3. Sự chuyển động

Một số lượng lớn các vi phạm an ninh được thực hiện bằng cách khai thác phần mềm tận dụng những điểm yếu hiện diện trong mã “đáng tin cậy”. Ở phần này, chúng tôi minh họa cách một lỗ hổng đơn giản trong một chương trình ứng dụng thông thường có thể được khai thác để đạt được tác dụng phụ không mong muốn, chẳng hạn như việc thực hiện các mã độc tùy ý, thúc đẩy nhu cầu về các giải pháp như một trong những đề xuất trong bài báo này.

Chúng tôi xem xét một chương trình mà là một phần của một tiện ích chuyển đổi định dạng âm thanh phổ biến, được gọi là SOX (Sound eXchange) toolkit. Hình. 1(a) trình bày một đoạn mã từ một tệp tin có chứa các chức năng liên quan đến việc đọc và viết của tệp tin “wav”. Chức năng *st wavstartread* được hiển thị trong hình 1(a) đọc byte len từ một đầu vào của 1 tệp tin vào một mảng ký tự, nơi tham số len được đọc từ tiêu đề tệp tin. Hình 1(b) cho thấy cách bố trí của khung stack cho chức năng st wavstartread(),khi hàm được gọi trong khi chương trình thực hiện. Stack frame chứa các bản sao của các đối số của hàm, địa chỉ trả lại trong hàm gọi đến, cũng như không gian lưu trữ cho các biến địa phương như các chuỗi ký tự. Để thực hiện một khai thác thành công, kẻ tấn công đã tạo ra một tệp tin wav đầu vào có chứa một mã nguồn mã độc và một giá trị lớn của len (len > 256). Khi chương trình được thực thi với tệp tin mã độc cài vào, nó gây ra tràn bộ nhớ đệm chuỗi ký tự, dẫn đến tham nhũng của các biến địa phương và địa chỉ trả về của hàm được lưu trữ trên các chương trình ngăn xếp. Khi chức năng st wavstartread() trở về, chương trình chuyển hướng đến địa chỉ kẻ tấn công. Thông qua việc xây dựng tệp tin đầu vào, kẻ tấn công có thể dễ dàng được thực hiện khởi động lệnh mã độc để tấn công.

Trong khi các lỗ hổng trong ví dụ trên là một thiếu xác nhận đầu vào, các lỗ hổng trong các chương trình lớn, phức tạp có thể được nhiều hơn nữa và khó hơn nữa trong việc phát hiện. Nhiều biến thể tương tự như khai thác (quay trở lại-thành-libc, định dạng chuỗi cuộc tấn công, đống overﬂow) trên chương trình securitycritical đã được báo cáo trong các tài liệu [3], [5]. Bên cạnh đó, hệ thống nhúng cũng rất dễ bị tấn công vật lý có liên quan đến giả mạo với thuộc tính hệ thống như cấp điện áp, tần số đồng hồ, và nội dung bộ nhớ. Không phụ thuộc vào cách họ có nguồn gốc, hầu hết các cuộc tấn công cuối cùng tự biểu hiện như một hành động nhằm lật đổ thực hiện chương trình “bình thường” - vi phạm kiểm soát đến hành vi, thực hiện các trình tự hướng dẫn hỏng v.v. Thay vì cố gắng để ngăn chặn tất cả các nguồn tấn công, chúng tôi tập trung vào de fi ning cho phép hành vi chương trình và chương trình giám sát thực hiện để nắm bắt những quang sai. Tuy nhiên, chi phí của việc theo dõi thực hiện làm cho một giải pháp dựa trên phần mềm không khả thi, và trình bày một trường hợp thuyết phục cho việc thiết kế một cách hiệu quả, theo dõi thời gian chạy phần cứng hỗ trợ.

4. HỖ TRỢ GIÁM SÁT KIẾN TRÚC PHẦN CỨNG

Trong phần này, chúng tôi cung cấp một cái nhìn tổng quan về kiến ​​trúc giám sát phần cứng. Sau đó chúng tôi mô tả một cách chi tiết các thuộc tính mà mô hình cho phép chương trình hành vi và thiết kế của màn hình phần cứng tương ứng mà kiểm tra.

1. Kiến trúc Tổng quan

Hình. 2 cho thấy sơ đồ khối khái niệm về kiến ​​trúc giám sát phần cứng hỗ trợ được đề xuất. Để dễ dàng minh hoạ, chúng tôi mô tả các bộ xử lý nhúng như một trong trật tự năm giai đoạn pipeline. Các yếu tố đầu vào màn hình bao gồm bộ đếm chương trình (PC) và đăng ký chỉ dẫn (IR) của hướng dẫn hoàn thành, và tình trạng đường ống từ các đơn vị kiểm soát pipeline. Một cách hiệu quả, giám sát được cung cấp với một dấu vết chu kỳ bằng chu kỳ của các hướng dẫn thực hiện và địa chỉ chương trình của họ. Kết quả đầu ra của màn hình bao gồm một tín hiệu ngăn và một tín hiệu không hợp lệ. Khi màn hình phát hiện vi phạm hành vi chương trình cho phép, nó khẳng định tín hiệu không hợp lệ, mà kết quả trong một ngắt không thể che giấu đến bộ vi xử lý. Tín hiệu này có thể được sử dụng để kích hoạt một cơ chế phản ứng, chẳng hạn như chấm dứt chương trình hoặc chuyển nhượng bộ vi xử lý với một chế độ an toàn.