Mandatory Integrity Control

\* Kiểm soát toàn vẹn bắt buộc (MIC) cung cấp cơ chế kiểm soát truy cập vào các đối tượng có thể bảo mật.

\* Cơ chế này:

+ Bổ sung cho quyền kiểm soát truy cập tùy ý (discretionary access control)

+ Đánh giá quyền truy cập trước khi kiểm tra quyền truy cập đối với danh sách kiểm soát quyền truy cập (DACL) của đối tượng được đánh giá

\* MIC sử dụng mức toàn vẹn và chính sách bắt buộc để đánh giá quyền truy cập. Các nguyên tắc bảo mật và các đối tượng có thể bảo mật được chỉ định các mức toàn vẹn để xác định mức độ bảo vệ hoặc quyền truy cập của chúng

\* Windows định nghĩa 4 mức toàn vẹn: thấp, trung bình, cao và hệ thống. Người dùng chuẩn nhận mức trung bình, người dùng nâng cao nhận mức cao.

+ Các tiến trình do người dùng khởi động và các đối tượng do người dùng tạo sẽ nhận mức toàn vẹn của chính người dùng đó (trung bình/cao) hoặc thấp nếu mức của tệp thực thi là thấp.

+ Các dịch vụ hệ thống nhận được tính toàn vẹn của hệ thống

+ Các đối tượng không có nhãn toàn vẹn được hệ điều hành coi là trung bình =>ngăn không cho mã toàn vẹn thấp sửa đổi các đối tượng không có nhãn

=> Windows đảm bảo rằng các quy trình chạy với mức toàn vẹn thấp không thể truy cập vào quy trình được liên kết với một vùng chứa ứng dụng

I. Nhãn toàn vẹn (Integrity Labels)

+ Nhãn toàn vẹn chỉ định mức độ toàn vẹn của các đối tượng có thể bảo mật và các nguyên tắc bảo mật

+ Nhãn toàn vẹn được biểu diễn bằng SID toàn vẹn.

* SID toàn vẹn cho một đối tượng có thể bảo mật được lưu trữ trong [danh sách kiểm soát truy cập hệ thống](https://learn.microsoft.com/en-us/windows/desktop/SecGloss/s-gly) (SACL) của đối tượng đó
* Bất kỳ đối tượng nào không có SID toàn vẹn đều được coi như có tính toàn vẹn trung bình.
* Mã SID toàn vẹn cho một nguyên tắc bảo mật được lưu trữ trong mã thông báo truy cập của nó. Mã thông báo truy cập có thể chứa một hoặc nhiều mã SID toàn vẹn.

II. Tạo tiến trình (Process Creation)

+ Người dùng khởi chạy tệp thực thi => quy trình mới được tạo với mức tối thiểu của mức toàn vẹn của người dùng và của tệp (⬄ quy trình mới không bao giờ thực thi với mức toàn vẹn cao hơn tệp thực thi)

+ giúp bảo vệ người dùng khởi chạy mã không đáng tin cậy khỏi các hành vi độc hại do mã đó thực hiện

+ Dữ liệu người dùng, ở mức toàn vẹn của người dùng thông thường, được bảo vệ chống ghi đối với quy trình mới này

III. Chính sách bắt buộc (Mandatory Policy)

+ SYSTEM\_MANDATORY\_LABEL\_ACE ACE trong SACL của một đối tượng có thể bảo mật chứa một mặt nạ truy cập chỉ định quyền truy cập mà các nguyên tắc có mức toàn vẹn thấp hơn đối tượng được cấp

+ Các giá trị xác định cho mặt nạ truy cập:

- [**SYSTEM\_MANDATORY\_LABEL\_NO\_WRITE\_UP**](https://learn.microsoft.com/en-us/windows/desktop/api/Winnt/ns-winnt-system_mandatory_label_ace)(Được mặc định)

**-** SYSTEM\_MANDATORY\_LABEL\_NO\_READ\_UP

**-** SYSTEM\_MANDATORY\_LABEL\_NO\_EXECUTE\_UP

+ Access Token cũng chỉ định 1 chính sách bắt buộc được LSA (Cơ quan bảo mật cục bộ) thiết lập khi access token được tạo. Chúng được chỉ định bởi cấu trúc TOKEN\_MANDATORY\_POLICY liên kết với access token. Có thể truy vấn bằng hàm GetTokenInformation với giá trị TokenInformationClass được đặt thành TokenMandatoryPolicy