Fraunhofer AISEC

Làm sáng tỏ quá nhiều về bảo vệ phần sụn của vi điều khiển

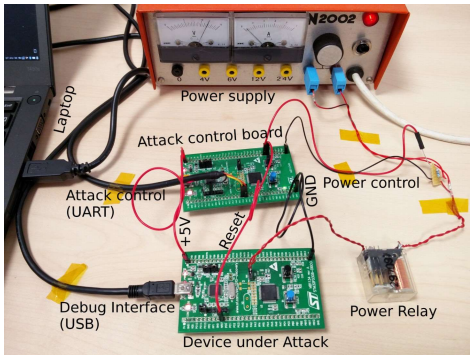
Làm sáng tỏ quá nhiều về bảo vệ phần sụn của vi điều khiển

Kỷ yếu của Hội thảo USENIX lần thứ 11 về Công nghệ tấn công (WOOT '17) - Vancouver, BC, Canada số CVE 2017-18347

Hầu hết mọi bộ vi điều khiển có đèn flash tích hợp đều có tính năng bảo vệ phần sụn đọc ra. Đây là một hình thức bảo vệ nội dung nhằm bảo vệ quyền sở hữu trí tuệ (IP) cũng như các khóa và thuật toán mật mã khỏi kẻ thù. Một loạt các bộ vi điều khiển là STM32 gần đây đã trở nên phổ biến và do đó ngày càng bị tấn công. Tuy nhiên, không có kinh nghiệm thực tế và thông tin nào về khả năng phục hồi của bộ vi điều khiển STM32 được công khai. Bài báo trình bày cuộc điều tra đầu tiên về khái niệm bảo mật STM32, đặc biệt nhắm mục tiêu vào chuỗi con STM32F0. Bắt đầu với phân tích khái niệm, chúng tôi phát hiện ra ba điểm yếu và phát triển chúng thành các lỗ hổng bằng cách trình bày Bằng chứng về khái niệm tương ứng. Lúc đầu, chúng tôi phát hiện ra rằng một cấu hình bảo mật phổ biến cung cấp khả năng bảo vệ thấp. Cấu hình này có thể bị khai thác bằng cách sử dụng phương pháp Bước khởi động nguội của chúng tôi để trích xuất dữ liệu quan trọng hoặc thậm chí cả chương trình cơ sở được bảo vệ bằng cách đọc ra. Thứ hai, chúng tôi tiết lộ một điểm yếu về thiết kế trong bộ lưu trữ cấu hình bảo mật cho phép kẻ tấn công hạ cấp mức độ bảo vệ phần sụn, do đó kích hoạt các cuộc tấn công bổ sung. Thứ ba, chúng tôi phát hiện và phân

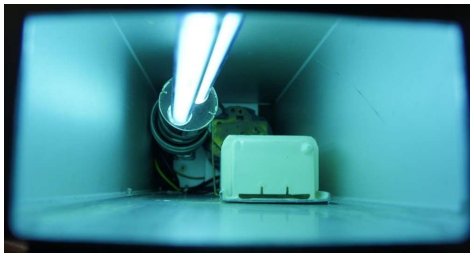
tích một lỗ hổng phần cứng trong giao diện gỡ lỗi, được quy cho một điều kiện chạy đua, cho phép chúng tôi trích xuất trực tiếp chương trình cơ sở được bảo vệ bằng cách sử dụng phương pháp lặp lại. Mỗi cuộc tấn công chỉ yêu cầu thiết bị giá rẻ, do đó làm tăng tác động của từng điểm yếu và dẫn đến một mối đe dọa nghiêm trọng hoàn toàn. chúng tôi tiết lộ một điểm yếu về thiết kế trong bộ lưu trữ cấu hình bảo mật cho phép kẻ tấn công hạ cấp mức độ bảo vệ phần sụn, do đó kích hoạt các cuộc tấn công bổ sung. Thứ ba, chúng tôi phát hiện và phân tích một lỗ hổng phần cứng trong giao diện gỡ lỗi, được quy cho một điều kiện chạy đua, cho phép chúng tôi trích xuất trực tiếp chương trình cơ sở được bảo vệ bằng cách sử dụng phương pháp lặp lại. Mỗi cuộc tấn công chỉ yêu cầu thiết bị giá rẻ, do đó làm tăng tác động của từng điểm yếu và dẫn đến một mối đe dọa nghiêm trọng hoàn toàn. chúng tôi tiết lộ một điểm yếu về thiết kế trong bộ lưu trữ cấu hình bảo mật, cho phép kẻ tấn công hạ cấp mức độ bảo vệ phần sụn, do đó kích hoạt các cuộc tấn công bổ sung. Thứ ba, chúng tôi phát hiện và phân tích một lỗ hổng phần cứng trong giao diện gỡ lỗi, được quy cho một điều kiện chạy đua, cho phép chúng tôi trích xuất trực tiếp chương trình cơ sở được bảo vệ bằng cách sử dụng phương pháp lặp lại. Mỗi cuộc tấn công chỉ yêu cầu thiết bị giá rẻ, do đó làm tăng tác động của từng điểm yếu và dẫn đến một mối đe dọa nghiêm trọng hoàn toàn.

Thiết lập phòng thí nghiệm cho Bước khởi động nguội



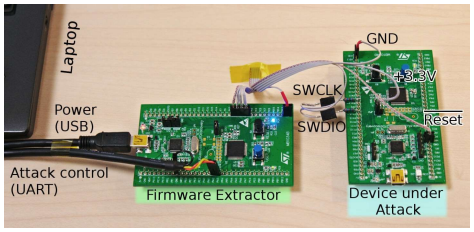
Bằng cách quan sát các thay đổi trong SRAM, người ta có thể thiết kế ngược luồng điều khiển cơ bản, tìm hiểu cách sử dụng các địa chỉ cụ thể và cũng có thể khám phá dữ liệu bí mật có thể nhìn thấy trong thời gian ngắn. Hệ thống chỉ được phép chạy trong một khoảng thời gian được kiểm soát chính xác và sau đó dừng lại. Nội dung của SRAM được đọc ra và ảnh chụp nhanh được tạo. Với thời lượng thời gian chạy được lựa chọn tốt và tăng dần, điều này tương tự như bước qua phần sụn, vì chỉ có một vài hướng dẫn được thực thi giữa mỗi ảnh chụp nhanh SRAM.

Thiết lập chiếu xạ UV-C để Hạ cấp bảo mật



Cơ chế bảo vệ Mức bảo vệ đầu đọc STM32 dựa trên các byte RDP và nRDP trong vùng bộ nhớ byte tùy chọn. Tại sự kiện bật nguồn, các byte tùy chọn được tải từ bộ nhớ flash và Mức RDP tương ứng được đặt. Bằng thực nghiệm, chúng tôi chỉ ra rằng một lỗ hổng trong quá trình triển khai sẽ phát triển thành một mối đe dọa thực tế. Vùng bộ nhớ byte tùy chọn có thể được sửa đổi cụ thể bằng ánh sáng UV-C thực hiện việc tiêm lỗi quang học.

Thiết lập để trích xuất chương trình cơ sở ra khỏi thiết bị bằng RDP Cấp 1



Bộ vi điều khiển sê-ri STM32F0 sử dụng giao diện Gỡ lỗi dây nối tiếp để gỡ lỗi và lập trình flash. Khi trình gỡ lỗi được gắn vào giao diện này trong Bảo vệ đầu đọc Cấp 1, logic bảo vệ flash sẽ cắt quyền truy cập vào bộ nhớ flash. Do điều kiện tương tranh trong quá trình triển khai, không chỉ một lần truy cập có thể được thực hiện mà toàn bộ phần sụn có thể được trích xuất từ một bộ vi điều khiển.

Liên hệ

Stefan Tatschner
nhà nghiên cứu bảo mật

Fraunhofer AISEC
Lichtenbergstrasse 11
85748 Garching b. München

stefan.tatschner@aisec.fraunhofer.de

Fraunhofer Institute for Applied and Integrated Security - Shedding too much Light on a Microcontroller's Firmware Protection

Online in Internet; URL: https://www.aisec.fraunhofer.de/en/FirmwareProtection.html

Date: 11.5.2023 17:13