HỌC VIỆN KỸ THUẬT MẬT MÃ

KHOA AN TOÀN THÔNG TIN

BÁO CÁO MÔN HỌC

AN TOÀN HỆ ĐIỀU HÀNH

Đề tài:

TÌM HIỂU VỀ INTEGRITY FLAWS

Sinh viên thực hiện: **Trần Cao Minh Bách – AT150204**

Vũ Thị Ánh - AT150504

Bạch Trường An – AT150201

Phạm Đỗ Thuỳ Linh - AT150232

Nguyễn Đình Hùng - AT150224

Giảng viên hướng dẫn: **Đồng Thị Thuỳ Linh**

Hà Nội, 11-2021

LỜI NÓI ĐẦU

Việc phát triển số, thay đổi số và số hoá các dịch vụ đang là xu hướng. Nhưng bên cạnh đó cũng tiềm ẩn nhiều vấn đề bất cập. Với những hệ thống lớn được phát triển lâu năm còn có thể tồn tại nhiều lỗ hổng, những lỗi nhỏ đến những lỗi rất lớn và nghiêm trọng khiến cho hệ thống bị ảnh hưởng cực kì lớn. Vì thế, trong thời kì số hoá hiện tại, các hệ thống mới được xây dựng, còn ít kinh nghiệm và khả năng tài lực hạn chế. Việc mắc những lỗi này là hoàn toàn có thể xảy ra, không những thế còn đem lại phiền toái cho người sử dụng, khiến dịch vụ cung cấp không đáp ứng được nhu cầu. Nặng hơn là việc tồn tại các lỗi trong hệ thống có thể là một điểm yếu nguy hiểm, có thể phá vỡ kết cấu của cả một hệ thống nếu không có cách để phòng thủ cũng như phương án phục hồi nếu bị kẻ xấu lợi dụng phá hoại và gây ra những thiệt hại không đáng có.

Đồ án này đề cập tới những vấn đề liên quan tới lỗ hổng của tính toàn vẹn trong hệ thống. Nó mang đến những khái niệm bao quát đến chi tiết cho từng phân loại trong lỗ hổng toàn vẹn. Với khái niệm, đồ án sẽ cung cấp cái nhìn khách quan, sự liên hệ tới nhưng thành phần trong hệ thống, các đối tượng có khả năng gây ra ảnh hưởng từ lỗ hổng có tồn tại trong hệ thống. Việc này giúp cung cấp kiến thức nhất định, giúp giải nghĩa các phần sau được chi tiết hơn.

Các vấn đề về phương thức và cách khai thác cũng được nghiên cứu và đề ra trong đồ án này. Các khái niệm của từng phương thức và cách khai thác được nêu chi tiết và cụ thể. Các ví dụ trực quan sẽ được đưa ra tương ứng với từng loại, đáp ứng cái nhìn khách quan cho vấn đề mà đồ án này nghiên cứu.

LỜI CAM ĐOAN

Tôi là Trần Cao Minh Bách, mã số sinh viên AT150204, sinh viên lớp AT15B, khóa AT15. Người hướng dẫn là Đồng Thị Thuỳ Linh. Tôi xin thay mặt, cam đoan toàn bộ nội dung được trình bày trong đồ án Tìm hiểu về Integrity Flaws là kết quả quá trình tìm hiểu và nghiên cứu của chúng tôi. Các dữ liệu được nêu trong đồ án là hoàn toàn trung thực, phản ánh đúng kết quả đo đạc thực tế. Mọi thông tin trích dẫn đều tuân thủ các quy định về sở hữu trí tuệ; các tài liệu tham khảo được liệt kê rõ ràng. Tôi xin chịu hoàn toàn trách nhiệm với những nội dung được viết trong đồ án này.

Hà Nội, ngày 25 tháng 11 năm 2021

Người cam đoan

Trần Cao Minh Bách

MỤC LỤC

TÓM TẮT ĐỒ ÁN

Hiện tại, việc phát triển số, số hoá mọi thứ đang là mũi nhọn phát triển của công nghệ thông tin. Các hệ thống được xây dựng lên để cung cấp dịch vụ số nhất định. Có nhiều hệ thống đôi khi vì kinh phí hạn hẹp mà các biện pháp phòng thủ còn lỏng lẻo vì không có kinh phí cho vấn đề nghiên cứu và phát triển các chính sách an toàn thông tin một cách phù hợp. Bên cạnh đó, việc phát triển số quá nhanh khiến cho các hệ thống không thể đáp ứng kịp khi người dùng tăng lên một cách đột ngột, khiến dịch vụ của hệ thống không thể đáp ứng được cho người dùng. Bên cạnh đó, các chính sách có lỗ hổng, khiến cho kẻ xấu có thể lợi dụng để khai thác vào nhưng lỗ hổng. Tất cả lý do trên khiến cho việc đảm bảo tính chất trong tam giác CIA bị lung lay. Ở đồ án này sẽ đề cập về những vấn đề liên qua đến tính chất Toàn vẹn của hệ thống nói chung và các ảnh hưởng khi khai thác những lỗ hổng của tính Toàn vẹn hệ thống. Đồ án chia thành 3 chương với nội dung các chương như sau:

Chương 1: Đề cập đến định nghĩa chung của tính toàn vẹn trong hệ thống, các loại lỗ hổng của tính toàn vẹn, các đối tượng có thể khai thác được từ việc có lỗ hổng toàn vẹn trong hệ thống.

Chương 2: Đề cập tới những phương thức và cách khai thác những lỗ hổng bao gồm định nghĩa và các ví dụ cơ bản để miêu tả về việc khai thác, từ đó đem lại cái nhìn khách quan cho vấn đề mà đồ án đề cập tới.

Chương 3: Đề cập chi tiết các loại lỗ hổng thực tế có thể xảy ra với các hệ thống. Với các định nghĩa và kịch bản sơ bộ giúp khái quát các vấn đề của một hệ thống thực tế có thể bị ảnh hưởng.

Kết luận: Đánh giá quá trình nghiên cứu và tìm hiểu của đồ án.

CHƯƠNG 1. KHÁI NIỆM CHUNG VỀ INTEGRITY FLAWS

Nội dung chương đề cập tới khái niệm chung của Intergrity Flaws, nhằm đưa cái nhìn khách quan nhất về dạng lỗ hổng này. Cùng với đó là những đối tượng có thể tham gia vào việc gây lỗi, cũng như các lỗ hổng của tính toàn vẹn.

1.1 Tính toàn vẹn của hệ điều hành

Tính toàn vẹn của hệ điều hành liên quan đến việc đảm bảo rằng hệ điều hành hoạt động bình thường. Do đó, một lỗ hổng toàn vẹn của hệ điều hành cho phép người dùng (hoặc chương trình) làm cho hệ điều hành hoạt động không đáng chính xác và không an toàn. Tính toàn vẹn được xác định trước các vấn đề về độ tin cậy (gian lận và sai sót) và các vấn đề về bảo mật (kiểm tra tài nguyên và quyền riêng tư).

1.2 Các loại lỗ hổng toàn vẹn

Tương ứng với mỗi thành phần của hệ thống thì việc chia lỗ hổng theo các thành phần này là cách đơn giản nhất để khái quát về nó. Với 6 loại sau:

a) Vật lý

Các lỗi liên quan đến vật lý thường là các lỗi mang tính chất khách quan như: thiên tai, thảm hoạ. Nhưng bên cạnh đó là các lỗi mang tính chủ quan như: việc bị đánh chặn viễn thông, độ bảo mật kém ở các thiết bị đầu cuối, truy cập không được phép vào phòng máy chứa các thông tin quan trọng.

b) Phần cứng

Là thành phần chính để người dùng có thể giao tiếp với các phần mềm thông qua cử chỉ vật lý. Vì vậy, những ảnh hưởng vật lý cơ bản như việc bị ngắt nguồn ở các thiết bị đầu cuối, hay các thiết bị đầu cuối không được đồng bộ tín hiệu đến với phần mềm hệ điều hành. Hoặc những lỗi như việc cung cấp các quyền một cách không chặt chẽ, khiến cho việc tiếp cận với các phần cứng dễ dàng, khiến cho nguy cơ bị phá hoại tăng cao.

c) Nhân viên – Nhân sự

Các lỗi liên quan đến nhân viên, nhân sự là các lỗi mang tính chủ quan là chính. Khi này những người có hành vi phá hoại và có ý định lạm dụng quyền lực để có thể thay đổi, đánh cắp hay phá hoại thông tin. Bên cạnh đó là khía cạnh chủ quan, khi nhân viên trong công ty bị dính bẫy của nhưng kẻ phá hoại từ đó lỡ khiếp cho kẻ xấu có cơ hội tiếp cận và phá hoại thông tin từ bên ngoài. Hay việc dán nhãn cho thông tin chưa chặt chẽ, người dùng trong hệ thống có thể phân quyền thiếu. Bên cạnh đó là vấn đề dính các loại Trojan Horse, worm hay virus cũng là những nguy cơ rất cao khiến mất tính toàn vẹn hệ thống xảy ra.

d) Thủ tục

Các thủ tục cài đặt không được kiểm soát chặt chẽ có thể dẫn tới việc người dùng cài đặt các phần mềm không rõ nguồn gốc, và có tồn tại các dạng virus, worn hay Trojan Horse, đe doạ đến sự toàn vẹn của hệ thống. Hoặc các thủ tục quá rườm rà, khiến người dùng không đọc kĩ cũng có thể khiến các cấu hình ban đầu không còn đảm bảo.

e) Phần mềm

Các phần mềm ứng dụng cho phép phân tách người dùng ra khỏi hệ thống một cách độc lập, sử dụng nó để có thể giao tiếp với hệ thống, nhằm giảm thiểu rủi ro đem lại cho hệ thống thực tế. Nhưng việc xây dựng và cấu hình hệ thống không chặt chẽ có thể khiến cho việc truy cập, kiểu soát các dữ liệu có thể xảy ra, cùng với đó là vấn đề logic trong chương trình, lỗi logic cũng có thể gây ra các ảnh hưởng ở nhiều mức độ khác nhau.

f) Hệ điều hành

Hệ điều hành cũng là một phần mềm, nên các vấn đề xảy ra ở trên phần mềm chính là lỗi trên hệ điều hành, nhưng việc tồn tại các lỗi ở hệ điều hành thì có thể gây ra các ảnh hưởng rất lớn, đặc biệt nghiêm trọng cho cả hệ thống. Vì vậy, việc đảm bảo hệ thống có một hệ điều hành ổn định, đảm bảo tính chuẩn xác và sự an toàn là vấn đề rất quan trọng.

1.3 Đối tượng gây ảnh hưởng

Trong quá trình sử dụng, người dùng trong hệ thống là một thành phần có khả năng xâm phạm tính toàn vẹn của cài đặt thông qua lỗ hổng. Khi được đưa vào sử dụng, các lỗi tồn tại trên có thể cho phép truy cập trái phép vào tài nguyên không được phép thông qua những phương thức khác nhau, từ đó gây hại đến hệ thống.

Với những người dùng ứng dụng, họ là những người chưa được cấp các đặc quyền với hệ thống ngoài quyền có thể sử dụng các dịch vụ cơ bản mà hệ thống cho phép được sử dụng. Họ được chia thành người sử dụng và nhà sản xuất. Người sử dụng là người nhận được các uỷ quyền các thông tin sản phẩn từ một ứng dụng dựa trên máy tính. Nhà sản xuất là nơi phân phối và lập trình các ứng dụng đó, nhưng người thiết kế và triển khai các ứng dụng cụ thể tạo ra thông tin cho người tiêu dùng.

Việc người dùng gây ảnh hưởng tới hệ thống hay làm mất đi tính toàn vẹn của hệ thống là điều hết sức hiển nhiên. Vì lý do đó, việc nhà sản xuất phải thiết kế và phân tích làm sao đảm bảo được tính cô lập, nhằm giúp cho đảm bảo được sự an toàn cho chính hệ thống, cũng như những người dùng khác. Nhưng, bên cạnh đó, trong nhà sản xuất, các thông tin người dùng cũng là vấn đề gây ra nhiều tranh cãi, vì nhiều vụ việc nhân viên trong các nhà sản xuất tự ý xâm phạm, khiến cho tính chất bảo mật và toàn vẹn bị vi phạm nghiêm trọng, từ đó việc đảm bảo các chính sách ở lớp người dùng này là vấn đề quan trọng và cấp thiết.

Bên cạnh đó, nhóm sử dụng ở dạng dịch vụ được chia thành dnajg hệ thống và người phục vụ quản trị. Người bảo trì hệ thống là thành viên của đội ngũ nhân viên bảo trình bao gồm người vận hành, người lập trình hệ thống và kĩ sư quản lý chính. Những người chịu trách nhiệm bảo trì và tính sẵn có của hệ thống phải đảm bảo được tính sẵn và toàn vẹn để có thể cung cấp được dịch vụ một cách liên tục tại bất kì đâu. Nhưng cũng vì thế người vận hành có thể truy cập vào thông tin người dùng, thông tin hệ thống. Đôi khi việc lạm quyền có thể gây mất tính bảo mật và toàn vẹn cho hệ thống trên.

Và cuối cùng là hệ người dùng vãn lai, không có thông tin trên hệ thống. Đây là những người dùng không có đặc quyền truy cập vào các sản phẩm hay thiết bị, thay đổi hay sửa đổi thông tin. Nhưng việc cố gắng truy cập, khai thác sẽ là trái phép, và

khả năng luôn luôn là việc tấn công và gây ra ảnh hưởng lớn cho toàn hệ thống nếu tồn tại các lỗ hổng có thể khai thác từ đó.

1.4 Đối tượng bị ảnh hưởng

Các đối tượng bị ảnh hưởng là các đối tượng trực tiếp có mặt trong hệ thống như các tài nguyên của hệ thống. Khi bị ảnh hưởng, các tài nguyên sẽ bị ảnh hưởng theo hướng dây chuyền khiến cho ảnh hưởng có thể gây ra tác hại to lớn. Các tài nguyên có giá trị như là các thiết bị đầu cuối hay là thông tin của hệ thống, dịch vụ. Thông tin thì bao gồm tất các các tệp của hệ thống như: chương trình, dữ liệu, thư mục tệp của hệ thống và tất các thư mục của người dùng.

Dịch vụ thì đại diện cho các hoạt động của hệ thống cung cấp nơi người dùng cuối, thường luôn phải đảm bảo tính sẵn sàng, nhưng bên cạnh đó là đảm bảo tính toàn vẹn cho các thông tin liên quan đến dịch vụ đó. Nếu người dùng có quyền truy cập thì việc đảm bảo người dùng được sử dụng đúng các dịch vụ trên và không để người dùng lạm quyền, sử dụng trái phép các dịch vụ không được uỷ quyền.

Tài nguyên ở dạng thiết bị là các thành phần vật lý, có nhiều nguy cơ ảnh hưởng nhất, khi mà các thiết bị có thể bị các tác nhân khách quan gây ảnh hưởng, mỗi thiết bị trong hệ thống là một mắt xích quan trọng, vì thế việc đảm bảo tính toàn vẹn với thiết bị là rất cần thiết. Bên cạnh đó, phần cứng như các thiết bị không hoạt động, thì dịch vụ cũng không thể nào cung cấp cho các người dùng cuối được.

CHƯƠNG 2. PHƯƠNG THỨC VÀ CÁCH KHAI THÁC TRÊN CÁC ĐỐI TƯỢNG

Loại lỗ hổng này xảy ra trên tất cả các thành phần của hệ thống thông tin. Chỉ cần sơ xuất trong quá trình cấu hình, cài đặt hệ thống, các đầu mối nhỏ trong cả một chuỗi cũng có thể gây ra lỗ hổng theo tính dây chuyền, khiến việc ngăn chặn lỗi hết sức muộn màng và gây nên nhiều tác hại nặng nề. Chương 2 sẽ đề cập tới các đối tượng đặc trưng có thể bị ảnh hưởng trong hệ thống. Bên cạnh đó là các ảnh hưởng này sẽ gây ra các tác động gì trên các đối tượng này.

2.1 Phương thức gây ra

2.1.1 Đánh chặn (Interception)

Đánh chặn là việc một cá nhân có cập trái phép vào thông tin cá nhân hoặc nhạy cảm. Một cuộc tấn công đánh chặn vi phạm trực tiếp đến tính Bảo mật của tam giác CIA, nó có thể là xem hoặc sao chép trái phép các dữ liệu, nghe lén một cuộc điện thoại hay đọc trộm email…

Người bị ảnh hướng trực tiếp chính là người dùng cuối (Users) vì kẻ tấn công có thể xem và thu thập những thông tin cá nhân như họ tên, số tài khoản… Từ những gói tin mà chúng thu thập được.

2.1.2 Thu thập (Scavenging)

Là quá trình tìm kiếm dữ liệu bí mật hoặc có giá trị thông qua các thóng tin từ dữ liệu hệ thống . Đây thường là bước đầu tiên trong hầu hết các cuộc tấn công có chủ đích.

Ở đây kẻ tấn công sử dụng kết hợp các tiện ích trên mạng cùng với các công cụ truy vấn, tìm kiếm để tìm hiểu về mục tiêu nhiều nhất có thể. Các cuộc tấn công này hầu như không thể bị phát hiện vì 2 lý do chính:

Nếu cuộc tấn công sử dụng các tiện ích như Ping, Traceroute… Lưu lượng dữ liệu chúng chiếm là rất nhỏ để có thể tìm ra ai là kẻ tấn công. Thêm nữa, rất khó để phân biệt được những người sử dụng hợp pháp và kẻ tấn công

Những thông tin lấy được qua Whois, Nslookup hoặc các công cụ tìm kiếm thường là những thông tin công khai, tức là ai cũng có thể tìm kiếm ra chúng.

2.1.3 Chiếm quyền ưu tiên(Pre-emtion)

Mọi yêu cầu của bạn khi được gửi đến máy chủ đều được sắp xếp để xử lý. Có nhiều giải thuật để sắp xếp những yêu cầu này một cách tối ưu, tuỳ theo đặc thù của mỗi hệ thống mà nó những giải thuật khác nhau, ví dụ như giải thuật First come first served (FCFS)- đến trước xử lý trước , hay Shortest Remain Time (SRT)- ưu tiên thời gian chạy của các tiến trình ngắn…

Tuỳ theo mỗi cách lập lịch sẽ có độ ưu tiên khác nhau, do đó có nhiều cách để tấn công. Ý tưởng chung của một cuộc tấn công chiếm quyền ưu tiên là chèn một hoặc nhiều tiến trình có mức độ ưu tiên hơn yêu cầu của nạn nhân. Dẫn đến việc yêu cầu của nạn nhân không được hoặc xử lý rất chậm.

Đối tượng bị ảnh hưởng có thể là hệ thống khi phải xử lý những tác vụ vô ích mà kẻ tấn công cài vào, nhưng trực tiếp ảnh hưởng đến tính Sẵn sàng của tam giác CIA vì hệ thống không thể xử lý ngay lập tức các yêu cầu từ người dùng.

2.1.4 Chiếm hữu (Possession)

Đây là cuộc tấn công mà kẻ tấn công tìm cách có được quyền điều khiển hoặc quyền sở hữu một thứ gì đó từ bạn như một phiên đăng nhập, một dịch vụ mà bạn đăng ký online.

Một phiên làm việc bắt đầu từ khi bạn đăng nhập và kết thúc khi bạn đăng xuất. Khi này mọi yêu cầu của bạn gửi đến server sẽ kèm theo cookie- là thứ để hệ thống xác định được người dùng là bạn. Nếu chúng có thể giả mạo cookie này thì có thể tương tác với hệ thống dưới danh nghĩa là bạn.

Khi giả mạo được bạn mới chỉ là bước đầu, kẻ tấn công có thể tìm kiếm và sử dụng những thông tin của bạn để làm nhiều việc gây bất lợi như chuyển tiền, thay đổi thông tin cá nhân, nhắn tin lừa đảo…

2.2 Cách khai thác trên các đối tượng

Với những phương thức được liệt kê bên trên, việc khai thác thường phân theo ba dạng dưới đây:

- Từ chối chiếm hữu/sử dụng
- Từ chối chiếu hiễm/sử dụng độc quyền
- Sửa đổi thông tin

Mỗi cách khai thác có một đặc thù riêng của nó, chính vì vậy mà ảnh hưởng gây ra là khác nhau.

2.2.1 Từ chối chiếm hữu/sử dụng

a) Đánh cắp thiết bị

Việc đánh cắp các thiết bị đầu cuối, các thiết bị trên đường truyền, hay bất kì các thiết bị trong hệ thống, đề khiến ảnh hưởng đến tính toàn vẹn của thông tin của hệ thống. Những kẻ xấu từ đó sẽ lấy cắp được những nguồn thông tin có giá trị từ các thiết bị đánh cắp được, từ đó có thể giả mạo để xâm nhập sâu hơn vào hệ thống. Bên cạnh đó là vấn đề gián đoạn dịch vụ, khi mà một thiết bị quan trọng không còn trong chuỗi, có thể khiến cho cả hệ thống tê liệt, dẫn tới việc từ chối những dịch vụ mà nó đang cung cấp cho người dùng.

b) Phá hoại thiết bị

Việc phá hoại là một vấn đề hết sức nguy hiểm, các thiết bị ngoài vấn đề về kinh tế, còn có thể là những thiết bị khó có khả năng thay thế sửa chữa, nếu không có hướng sao lưu dữ liệu trong nhưng thiết bị ấy, việc mất đảm bảo toàn vẹn là điều không thể tránh khỏi.

c) Làm xuống cấp dịch vụ

Các dịch vụ đang được cung cấp bình thường, nhưng vì kẻ phá hoại sử dụng các cách tấn công từ chối dịch vụ như DoS hay DDoS, việc dịch vụ xuống cấp trong thời gian dài có thể ảnh hưởng tới đường truyền, dữ liệu trên đường truyền có thể không đảm bảo cho việc toàn vẹn, có khả năng gây thất thoát dữ liệu, lỗi dữ liệu trên đường truyền.

d) Làm gián đoạn dịch vụ

Việc làm gián đoạn dịch vụ đôi khi cũng tương tự như xuống cấp vì vậy các ảnh hưởng cũng tương tự như thế.

e) Phá hoại dữ liệu

Việc phá hoại dữ liệu là vô cùng nguy hiểm, nó trực tiếp ảnh hưởng tới tính toàn vẹn, không như các cách khai thác trên. Việc tấn công và khai thác từ nó khiến cho người dùng bị ảnh hưởng trực tiếp, hệ thống phải mất nhiều thời gian mới có thể phục hồi lại như trước khi bị phá hoại. Nó gián tiếp làm giảm chất lượng dịch vụ, đôi khi làm gián đoạn và khiến cho người dùng cuối khó lòng chấp nhận được.

2.2.2 Từ chối chiếm hữu/sử dụng độc quyền

a) Đọc/Sao chép lại dữ liệu

Việc người dùng, hay ứng dụng khác không được cấp quyền nhưng vẫn có thể truy cập vào được những dữ liệu quan trọng, có tính cần bảo mật lớn hơn, ví dụ việc người dùng này đọc được các thông tin nhạy cảm của người dùng khác. Việc này khiến cho dữ liệu bị thất thoát, dễ làm mất tính bảo mật và sự toàn vẹn của dữ liệu. Các thông tin giờ đây không còn là sự sở hữu duy nhất của 1 đối tượng cụ thể nữa, mà là của nhiều đối tượng và là sự trái phép.

b) Đánh cắp dịch vụ

Bằng một cách nào đó, các dịch vụ được cung cấp bị điều khiển bởi một yếu tố khác thường, làm việc cung cấp dịch vụ có thể gây gián đoạn cho các người dùng khác, nó có thể khiến cho người dùng khó chịu. Đôi khi việc đánh cắp dịch vụ còn làm hao tổn kinh tế của đơn vị cung cấp dịch vụ, chiếm dụng có thể đem lại lợi ích trái phép cho kẻ đánh cắp.

2.2.3 Sửa đổi thông tin

a) Sửa đổi dữ liệu

Việc sửa đổi thông tin là vấn đề trực tiếp khiến cho thông tin không còn toàn vẹn nếu như người sửa đổi là một người không được cấp quyền hoặc sửa đổi trái phép,

đó là chủ quan. Đôi khi vấn đề khách quan còn xảy ra khi thông tin sửa đổi bị nhầm lẫn do người có quyền thực hiện.

b) Sửa đổi thiết bị

Việc sửa đổi thiết bị trái phép có thể khiến cho hệ thống hoạt động kém ổn định, các thiết bị cũ có thể xung đột với thiết bị mới, khiến cho các dữ liệu bị lỗi. Từ đó sẽ không đảm bảo tính toàn vẹn. Bên cạnh đó thay đổi thiết bị trái phép cũng không đảm bảo được sự toàn vẹn của hệ thống như những lý do trên đã đề cập.

CHƯƠNG 3. CÁC HÌNH THỨC KHAI THÁC LỖ HỔNG

Ở chương này sẽ đề cập tới những lỗi bảo mật từ đó thấy được tầm quan trọng của việc đảm bảo sự toàn vẹn của hệ thống nói chung và sự toàn vẹn của hệ điều hành nói riêng. Từng mục cũng sẽ có những ví dụ cụ thể, giúp cho ta có cái nhìn khái quát nhất từng lỗi.

3.1 Xác thực không đầy đủ

Ở mức độ hoàn thiện nhất định, một chương trình với những câu lệnh có đặc quyền này gồm các yêu cầu các dịch vụ từ bước thứ 2, với một tập các câu lệnh có đặc quyền khác. Việc bảo vệ tính toàn vẹn cho hệ thống đòi hỏi việc xác thực phải kĩ lưỡng. Đối với hầu hết các hệ điều hành hiện nay, ranh giới giúp bảo toàn tính toàn vẹn hệ thống là ranh giới giữa chương trình điều khiển với chương trình người dùng. Khi đó, chương trình người dùng sẽ có những hạn chế nhất định, giúp cho hệ thống an toàn hơn. Bên cạnh đó, việc tách biệt này khiến cho các thành phần của hệ thống hoạt động độc lập, không làm gián đoạn quá trình hoạt động.

Các chương trình người dùng muốn sử dụng thì hệ thống sẽ gọi các chương trình con và nạp vào nhiều tham số. Và để gọi được thì người dùng cần thông qua chương trình điều khiển, lúc ấy, các dịch vụ được yêu cầu mới có thể thực thi. Việc tạp ra sự tách biệt này giữa các chương trình nhằm hạn chế được việc người dùng nào đó cố ý hay vô tình làm ảnh hưởng đến hoạt động của chương trình điều khiển, kéo theo ảnh hưởng dây chuyền các dịch vụ đang cung cấp cho người dùng khác. Nếu cơ chế kiểm tra các tham số đầu vào này không được chặt chẽ, việc kẻ tấn công có thể lợi dụng và đánh lừa chương trình điều khiển thực hiện được một yêu cầu vượt quá quyền hạn, từ đó gây ra sự mất an toàn cho toàn hệ thống. Và các trường cần phải xem xét cũng như kiểm tra kĩ như:

- Các kiểu và định dạng dữ liệu.
- Số lượng và thứ tự
- Phạm vi của giá trị
- Quyền truy cập vào các vị trí lưu trữ
- Tính nhất quán giữ các tham số (vị trí lữu trữ, …)

Từ những tham số trên, lỗ hổng này có thể có kịch bản nguy hiểm xảy ra nếu người dùng thành công trong việc nạp tham số không hợp lệ vào chương trình điều khiển. Việc chấp nhận một tham số bao gồm một địa chỉ bên ngoài không gian bộ nhớ được cấp phát cho người dùng đó có thể khiến:

- Chương trình có thể lấy được dữ liệu trái phép cho người dùng đó.
- Một tập hợp các điều kiện có thể được tạo ra gây ra sự cố cho hệ thống.
- Có thể thực thi được dòng lệnh nhằm điều khiển hệ thống.

Với một kịch bản có sẵn như sau có thể khiến cho hệ thống ảnh hưởng nghiêm trọng:

- Một lệnh, khi được thực thi, sẽ chuyển quyền điều khiển đến một điểm xác định trước trong chương trình của người dùng được nạp vào một thanh ghi.
- Một lệnh hệ thống sau đó được thực hiện làm cho các thanh ghi được lưu bằng chương trình điều khiển trong Vùng lưu đăng ký.
- Sau khi trả lại quyền kiểm soát cho người dùng, một lệnh gọi hệ thống khác sẽ được thực hiện. Trong số các tham số cho lệnh gọi hệ thống này, là một con trỏ (địa chỉ) phải trỏ đến một vị trí trong chương trình điều khiển. Địa chỉ này sẽ được sử dụng để chuyển quyền kiểm soát sang quy trình dịch vụ chương trình khác thích hợp. Đương nhiên, địa chỉ được cung cấp là vị trí trong Vùng lưu đăng ký nơi chuyển trở lại chương trình của người dùng đã được thực hiện bởi lệnh gọi hệ thống trước đó.
- Trong khi thực hiện lệnh gọi hệ thống thứ hai, quyền điều khiển được trả lại ở trạng thái điều khiển/giám sát cho người dùng, cho phép người dùng kiểm soát hệ thống.

3.2 Xác thực không đồng nhất

Việc có nhiều định nghĩa của cùng một cấu trúc trong một hệ điều hành, thì sẽ có khả năng xảy ra mâu thuẫn giữa các định nghĩa này, việc đó sẽ tạo ra một lỗ hổng bảo mật. Lỗi này vượt ra ngoài lỗi xác thực thông số không đầy đủ. Một trường hợp có thể tồn tại trong đó mỗi quy trình của một số chương trình điều khiển sẽ kiểm tra hoàn toàn các điều kiện mà nó cho là hợp lệ; tuy nhiên, nhiều bộ tiêu chí không hoàn toàn nhất quán với nhau.

Một ví dụ về loại lỗ hổng này:

Hệ điều hành duy trì các thư mục (ví dụ: danh mục) của các tệp dữ liệu được sử dụng bởi hệ thống và người dùng. Nội dung của các thư mục này thường được truy cập bởi nhiều chương trình. Mỗi chương trình này quy chuẩn riêng về cách tạo thành một điều kiện hợp lệ trong hệ thống tệp.

Hãy xem xét điều gì đó cơ bản như các ký tự trong các tham số đại diện cho (các) tên của người dùng được cấp quyền truy cập tệp. Quy trình tạo mục nhập chỉ mục-tệp-chính có thể chấp nhận một ký tự (chẳng hạn như một ô trống được nhúng) là hợp lệ trong một tên quyền cụ thể; trong khi tất cả các chương trình giao diện khác sửa đổi/xóa các mục nhập chính tệp chỉ mục giả định các khoảng trống sẽ không bao giờ hợp lệ và do đó không chấp nhận chúng. Trong các điều kiện như vậy, các quyền đối với tệp cụ thể có thể được tạo (chẳng hạn như quyền truy cập được chia sẻ vào tệp) mà sau đó không thể bị xóa.

3.3 Chia sẻ ngầm dữ liệu quan trọng

Để đảm bảo tính toàn vẹn, hệ điều hành phải có khả năng cô lập từng người dùng với tất cả những người khác và với chương trình điều khiển. Sự cô lập này liên quan đến các luồng điều khiển và thông tin. Bất cứ khi nào việc cô lập các thông tin không hoàn thiện, hệ thống có thể cho phép người dùng có đặc quyền cao hơn truy cập thông tin có đặc quyền thấp hơn hoặc có thể cho phép một người dùng truy cập thông tin của người dùng khác theo mong muốn của người dùng đó.

Trong nhiều hệ điều hành, phần điều khiển/chương trình của hệ điều hành chia sẻ không gian bộ nhớ với các chương trình người dùng, dưới dạng không gian làm việc hoặc là nơi thuận tiện để đưa thông tin liên quan đến chương trình người dùng đó. Đây là một chính sách thiết kế có chủ ý nhằm tạo điều kiện cho người dùng cá nhân hoá cho các tài nguyên mà họ sử dụng. Nếu người dùng yêu cầu hoạt động tệp hoặc các loại tài nguyên hệ thống khác, hệ thống sẽ duy trì thông tin và không gian làm việc cho yêu cầu của người dùng trong một khu vực. Bởi vì không gian làm việc được chia sẻ, nhưng ở một chế độ không có sẵn cho người dùng, những người triển khai hệ điều hành thường bất cẩn đối với trạng thái mà không gian làm việc còn lại sau khi nhận được yêu cầu của người dùng.

Ví dụ: chương trình điều khiển có thể sử dụng không gian làm việc như vậy để đọc trong chỉ mục chính của tệp người dùng cùng với mật khẩu được liên kết của họ như một phần của tìm kiếm dữ liệu do một người dùng nhất định yêu cầu. Chức năng này là cần thiết để hệ thống xác định rằng yêu cầu được hình thành đúng cách và được cấp quyền cho người dùng thực hiện yêu cầu. Nếu chương trình điều khiển thấy rằng yêu cầu không đúng, nó sẽ trả lại quyền điều khiển cho chương trình người dùng bắt nguồn yêu cầu, với dấu hiệu của lỗi trong yêu cầu. Tuy nhiên, trong ví dụ này, chương trình điều khiển không làm gì với thông tin còn lại trong không gian làm việc được chia sẻ. Do đó, người dùng giờ đây có thể truy cập không gian làm việc và lấy từ đó các mã định danh và mật khẩu mà sau đó có thể sử dụng để giả mạo vào hệ thống. Như được hiển thị bên dưới, ngay cả khi hệ thống xóa thông tin trước khi trả lại quyền kiểm soát cho chương trình của người dùng, người dùng có thể lấy thông tin thông qua một số hình thức xử lý đồng thời, chẳng hạn như thao tác I/O độc lập đọc từ không gian làm việc được đề cập. Có những biến thể khác của lỗ hổng này. Đôi khi các tệp công việc và không gian làm việc không bị xóa khi người dùng giải phóng chúng và người dùng khác có thể quét "bảng đen chưa được xóa" này khi không gian tệp hoặc không gian tạm thời chưa thể xóa được chỉ định tiếp theo.

Đôi khi các tác động đầy đủ của thông tin cung cấp cho người dùng không được các nhà thiết kế của hệ thống nhận ra. Ví dụ: các chương trình điều khiển thường xuyên xác nhận việc xử lý các yêu cầu dịch vụ của người dùng bằng cách đặt mã báo cáo lại/cờ trạng thái. Các điều kiện trả lại khác nhau (chẳng hạn như: "illegal parameter", "segment error", "password OK", v.v.) và các hình thức giao tiếp giữa các quá trình khác (ví dụ: xác nhận GỬI/NHẬN) có thể biểu thị thông báo cho phép người dùng bảo mật chặt chẽ.

3.4 Xác thực bất đồng bộ

Tính toàn vẹn của hệ thống yêu cầu duy trì tính toàn vẹn của thông tin được truyền giữa các quá trình hợp tác hoặc trình tự chương trình điều khiển. Nếu tuần tự hóa không được thực thi trong cửa sổ thời gian giữa việc lưu trữ giá trị dữ liệu và tham chiếu của nó (hoặc giữa hai tham chiếu tuần tự), thì tính nhất quán của giá trị dữ liệu đó có thể bị phá hủy bởi một quy trình không đồng bộ.

Thông tin kiểm soát đặc biệt dễ bị sửa đổi bất cứ khi nào nó được đặt trong bộ nhớ mà quy trình cấp dưới có thể truy cập được. Đây đôi khi được gọi là vấn đề "kiểm tra thời gian sử dụng". Như được mô tả trong phần ngụ ý chia sẻ lỗ hổng dữ liệu đặc quyền, một hệ điều hành có thể thường xuyên chia sẻ không gian bộ nhớ với các chương trình người dùng. Không gian này có thể không chỉ được sử dụng để lưu trữ thông tin một cách thụ động mà còn có thể chứa các thông số hệ thống hoặc người dùng đại diện cho dữ liệu mà các hành động trong tương lai sẽ dựa trên đó. Bất cứ khi nào có "cửa sổ thời gian" giữa thời gian chương trình điều khiển xác minh một tham số và thời gian nó truy xuất tham số từ bộ nhớ dùng chung để sử dụng, một lỗ hổng bảo mật tiềm ẩn sẽ được tạo ra. Điều này là do các hệ điều hành hiện đại cho phép người dùng có hai hoặc nhiều hoạt động (quy trình) thực thi đồng thời và chia sẻ phân bổ bộ nhớ của người dùng đó. Ví dụ: người dùng có thể bắt đầu thao tác I/O và sau đó tiếp tục thực hiện chương trình của mình trong khi thao tác I/O hoàn tất.

Trong một ví dụ khác, người dùng chia sẻ thời gian có thể tạm thời tạm dừng một hoạt động bằng cách nhấn phím "chú ý" hoặc xác nhận tiêu cực (NAK) trên thiết bị đầu cuối của họ, thực hiện thao tác thứ hai, sau đó trả lại quyền điều khiển cho thao tác đầu tiên để hoàn thành. Một số hệ thống cho phép "đa nhiệm", trong đó hai hoặc nhiều chương trình đang chia sẻ bộ nhớ được chỉ định của một người dùng (không gian a-ddress) và đang thực thi đồng thời —có thể mỗi chương trình được thực thi đồng thời bởi CPU riêng biệt của một hệ thống máy tính đa xử lý.

Dưới đây là kịch bản một ví dụ về việc xác thực bất đồng bộ:

- Trong khung thời gian 1, người dùng đưa ra yêu cầu I/O cho chương trình điều khiển. Chương trình điều khiển xác nhận tất cả các tham số I/O (bao gồm cả con trỏ địa chỉ tới bộ đệm hợp lệ trong bộ nhớ được gán hợp pháp cho người dùng), xếp hàng yêu cầu I/O [phải đợi cho đến khi thiết bị thích hợp không còn bận), và sau đó trả lại quyền kiểm soát cho người dùng.
- Trong khung thời gian 2, người dùng thay thế con trỏ địa chỉ hợp lệ tới bộ đệm của mình bằng một địa chỉ trỏ đến một vị trí trong chương trình điều khiển.
- Khi I/O đang thực hiện trong khung thời gian 3, dữ liệu mà người dùng yêu cầu sẽ được đọc vào (hoặc ra khỏi) chương trình điều khiển thay vì bộ đệm hợp lệ của anh ta. Do đó, các hướng dẫn trong chương trình điều khiển có

thể được phủ lên với các hướng dẫn do người dùng cung cấp hoặc thông tin về chương trình điều khiển đặc quyền có thể được đọc ra tệp của người dùng.

Trong một số hệ thống, chương trình điều khiển có thể sử dụng vùng lưu thanh ghi tràn, nằm trong vùng lưu trữ có thể truy cập của người dùng, bất cứ khi nào vùng lưu chính của chương trình điều khiển được lấp đầy. Thông tin đã lưu này thường chứa trạng thái chương trình và thông tin điều khiển.

Tình huống này có thể làm phát sinh một biến thể khác của lỗi xác thực không đồng bộ, nếu người dùng có thể sửa đổi thông tin điều khiển đó. Một ví dụ về nỗ lực thâm nhập như vậy như sau:

- Người dùng tạo một bản ghi I/O chỉ chứa một địa chỉ trỏ đến một vị trí mong muốn trong một trong các chương trình của người dùng.
- Sau đó, nhiều bản sao của bản ghi này sẽ được xuất ra dưới dạng tệp.
- Người dùng tiếp theo bắt đầu thao tác I/O để đọc các bản ghi này lặp đi lặp lại vào khu vực bộ nhớ của người dùng được chương trình điều khiển sử dụng làm bộ nhớ tràn cho các thanh ghi.
- Sau đó, người dùng đưa ra một yêu cầu dịch vụ hệ thống khiến chương trình điều khiển thực hiện một số lệnh gọi nội bộ màn hình lồng nhau, do đó làm tràn vùng lưu chính của nó. [Việc phát hành lặp lại các yêu cầu dịch vụ nhất định cũng có thể đạt được mục đích này.)
- Các thanh ghi được lưu bởi chương trình điều khiển trong vùng lưu tràn sẽ được phủ lên bởi các bản ghi đầu vào có chứa địa chỉ trỏ đến mã của người dùng. (Người dùng có thể cần một số điều chỉnh về thời gian để thực hiện điều này.)
- Khi chương trình điều khiển cuối cùng khôi phục các thanh ghi và trạng thái từ vùng tràn, nó sẽ chuyển quyền điều khiển sang chương trình của người dùng ở trạng thái giám sát/điều khiển - do đó cho phép người dùng toàn quyền kiểm soát hệ điều hành.

Hệ điều hành có thể lưu trữ thông tin trong một khoảng thời gian trong bộ nhớ phụ dùng chung cũng như trong bộ nhớ chính. Ví dụ: một hệ điều hành có thể có cung cấp điểm kiểm tra/khởi động lại để ghi lại trạng thái của một chương trình đang chạy

tại các điểm khởi động lại thuận tiện dưới dạng kết xuất "điểm kiểm tra". Các kết xuất điểm kiểm tra này chứa cả dữ liệu người dùng và thông tin điều khiển chỉ định trạng thái điều khiển sẽ được chỉ định nếu chương trình được khởi động lại. Các kết xuất điểm kiểm tra được người dùng ghi lại trong một tệp được chỉ định cho hệ thống và người dùng đó có thể truy cập để thao tác. Thông qua thao tác như vậy, người dùng có thể khiến chương trình của mình được khởi động lại với thông tin trạng thái đã sửa đổi mang lại cho chương trình của anh ta các đặc quyền lớn hơn so với quy định ban đầu. Ví dụ, điều này có thể dẫn đến việc người dùng giành được quyền kiểm soát/giám sát trạng thái.

3.5 Nhận dạng/ Xác thực/ Uỷ quyền không đầy đủ

Nhận dạng, ủy quyền và xác thực là các thành phần thiết yếu của khái niệm truy cập có kiểm soát. Sự ủy quyền — bản quyền truy cập được kiểm soát — đa phần dựa trên nhận dạng duy nhất, được xác thực của các cá nhân và tài nguyên. Một hệ điều hành về cơ bản là một trình quản lý tài nguyên. Do đó, một hệ điều hành phải đối mặt với các vấn đề về tính toàn vẹn bất cứ khi nào 1) nó không yêu cầu ủy quyền cho một cá nhân hoặc quy trình để truy cập vào bất kỳ dữ liệu nào hoặc sử dụng bất kỳ tài nguyên nào không phải có sẵn cho tất cả, hoặc 2) nó không xác định duy nhất các tài nguyên mà nó đang giải quyết.

Một lỗ hổng được tạo ra bất cứ khi nào hệ thống cho phép người dùng sở hữu một tập hợp các đặc quyền/khả năng bỏ qua hợp pháp các cơ chế bảo mật (truy cập có kiểm soát) và thực hiện một hành động chỉ được phép đối với những người dùng có các đặc quyền/khả năng khác nhau hoặc bất cứ khi nào nó cho phép tất cả người dùng thực hiện một hành động chỉ nên bị hạn chế đối với những người dùng có đặc quyền lớn hơn.

Một lỗ hổng nhận dạng/cách ly không đầy đủ có thể được tạo ra bất cứ khi nào một quy trình hệ thống dựa vào các cơ chế (được thực hiện ở nơi khác trong hệ thống) để đảm bảo sự cô lập của các tài nguyên hệ thống và do đó, tính đầy đủ của việc nhận dạng chúng. Đây có thể là một chính sách tồi nếu trên thực tế, các cơ chế không phù hợp.

Ví dụ, để được xác định duy nhất một chương trình phải được xác định bằng cả tên chương trình và tên của thư viện mà từ đó nó được tải. Nếu không, người dùng rất dễ tải trước một chương trình giả mạo có tên giống với một số quy trình chương trình điều khiển (phải được tải động khi cần thiết) và quy trình giả mạo này được chương trình điều khiển sử dụng thay cho quy trình xác thực .

Để thực hiện điều này, người dùng tạo một hoạt động dẫn đến chương trình điều khiển yêu cầu lại quy trình này. Trình tải sẽ thấy rằng quy trình được đặt tên (giả mạo) đã được tải (hợp pháp) và sẽ thiết lập chương trình kiểm soát để sử dụng chương trình giả mạo.

Ví dụ khác, cơ chế kiểm tra mật khẩu hoặc ID người dùng có thể bị phá vỡ nếu nó không giới hạn hiệu quả số lần người dùng có thể cố gắng đăng nhập vào hệ thống hoặc nếu nó không giới hạn thời gian đã trôi qua được phép hoàn tất đăng nhập. Trong những trường hợp như vậy, người dùng có thể sử dụng một máy tính khác để liệt kê đầy đủ tất cả các tổ hợp bit mật khẩu và do đó phá vỡ tính bảo mật của mật khẩu.

Một số hệ thống có tính năng kiểm tra ủy quyền mở rộng được liên kết với hầu hết, nhưng không phải tất cả, các phương thức truy cập tệp và không hạn chế việc sử dụng các phương thức truy cập không thực hiện kiểm tra ủy quyền. Bất kỳ người dùng nào có được tài liệu cho các phương pháp truy cập sau này (khả năng không cần thiết) chỉ cần sử dụng chúng để truy cập vào bất kỳ tệp nào trong hệ thống. Đây là một ví dụ về việc bỏ qua các cơ chế truy cập được kiểm soát.

Bảng 3-6 tóm tắt các danh mục và trình bày các ngoại lệ bổ sung của lỗ hổng nhận dạng, ủy quyền và xác thực không đầy đủ.

3.6 Vi phạm giới hạn

Hệ điều hành được mô tả bằng cả cách thể hiện của nó trong hướng dẫn máy tính và bằng tài liệu bên ngoài của nó. Bất cứ khi nào hai mô tả này khác nhau, một lỗ hổng toàn vẹn có thể tồn tại. Một lỗ hổng bảo mật được tạo ra bất cứ khi nào giới hạn hệ điều hành được lập thành văn bản hoặc quy trình cấm theo quy trình không được thực thi.

Ví dụ: những người triển khai hệ điều hành không được xử lý tình huống đạt đến giới hạn trên về kích thước của bảng hoặc bộ đệm hoặc khi không gian hàng đợi

trở nên bão hòa. Tài liệu có thể chỉ định chính xác các giới hạn trên và cấm vượt quá giới hạn, nhưng nếu người dùng cố tình hoặc vô tình gây ra tràn hoặc quá tải, thì các kết quả khác nhau có thể xảy ra - đôi khi có thể xảy ra sự cố hệ thống, đôi khi hoạt động của hệ thống bị suy giảm dữ liệu nhạy cảm có thể bị mất và trong một số trường hợp, dữ liệu đó có thể bị xâm phạm.

3.7 Lỗi logic

Trong bất kỳ hệ điều hành chính nào, đều có - tại bất kỳ thời điểm nào - một số "lỗi" hoặc lỗi logic. Nhiều lỗi trong số này phụ thuộc vào các tình huống thời gian không thể thống kê được và không nằm trong tầm kiểm soát của bất kỳ người dùng cá nhân nào. Tuy nhiên, một số lỗi logic này có thể bị người dùng cố ý khai thác để làm tổn hại đến tính toàn vẹn của hệ thống.

Một ví dụ liên quan đến việc xử lý lỗi không chính xác. Ví dụ, hệ thống có thể thực hiện một hành động bất hợp pháp trước khi báo hiệu một điều kiện lỗi. Ví dụ, hãy xem xét rằng một người dùng yêu cầu một loạt các sửa đổi được thực hiện đối với mục nhập thư mục tệp của một người dùng khác, mà người dùng đầu tiên có quyền chỉ đọc. Nếu hệ thống thực hiện các hành động được yêu cầu và sau đó xác định rằng các hành động vượt quá sự cho phép của người dùng yêu cầu, thì tính bảo mật của hệ thống đã bị xâm phạm thông qua một lỗi logic. Điều này cũng có thể xảy ra nếu một dịch vụ hệ thống như kết xuất bộ nhớ được khởi tạo đồng thời với việc kiểm tra ủy quyền của người dùng để yêu cầu dịch vụ được chỉ định cho các khu vực lưu trữ được chỉ định. Vào thời điểm lỗi được phát hiện, các khu vực cấm có thể đã được liệt kê.

Ở mức độ tinh tế hơn, người dùng có thể phát hiện ra rằng các hướng dẫn số học nửa từ được sử dụng để xử lý không đúng tham số địa chỉ trả lại nửa từ. Nếu số nửa từ lớn nhất có thể được sử dụng làm địa chỉ, có thể xảy ra hiện tượng tràn không lường trước được, dẫn đến địa chỉ trỏ đến vị trí 0001 trong bộ nhớ chương trình điều khiển, điều này có thể gây ra sự cố hệ thống.

Trong một tình huống khác, bằng cách nhấn vào nút ngắt "chú ý" (hoặc NAK) trên thiết bị đầu cuối của anh ấy trong quá trình in thông báo lỗi đăng nhập, người dùng có thể khiến hệ thống chấp nhận sai một nỗ lực đăng nhập mới mà không tiến bộ đếm được đặt thành ghi lại số lần đăng nhập trước đó. Lỗi hệ thống này cho phép tự

động hóa việc liệt kê đầy đủ các mật khẩu, không có dấu hiệu cho người vận hành hệ thống biết rằng điều này đang diễn ra.

Trong một ví dụ cuối cùng về xử lý lỗi không chính xác, đôi khi xảy ra trường hợp cơ chế bảo vệ bị vô hiệu hóa hoặc sửa đổi do lỗi người dùng (cố ý) và không thể đặt lại khi chương trình điều khiển sau đó trả lại quyền điều khiển cho người dùng. Điều này có thể dẫn đến việc người dùng nhận được các đặc quyền trái phép.

Có thêm hai loại lỗi logic có thể khai thác. Những điều này được liệt kê ở đây cho đầy đủ và không có ví dụ:

- Bắt đầu hoặc kết thúc quá trình/chức năng không chính xác.
- Bẫy lỗi phần mềm trạng thái kiểm soát.

KẾT LUẬN

Kết luận chung

Các vấn đề liên quan đến tính toàn vẹn là một trong những vấn đề cực kì quan trọng trong triển khai và vận hành hệ thống. Một mắc xích trong hệ thống không đảm bảo được tính toàn vẹn có thể gây ra sự thiếu đồng nhất, gián đoạn hay nguy hiểm hơn là sự sụp đổ của cả hệ thống ấy. Việc đảm bảo tình toàn vẹn cần phải xem xét từ nhiều khía cạnh như các khía cạnh khách quan và chủ quan, khía cạnh người dùng và người cung cấp dịch vụ, khía cạnh của nhà cung ứng với dữ liệu được cung cấp. Các dữ liệu là điều tất yếu cần đến sự đảm bảo tính toàn vẹn. Nhưng như đề cập trong đồ án, việc khai thác còn có thể dựa vào những tác nhân vật lý có thể do các lỗ hổng trong chính sách, có thể khiến thay đổi các thiết bị vật lý, thay đổi được những điều tưởng chừng như không có ảnh hưởng nhiều, nhưng khi suy xét kĩ lưỡng thì nó là một vấn đề cực kì lớn, có thể phá huỷ nếu không có các phương án đề phòng và có một chính sách chặt chẽ.

Với thời gian và kinh nghiệm còn hạn chế, nhiều vấn đề còn chưa được đưa ra, chưa có sự cụ thể và mang tính chất thực tế hay chi tiết cho từng trường hợp. Nhưng đồ án đáp ứng được yêu cầu ban đầu đưa ra. Đồ án có thể đảm bảo được những thông tin đưa ra đủ để có thể giúp khái quát nhiều khái niệm và các thông tin quan trọng trong vấn đề lỗ hổng toàn vẹn (Integrity Flaws), hay chi tiết và các ví dụ kèm theo phù hợp với nội dung được đề cập tới.

TÀI LIỆU THAM KHẢO

[1] Security Analysis and Enhancements of Computer Operating Systems.
[2] Operating System Integrity.