NT212 – AN TOÀN DỮ LIỆU VÀ KHÔI PHỤC THÔNG TIN SAU SỰ CỐ

BÁO CÁO BÀI TẬP 2

Data Integrity trong hệ điều hành Microsoft Windows

***

THÔNG TIN CHUNG

1. Thông tin sinh viên

STT	Họ và tên	MSSV	Email
1	Dương Phạm Huy Thông	22521431	22521431@gm.uit.edu.vn

---

2. Nội dung thực hiện

Yêu cầu: Nghiên cứu và trình bày về các cơ chế để đảm bảo Data Integrity đã được thiết lập sẵn trong hệ điều hành Micorsoft Windows. Đánh giá mức độ hiệu quả tương ứng.

Bên dưới đây là toàn bộ bài báo cáo chi tiết đã được nhóm thực hiện.

BÀI LÀM

1. Tổng quan về các cơ chế đảm bảo Data Integrity trên hệ điều hành Windows.

Tính toàn vẹn dữ liệu (Data Integrity) là khả năng đảm bảo rằng dữ liệu không bị thay đổi trái phép, xóa, hoặc hỏng hóc do các tác nhân bên ngoài như phần mềm độc hại, lỗi hệ thống, hoặc truy cập trái phép[1]. Để đảm bảo tính toàn vẹn của dữ liệu, hệ điều hành Windows được thiết kế với nhiều lớp bảo vệ liên kết chặt chẽ từ phần cứng đến phần mềm.

Một ví dụ tiêu biểu cho cơ chế đảm bảo tính toàn vẹn dữ liệu trên hệ điều hành Windows có thể kể đến là **BitLocker**[2], Windows tích hợp các cơ chế bảo mật tiên tiến như mã hóa toàn diện như BitLocker giúp bảo vệ dữ liệu lưu trữ, kiểm soát truy cập thông qua các thiết lập phân quyền và xác thực mạnh mẽ. Ngoài ra, Windows còn cung cấp cơ chế giám sát liên tục nhằm phát hiện và ngăn chặn các hành vi bất thường[3]. Quá trình khởi động an toàn (**Secure Boot**) cũng là một thành phần quan trọng, đảm bảo rằng hệ thống chỉ khởi động các phần mềm đã được xác thực, qua đó loại bỏ nguy cơ từ bootkits và các mã độc tiềm ẩn ngay từ giai đoạn khởi động hệ thống.

Để tìm hiểu chi tiết về các cơ chế đảm bảo tính toàn vẹn dữ liệu trên hệ điều hành Windows, chúng ta cần phân tích các yếu tố ảnh hưởng đến tính toàn vẹn của dữ liệu mà người dùng có thể đối mặt

> ***Phần cứng:*** *Một trong những yếu tố quan trọng là sự hỗ trợ từ các thành phần phần cứng như Module* ***Trusted Platform Module (TPM)*** *và* ***CPU hỗ trợ ảo hóa****. TPM là một bộ vi xử lý chuyên dụng được tích hợp vào nhiều thiết bị hiện đại, có nhiệm vụ lưu trữ và quản lý các khóa mã hóa, qua đó bảo vệ dữ liệu khỏi các truy cập trái phép[4]. Ngoài ra, các tính năng ảo hóa của CPU cho phép Windows triển khai các giải pháp bảo mật dựa trên ảo hóa (****Virtualization-Based Security – VBS****), giúp cô lập các thành phần nhạy cảm của hệ điều hành khỏi các mối đe dọa bên ngoài.*[5]

---

[1] Dansimp. (n.d.). *Windows security - Windows security*. Learn.microsoft.com. https://learn.microsoft.com/en-us/windows/security/

[2] Teresa-Motiv. (n.d.). *BitLocker recovery: known issues - Windows Client*. Learn.microsoft.com. https://learn.microsoft.com/en-us/troubleshoot/windows-client/windows-security/bitlocker-recovery-known-issues

[3] bmansheim. (n.d.). *Track changes to system files and registry keys*. Learn.microsoft.com. https://learn.microsoft.com/en-us/azure/defender-for-cloud/file-integrity-monitoring-overview

[4]vinaypamnani-msft. (2023, July 31). *How Windows uses the TPM - Windows Security*. Learn.microsoft.com. https://learn.microsoft.com/en-us/windows/security/hardware-security/tpm/how-windows-uses-the-tp

[5] windows-driver-content. (2023, March 20). *Virtualization-based Security* (VBS). Learn.microsoft.com. https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-vbs

Phần mềm: *Windows không chỉ dựa vào phần cứng mà còn tích hợp các cơ chế bảo mật ở tầng phần mềm. Cập nhật bảo mật định kỳ và trình điều khiển tương thích đóng vai trò then chốt trong việc giảm thiểu các lỗ hổng bảo mật. Hệ thống cập nhật* ***Windows Update***[6] *thường xuyên cung cấp các bản vá lỗi quan trọng nhằm khắc phục các lỗ hổng được phát hiện, đồng thời cải thiện các tính năng bảo vệ hệ thống.*

Chính sách người dùng: *Một khía cạnh không kém phần quan trọng là việc thiết lập và quản lý các chính sách người dùng phù hợp. Quyền truy cập được quản lý chặt chẽ thông qua các cơ chế như* ***Active Directory*** [7]*và* ***Group Policy*** [8]*giúp đảm bảo rằng chỉ những người dùng có thẩm quyền mới được truy cập vào các tài nguyên nhạy cảm. Bên cạnh đó,* ***xác thực đa yếu tố (MFA)*** [9]*cung cấp một lớp bảo mật bổ sung, giảm thiểu nguy cơ truy cập trái phép ngay cả khi thông tin đăng nhập bị lộ. Những chính sách này không chỉ góp phần ngăn chặn việc thay đổi dữ liệu một cách trái phép mà còn đảm bảo rằng các hành động của người dùng luôn được giám sát và kiểm soát theo chuẩn mực của các quy định bảo mật hiện hành*

Mục tiêu chính của Windows trong việc bảo vệ tính toàn vẹn dữ liệu là ngăn chặn các cuộc tấn công từ mã độc, bảo vệ dữ liệu nhạy cảm khỏi bị truy cập trái phép, cũng như đảm bảo rằng hệ thống khởi động và hoạt động một cách an toàn và đáng tin cậy. Việc tích hợp các biện pháp bảo vệ từ phần cứng đến phần mềm cho phép Windows không chỉ ngăn chặn các mối đe dọa an ninh mà còn hỗ trợ các tổ chức và người dùng tuân thủ các quy định pháp lý quốc tế như GDPR[10] và HIPAA[11]. Nhờ đó, rủi ro mất mát dữ liệu được giảm thiểu đáng kể, đồng thời nâng cao niềm tin của người dùng và doanh nghiệp vào hệ thống của mình. Những lợi ích này không chỉ giúp bảo vệ tài sản số mà còn tạo nền tảng vững chắc cho sự phát triển và đổi mới công nghệ trong môi trường doanh nghiệp.

---

[6] Windows Update: FAQ. (n.d.). Support.microsoft.com. https://support.microsoft.com/en-us/windows/windows-update-faq-8a903416-6f45-0718-f5c7-375e92dddeb2

[7] Microsoft. (2022, August 16). Active directory domain services overview. Microsoft. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

[8] Microsoft. (2022, August 16). Active directory domain services overview. Microsoft. https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

[9] Microsoft. (2023, October 23). Microsoft Entra multifactor authentication overview. Learn.microsoft.com. https://learn.microsoft.com/en-us/entra/identity/authentication/concept-mfa-howitworks

[10] Microsoft. (2023, January 26). *General Data Protection Regulation - Microsoft GDPR*. Learn.microsoft.com. https://learn.microsoft.com/en-us/compliance/regulatory/gdpr

[11] robmazz. (n.d.). *Health Insurance Portability and Accountability Act (HIPAA) & Health Information Technology for Economic and Clinical Health (HITECH) Act - Microsoft Compliance*. Learn.microsoft.com. https://learn.microsoft.com/en-us/compliance/regulatory/offering-hipaa-hitech

2. Các chức năng bảo toàn dữ liệu trên Windows

a. BitLocker Drive Encryption

BitLocker Drive Encryption là một công cụ mã hóa toàn bộ ổ đĩa được tích hợp trong các phiên bản Windows như Windows 10 Pro, Enterprise và Education. Nó giúp bảo vệ dữ liệu bằng cách mã hóa toàn bộ ổ đĩa, ngăn chặn truy cập trái phép ngay cả khi thiết bị bị mất hoặc đánh cắp. BitLocker sử dụng thuật toán mã hóa AES với độ dài khóa lên đến 256-bit để mã hóa dữ liệu trên ổ đĩa. Khi kết hợp với Mô-đun Nền tảng Tin cậy (TPM), BitLocker có thể xác minh tính toàn vẹn của hệ thống trước khi giải mã và khởi động hệ điều hành. Nếu TPM không khả dụng, BitLocker có thể hoạt động dựa trên mật khẩu hoặc khóa khởi động được lưu trữ trên USB.[12]

BitLocker được đánh giá cao trong việc bảo vệ dữ liệu khỏi truy cập trái phép, đặc biệt hữu ích trong môi trường doanh nghiệp và cho người dùng cá nhân có nhu cầu bảo mật cao. Tuy nhiên, hiệu quả của BitLocker phụ thuộc vào việc triển khai đúng cách và quản lý khóa khôi phục một cách an toàn.

Cách thức hoạt động chủ yếu của BitLocker

Thuật Toán Mã Hóa: Sử dụng AES trong chế độ XTS với độ dài khóa 128 hoặc 256 bit, đảm bảo dữ liệu được mã hóa mạnh mẽ.

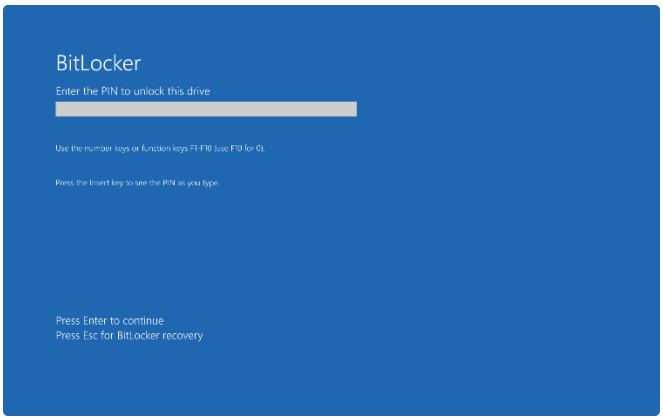
Tích Hợp TPM 2.0: Làm việc với Trusted Platform Module (TPM) để lưu trữ khóa mã hóa an toàn, đảm bảo chỉ thiết bị gốc mới có thể giải mã. TPM kiểm tra tính toàn vẹn hệ thống trước khi khởi động, ngăn chặn truy cập nếu phát hiện thay đổi.

Tùy Chọn Xác Thực: Hỗ trợ xác thực bổ sung như PIN, mật khẩu, hoặc USB key, tăng cường bảo mật khi khởi động.

---

[12] *Khởi chạy BitLocker Drive Encryption*. (2025). Kaspersky.com. https://support.kaspersky.com/keswin/12.7/vi-VN/130689.htm?utm_source=chatgpt.com

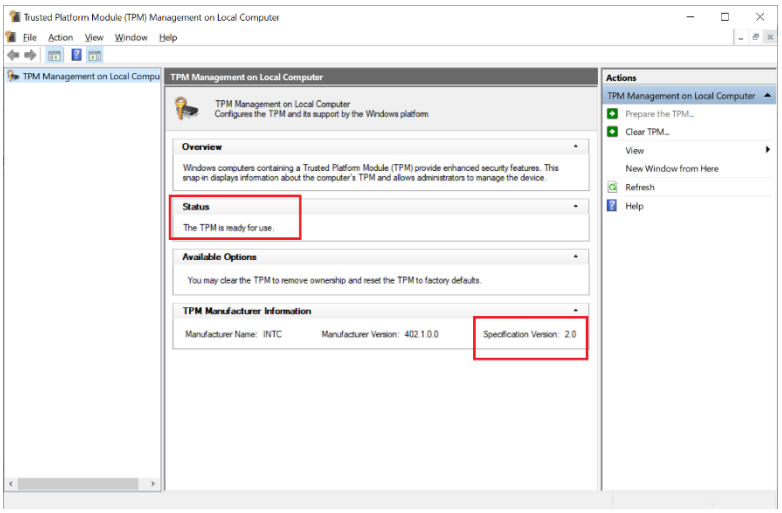
Quy Trình Khởi Động: Đảm bảo rằng chỉ khi hệ thống được xác minh an toàn, dữ liệu mới được giải mã, ngăn chặn các cuộc tấn công phần cứng.



Nghiên cứu từ Microsoft cho thấy BitLocker hiệu quả trong việc bảo vệ dữ liệu, đặc biệt khi kết hợp với TPM. Tuy nhiên, nó có thể bị tấn công lạnh (cold boot attack) hoặc DMA (Direct Memory Access) nếu máy không được tắt hoàn toàn, đòi hỏi người dùng phải cẩn thận trong việc quản lý thiết bị.[13] BitLocker giảm thiểu rủi ro truy cập trái phép, nhưng hiệu quả phụ thuộc vào cách triển khai.

b. Trusted Platform Module (TPM 2.0)

PM 2.0 là một chip bảo mật được tích hợp trên bo mạch chủ của máy tính hoặc trong bộ vi xử lý, cung cấp các chức năng liên quan đến bảo mật ở cấp độ phần cứng. Nó được sử dụng để tạo, lưu trữ và quản lý các khóa mã hóa, chứng chỉ số và thông tin xác thực một cách an toàn.



[13] *Tổng quan về BitLocker - Hỗ trợ của Microsoft*. (2025). Microsoft.com. https://support.microsoft.com/vi-vn/windows/t%E1%BB%95ng-quan-v%E1%BB%81-bitlocker-44c0c61c-989d-4a69-8822-b95cd49b1bbf

Cách thức hoạt động của TPM 2.0[14]:

Lưu Trữ Khóa: Lưu trữ khóa mã hóa và các thông tin nhạy cảm trong môi trường phần cứng an toàn, ngăn chặn truy cập từ phần mềm độc hại.

Quản Lý Khóa: Tích hợp với BitLocker để quản lý khóa, đảm bảo chỉ thiết bị gốc mới có thể giải mã dữ liệu.

Kiểm Tra Khởi Động: Xác minh tính toàn vẹn của quá trình khởi động, đảm bảo không có thay đổi không mong muốn trong firmware hoặc hệ điều hành

TPM 2.0 cung cấp lớp bảo mật mạnh mẽ, đặc biệt khi kết hợp với Secure Boot, ngăn chặn các cuộc tấn công phần cứng như thay đổi firmware. Tuy nhiên, hiệu quả phụ thuộc vào việc triển khai đúng, và không bảo vệ được nếu kẻ tấn công có quyền truy cập vật lý vào thiết bị trong thời gian dài. Trong môi trường doanh nghiệp, chúng được sử dụng để xác thực thiết bị, bảo vệ thông tin nhạy cảm như dữ liệu khách hàng với ưu điểm tăng cường bảo mật phần cứng. Tuy nhiên chúng lại yêu cầu phần cứng mới, chi phí triển khai cao.

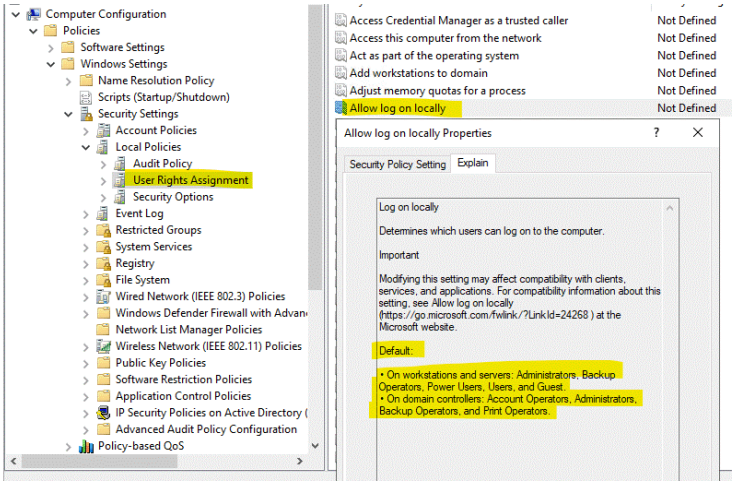
c. Hypervisor-Protected Code Integrity (HVCI)

Memory Integrity hay **Hypervisor-Protected Code Integrity (HVCI)** là một tính năng của **Virtualization-Based Security (VBS)** có trong Windows 10, Windows 11 và Windows Server 2016 trở lên[15]. Tính năng này sử dụng hypervisor của Windows để tạo một môi trường ảo hóa cô lập, đóng vai trò như gốc tin cậy cho hệ điều hành, giả định rằng kernel có thể bị xâm phạm. Memory integrity bảo vệ và củng cố Windows bằng cách chạy kiểm tra tính toàn vẹn của mã ở chế độ kernel trong môi trường ảo hóa cô lập này. Nó cũng hạn chế các phân bổ bộ nhớ kernel có thể được sử dụng để xâm phạm hệ thống, đảm bảo rằng các trang bộ nhớ kernel chỉ được thực thi sau khi vượt qua kiểm tra tính toàn vẹn của mã bên trong môi trường chạy an toàn, và các trang thực thi không bao giờ có thể ghi được.

---

[14] windows-driver-content. (n.d.). *Trusted Plaform Module (TPM) 2.0*. Learn.microsoft.com. https://learn.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-tpm

[15] barrygolden. (2024, December 18). *Hypervisor-Protected Code Integrity (HVCI) - Windows drivers*. Microsoft.com. https://learn.microsoft.com/en-us/windows-hardware/drivers/bringup/device-guard-and-credential-guard



Về mức độ hiệu quả, HVCI giúp cải thiện mô hình bảo mật của Windows và cung cấp sự bảo vệ mạnh mẽ hơn chống lại phần mềm độc hại cố gắng khai thác kernel của Windows. Tuy nhiên, hiệu suất của hệ thống có thể bị ảnh hưởng, đặc biệt trên các bộ vi xử lý cũ không hỗ trợ các tính năng như Mode-Based Execution Control (MBEC) của Intel hoặc Guest Mode Execute Trap (GMET) của AMD[16]. Trên các bộ vi xử lý này, HVCI phải dựa vào mô phỏng, dẫn đến tác động lớn hơn đến hiệu suất. Ngoài ra, việc bật HVCI có thể gây ra vấn đề tương thích với một số driver không được thiết kế để hoạt động trong môi trường được bảo vệ bởi HVCI. Do đó, trước khi triển khai HVCI trong môi trường doanh nghiệp, nên kiểm tra tính tương thích của tất cả các driver và ứng dụng quan trọng để đảm bảo hệ thống hoạt động ổn định.

d. Secure Boot

Secure Boot là một tính năng bảo mật quan trọng trong hệ thống sử dụng **UEFI (Unified Extensible Firmware Interface)**, giúp đảm bảo rằng chỉ các phần mềm và firmware đã được xác thực mới được phép khởi động[17]. Tính năng này hoạt động bằng cách kiểm tra chữ ký số của firmware, bootloader và hệ điều hành trước khi cho phép chúng thực thi, ngăn chặn các mã độc như bootkits và rootkits xâm nhập vào quá trình khởi động hệ thống.

Cách thức hoạt động của Secure Boot tập trung vào việc kiểm tra chữ ký số của các thành phần thiết yếu trong quá trình khởi động. Mỗi phần mềm như firmware, bootloader và kernel của hệ điều hành phải có chữ ký số được chứng thực từ nhà sản xuất hoặc nhà cung cấp đáng tin cậy. Qua đó, hệ thống sẽ chỉ cho phép thực thi những thành phần đạt chuẩn, ngăn chặn các bootkits – mã độc có khả năng chạy trước khi hệ

---

[16] vinaypamnani-msft. (2024, October 31). Enable memory integrity. Microsoft.com. https://learn.microsoft.com/en-us/windows/security/hardware-security/enable-virtualization-based-protection-of-code-integrity?utm_source=chatgpt.com&tabs=security

[17] Windows 11 and Secure Boot - Microsoft Support. (n.d.). Support.microsoft.com. https://support.microsoft.com/en-us/windows/windows-11-and-secure-boot-a8ff1202-c0d9-42f5-940f-843abef64fad

điều hành khởi động – từ việc xâm nhập vào quá trình khởi động, đảm bảo rằng hệ thống luôn được bảo vệ từ giai đoạn đầu tiên.

Nhờ cơ chế xác thực chặt chẽ này, Secure Boot đóng vai trò then chốt trong việc duy trì tính toàn vẹn và ổn định của hệ thống, đặc biệt trong các môi trường đòi hỏi mức độ bảo mật cao như doanh nghiệp, y tế và các thiết bị IoT. Mặc dù việc triển khai yêu cầu phần cứng hỗ trợ UEFI và có thể gặp một số thách thức về tương thích với các thiết bị cũ, lợi ích bảo mật mà Secure Boot mang lại đã được xác nhận bởi các chuyên gia bảo mật hàng đầu, góp phần làm giảm thiểu nguy cơ tấn công từ bootkits và rootkits ngay từ giai đoạn khởi động.