**Thứ tự tìm kiếm DLL**

Khi một chương trình (ví dụ: program.exe) cần một file DLL (ví dụ: example.dll), Windows sẽ tìm kiếm theo thứ tự sau:

1. **Thư mục của chương trình đang chạy (Directory of Program):**
   * Windows kiểm tra thư mục chứa file thực thi (program.exe). Nếu tìm thấy file DLL ở đây, nó sẽ được sử dụng.
2. **Thư mục System32:**
   * Nếu DLL không được tìm thấy trong thư mục chương trình, Windows sẽ tìm trong thư mục C:\Windows\System32. Đây là nơi chứa các file hệ thống 64-bit.
3. **Thư mục System:**
   * Thư mục C:\Windows\System chứa các file hệ thống hỗ trợ, thường là dành cho các ứng dụng cũ hơn.
4. **Thư mục Windows:**
   * Nếu DLL vẫn chưa được tìm thấy, Windows sẽ kiểm tra thư mục gốc của hệ điều hành (C:\Windows).
5. **Thư mục làm việc hiện tại (Current Directory):**
   * Là thư mục hiện tại mà chương trình thực thi đang hoạt động.
6. **Các thư mục trong biến môi trường %PATH%:**
   * Cuối cùng, Windows sẽ tìm DLL trong các thư mục được liệt kê trong biến môi trường %PATH%. Đây là danh sách các đường dẫn mà hệ thống sử dụng để tìm kiếm file thực thi.

**Ví dụ thực tế**

Giả sử có chương trình program.exe cần tải file example.dll, và hệ thống có các file DLL với nội dung khác nhau ở các vị trí sau:

1. **Thư mục chứa program.exe:** example.dll (phiên bản hợp pháp).
2. **Thư mục C:\Windows\System32:** example.dll (phiên bản hệ thống).
3. **Thư mục trong %PATH%:** example.dll (phiên bản mã độc).

**Kết quả:**

* Nếu example.dll tồn tại trong thư mục của chương trình, phiên bản hợp pháp sẽ được sử dụng.
* Nếu không, hệ thống sẽ sử dụng phiên bản trong C:\Windows\System32.
* Nếu không tìm thấy trong các vị trí trước, nó sẽ tải phiên bản từ %PATH%, có thể dẫn đến nguy cơ mã độc được thực thi.

**Mở rộng: Lỗ hổng DLL Hijacking**

**Khái niệm:**

* DLL Hijacking là kỹ thuật mà hacker sử dụng để "chiếm quyền" tìm kiếm DLL. Nếu một file DLL không tồn tại trong các vị trí hợp lệ, hệ thống sẽ cố gắng tìm kiếm ở các vị trí khác, mở ra cơ hội cho hacker đặt file DLL giả mạo.

**Ví dụ lỗ hổng:**

* Một ứng dụng hợp pháp yêu cầu example.dll nhưng không bao gồm file này trong thư mục chương trình.
* Hacker đặt một file example.dll độc hại trong cùng thư mục với program.exe.
* Khi chương trình chạy, file DLL độc hại sẽ được tải trước.

**Phòng chống:**

* **Ký số (Code Signing):** Các file DLL nên được ký để đảm bảo tính xác thực.
* **Sử dụng SetDllDirectory():** Hạn chế các thư mục mà chương trình sẽ tìm kiếm DLL.
* **Cài đặt chế độ Safe DLL Search:** Windows có thể được cấu hình để ưu tiên tìm DLL từ thư mục hệ thống trước.

![A screenshot of a computer

Description automatically generated]()