 10 needs to conform to certain rules, such as specification, policy, standard or law so as to provide assurance to the users. It complies to privacy laws such as GDPR, HIPAA, and PIPEDA which will be discussed below.

A. *GDPR (General data Protection Regulation)*

General Data Protection Regulation requires businesses to protect the personal data and privacy of EU citizens. GDPR also regulates the transport of data outside the EU.

1) Need for GDPR Compliance: RSA surveyed about 8,000 consumers in European and American countries for their Data Privacy & Security Report. The report stated that 75% of the consumers had a major security concern as they lost their banking and financial data.

It also states that in the event of the breach the consumers would blame the providers for their loss of data, not the attacker. The report concluded that consumers expect more responsiveness and transparency from the steward of their data [16].

A company will be fined €20 million or up to 4% of their global turnover if a company fails to comply with GDPR, for example by losing customer data or failing to make personal data available to the consumers.

2) Types of Data that GDPR Protect:

- Identity information such as name, address and ID numbers.
- Web data such as location, IP address, cookie data and RFID tags.
- Health and Genetic Data.
- Biometric Data.
- Racial or Ethnic Data.
- Political opinions
- Sexual orientation [17].

3) How Windows 10 Complies with GDPR: For clarifying and enabling individual privacy rights Microsoft has taken an important step forward for complying to GDPR. It also believes that privacy is a fundamental right of each individual [18].

a) Threat Protection:

- Pre-breach threat resistance - The malware and hacking industry gets disrupted by moving the playing field to one where they lose the attack vectors that they rely upon.
- Post-breach detection and response - Respond to advanced threats and data breaches by detecting and investigating them.

b) Identity Protection: This advanced technology protects user identities from abuse.

c) Information protection: In order to meet compliance requirements and maintaining user productivity windows 10 provides comprehensive data protection [19].

B. HIPAA

The HIPAA (Health Insurance Portability and accountability Act) Privacy Rule is to protect medical records and other personal health information of everyone.

1) Need for HIPAA Compliance: According to HIPAA, if you are belonging to the category of "covered entities" or "business associates," and you handle "protected health information (PHI)," you and your business are required to be HIPAA-compliant. A company may be fined ranging from $100 to $50,000 if they fail to comply with HIPAA [20]**.**

2) Windows 10 Compliance with HIPAA: Microsoft becomes responsible and enters into contracts to make sure that the business associates will adequately protect PHI if they provide services to covered entities [21].

Microsoft Windows 10 Enterprise users have a privilege to decide whether their Personally Identifiable Information should be shared with IOT or not. Cybersecurity, privacy, and compliance can break or make an organization in Healthcare and Life Sciences industry. By recognizing this Microsoft have designed the Enterprise edition to be flexible, secure and to meet regulatory compliance mandates [22].

Microsoft partnered with HIPAA One (HIPAA software market-leader) to develop a detailed recommendation on configuring Windows 10 such that it will comply with HIPAA and maintain the security of Protected Health Information (PHI) [22].

Windows 10 Enterprise edition in compliance with HIPAA not only assists healthcare entities but also introduces many security capabilities to protect the sensitive data against malware, viruses and cyber-attacks.

C. PIPEDA

The Personal Information Protection and Electronic Documents Act (PIPEDA) administer how the private organizations` are collecting, using and disclosing the personal information in the name of the business and commercial purpose. It is made by Canadian law relating to data privacy.

1) PIPEDA-Windows 10 Controversy: On July 2015 a complaint was filed to the commissioner of Canada stating that when the computer OS is updated to Windows 10, several privacy settings are set to on by default. The investigation was first focussed on Windows Version 1507 as it was the available version at the time of the complaint.

During the investigation, Microsoft released two new versions of Windows 10: The Anniversary Update (1607) and shortly thereafter, the Creators Update (1703) [23].

A preliminary report identified certain contraventions accompanied by some recommendations has been released to Microsoft to bring Microsoft into compliance with the PIPEDA [23].

In response to the issuance of the preliminary report, Windows 10 (Version 1803) update was released, which addressed certain concerns. To resolve the remaining concerns Microsoft assured to implement more measures [23].

X. SECURITY EVALUATION AND ASSURANCE

Microsoft supports the Common Criteria certification program to optimizing the security of its products and services. It continuously ensures that the features and functions required by Common Criteria protection profiles are incorporated into its products. The following standards and documents have been used for the evaluation of Windows 10.

- [CC] Common Criteria for Information Technology Security Evaluation, Version 3.1 [24].
- [GPOSPP] General Purpose Operating Systems Protection Profile, Version 4.1 [26].
- [CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1

A. Security Objectives

The security objectives for Windows which are needed to comply with the GP OS PP are [24],

1) Accountability: Windows 10 ensures that the existing information allows administrators to discover unintentional issues with the configuration and operation of the OS and discover its cause.

2) Integrity: Windows 10 ensures the integrity of their update packages. It provides execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems.

3) Management: Windows 10 facilitates management by users and the enterprise by providing consistent and supported interfaces for their security relevant configuration and maintenance.

4) Protected storage: Windows 10 address the issue of loss of confidentiality of credentials in the event of loss of physical control of the storage medium. It provides protection for data at rest. It also provides access controls which allow users to keep their files private from other users of the same system.

5) Protected Communication: Windows 10 address both passive (eavesdropping) and active (packet modification) network attack threats and provide mechanisms to create trusted channels for sensitive data.

B. TOE Security Functional Requirements

The security functional requirements of windows 10 are [24],

1) Security Audit: Windows 10 has the ability to collect audit data, review audit logs, protect audit logs from overflow, and restrict access to audit logs.

2) Protection of Windows security functions: Windows protects against unauthorized data disclosure and modification by using a suite of Internet standard protocols like IPsec. Windows includes self-testing features that ensure the integrity of executable program images and its cryptographic functions.

3) User Data Protection: Protects user data and provides virtual private networking capabilities.

4) Identification and Authentication: Each Windows user must be identified and authenticated based on administrator-defined policy prior to performing any TOE Security mediated functions.

5) Session Locking: Windows provides the ability for a user to lock their session either immediately or after a defined interval.

6) TOE Access: Windows allows an authorized administrator to configure the system to display a logon banner before the logon dialog.

7) Security Management: Windows includes several functions to manage security policies. Policy management is controlled through a combination of access control, membership in administrator groups, and privileges.

C. TOE Security Assurance Requirements

Commercial operating systems that provide conventional, user-based security features are typically evaluated at EAL 4. EAL 4 reasonably assures users that their operating systems, together with firewalls and other security measures, will protect them from standard attacks [25].

It is being clearly stated that Microsoft windows 7 has EAL 4 (Methodically Designed, Tested and Reviewed) and so we assume that Microsoft Windows 10 also has EAL 4 or EAL 4+ [26].

D. Testing Results

1) Product Testing: The independent testing of TOE has covered 100% of SFRs of the security target and assurance activities defined in the [GPOSPP] for each SFR. There has not been any deviation from the expected results under the environment defined in the security target [27].

2) Penetration Testing: The lab has checked that all the public vulnerabilities previously published have been fixed as the TOE has been configured with all critical updates until July 30, 2018 [27].

E. Evaluation Results

The TOE has been evaluated and it has been found that all the assurance components defined in the [GPOSPP] have been assigned a "PASS" verdict. Consequently, the laboratory Epoche & Espri S.L.U. assigns the "PASS" VERDICT to the whole evaluation due all the evaluator actions are satisfied for the assurance packages defined in the [GPOSPP] as defined by the Common Criteria v3.1 [27].

XI. Open Research Problems

A. Microsoft AccountGuard

Microsoft Account Guard is a new security service offered at no additional cost to customers in the political space. The service is designed to protect highly targeted customers from cybersecurity threats [29]. Microsoft Account Guard features are given below.

1) Unified threat detection and notification across accounts: Microsoft AccountGuard will provide notification in a unified way about cyber threats across both email and the personal accounts of these organization's leaders and staff who opt-in.

2) Security guidance and ongoing education: Organizations registered r for Microsoft AccountGuard will be given the best practice guidance and materials to address the unique problems faced by politically oriented organizations.

3) Early adopter opportunities: Organizations registered for Microsoft AccountGuard will be first to deploy the latest technology and will receive access to private previews of security features offered to the government account customers.

There were hacking and disinformation attacks on the French presidential election in 2017. So, it is being stated that Microsoft Account Guard is recently expanded to twelve new markets across Europe to eligible organizations [30]. Also now it is helping to secure the 2020 US General elections and broader political & think tank community.

B. Microsoft Threat Protection

Microsoft threat protection brings together the unparalleled intelligence, comprehensive identity protection and automation into one solution to secure the modern

organization [31]. They enhance and develop capabilities to provide more security to the customers by Combining artificial intelligence with human expertise for unparalleled security.

Human expertise will always be pivotal for strong security. To benefit from the knowledge of seasoned security analysts, Microsoft Threat Experts was announced to augment customers Security Operation Centers (SOCs). Microsoft Threat Experts blends the benefits of human analysts with the industry's leading endpoint security service. It helps SOCs to identify and respond to threats quickly and accurately by providing context-rich intelligence [31]. It offers features such as,

1) Targeted attack notifications: Provides notifications to customers in case a breach is identified and offers to monitor by Microsoft's threat experts.

2) Experts on demand: Security experts provide technical consultation on relevant detections and adversaries.

C. Bitlocker Encryption in SSD

Recent research [32] spotted vulnerabilities in the embedded encryption of many SSD models that they are S failing to cryptographically tie the owner's password to the actual data encryption key that allowed them to access the data without a password. Though we enable Bitlocker encryption on our system Windows 10 Bit locker defaults to SSD encryption, when available.

Switching from software encryption to hardware encryption has some complex steps [33] to be followed. Drive need to be unencrypted first and then re-encrypted using software encryption. And then default encryption settings should be changed to software encryption. This will not solve the problem as it does not re-encrypt the existing data. Only after reformatting the drive and making a new installation will enforce the software encryption.

Microsoft should work with the companies that sell SSDs so that they can come up with a unified solution to this problem.

XII. REFERENCES

[1] Aryeh Goretsky, "Microsoft Windows Security and Privacy," an ESET White Paper. Published January.01,2017.

[2] Microsoft, "Advanced troubleshooting for Windows boot problems", November.15,2018 [Online]. Available:https://docs.microsoft.com/en-us/windows/client-management/advanced-troubleshooting-boot problems.

[3] Powerscribe solution, "What is HDD and Why it's Important" Published November 2015 [Online]. Available: https://www.powerscribe.com/hdd-and-importance.

[4] Whitson Gordon, "What is HDD and Why it's Important" Published May 4, 2018 [Online]. Available: https://www.popsci.com/store-share-sensitive-files.

[5] Microsoft, "Understanding malware & other threats" Published February 2019 [Online]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/understanding-malware

[6] CVE Details, "Microsoft Windows 10 : List of security vulnerabilities - CVE Details" [Online]. Available: https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-32238/Microsoft-Windows-10.html

[7] NIST, "NATIONAL VULNERABILITY DATABASE" Published January 2019 [Online]. Available: https://nvd.nist.gov/vuln/detail/CVE-2019-0582

[8] Microsoft, "Virtualization-based Security (VBS)",April 10, 2017[ONLINE]. Available: https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs

[9] Microsoft, "Secure boot" Published October 2017 [Online]. Available: https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-secure-boot

[10] Microsoft, "Device Guard: Windows Defender Application Control and virtualization-based protection of code integrity" Published June 6 2018[Online]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/device-guard/introduction-to-device-guard-virtualization-based-security-and-windows-defender-application-control

[11] Russell Smith, "What is Windows 10 Device Guard?" Published April 2015 [Online]. Available: https://www.petri.com/what-is-windows-10-device-guard

[12] Microsoft, "Protect derived domain credentials with Windows Defender Credential Guard" Published August 2017 [Online]. Available:https://docs.microsoft.com/enus/windows/security/identity-protection/credential-guard/credential-guard

[13] Margaret Rouse, "Microsoft Windows Defender Credential Guard" Published January 2018 [Online]. Available: https://searchenterprisedesktop.techtarget.com/definition/Microsoft-Windows-Defender-Credential-Guard

[14] Microsoft, "Windows Defender Advanced Threat Protection" Published March 2019 [Online]. Available: https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-atp/windows-defender-advanced-threat-protection

[15] Satya Nadella, "Privacy at Microsoft" Published November 6 2018 [Online]. Available: https://privacy.microsoft.com/en-GB/

[16] RSA, "RSA data privacy and security report" [Online]. Available: https://www.rsa.com/content/dam/en/e-book/rsa-data-privacy-report.pdf

[17] Michael Nadeau, "General Data Protection Regulation (GDPR): What you need to know to stay compliant", April.23, 2018 [Online]. Available: https://www.csoonline.com/article/3202771/general-data-protection-regulation-gdpr-requirements-deadlines-and-facts.html

[18] Microsoft, "Windows and the GDPR: Information for IT Administrators and Decision Makers", October.05,2018 [Online]. Available: https://docs.microsoft.com/en-us/windows/privacy/gdpr-it-guidance

[19] Marisa Rogers, "Windows resources to help support your GDPR compliance", September.5, 2017 [Online]. Available: https://blogs.windows.com/windowsexperience/2017/09/25/windows-resources-to-help-support-your-gdpr-compliance/#17Jy0ZeZXv4dH6Gl.97

[20] Forbes, "Does Your Business Need to Be HIPAA-Compliant?", February.6,2014 [Online]. Available: https://www.forbes.com/sites/thesba/2014/02/06/does-your-business-need-to-be-hipaa-compliant/#5e34c2873d7c

[21] Microsoft, "Microsoft and HIPAA and the HITECH Act", [Online]. Available:https://www.microsoft.com/enus/trustcenter/compliance/hipaa

[22] Connor Flanagan, "HIPAA Compliance with Microsoft Windows 10 Enterprise", December.21,2017 [Online]. Available: https://cloudblogs.microsoft.com/industry-blog/health/2017/12/21/hipaa-compliance-with-microsoft-windows-10-enterprise/

[23] Office of Privacy Commissioner of Canada, "Microsoft to obtain opt-in consent, enhance transparency for Windows 10 privacy settings", June.20,2018 [Online]. Available: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into businesses/2018/pipeda-2018-004/

[24] Common Criteria, "Security Target-Microsoft Windows Common Criteria Evaluation" Published April 2018 [Online]. Available:https://www.commoncriteriaportal.org/files/epfiles/2018-25-ST_lite.pdf

[25] NIST, "Network information security and technology news", December.14, 2005 [Online]. Available: https://www.nist.org/news.php?extend.37

[26] Wikipedia, "Evaluation Assurance level", [Online]. Available: https://en.wikipedia.org/wiki/Evaluation_Assurance_Level

[27] Common Criteria, "CERTIFICATION REPORT" Published April 2018 [Online]. Available:

https://www.commoncriteriaportal.org/files/epfiles/2018-25-INF-2642.pdf

[28] National Information Assurance Partnership, “Protection Profile for General Purpose Operating Systems” Published March 2016 [Online]. Available: https://www.commoncriteriaportal.org/files/ppfiles/pp_os_v4.1.pdf

[29] Tom Burt, “Protecting democracy with Microsoft AccountGuard” Published Aug 20. 2018 [Online]. Available: https://blogs.microsoft.com/on-the-issues/2018/08/20/protecting-democracy-with-microsoft-accountguard/

[30] Tom Burt, “Intent New steps to protect Europe from continued cyber threats” Published February 20 .2019 [Online]. Available: https://blogs.microsoft.com/eupolicy/2019/02/20/accountguard-expands-to-europe/

[31] Debraj Ghosh, “Intent The evolution of Microsoft Threat Protection, RSA edition part 1” Published March 14, 2019 [Online]. Availablehttps://www.microsoft.com/security/blog/2019/03/14/evolution-microsoft-threat-protection-rsa-edition-1/

[32] Carlo Meijer, Bernard van Gastel “ Self-encrypting deception: weaknesses in the encryption of solid state drives (SSDs),” Radboud University Published : November 5 2018.

[33] Kurt Mackie, “Microsoft Issues Security Advisory on Solid-State Drive Hardware Encryption” Published November 6 2018 [Online]. Available: https://redmondmag.com/articles/2018/11/06/microsoft-ssd-security-advisory.aspx