

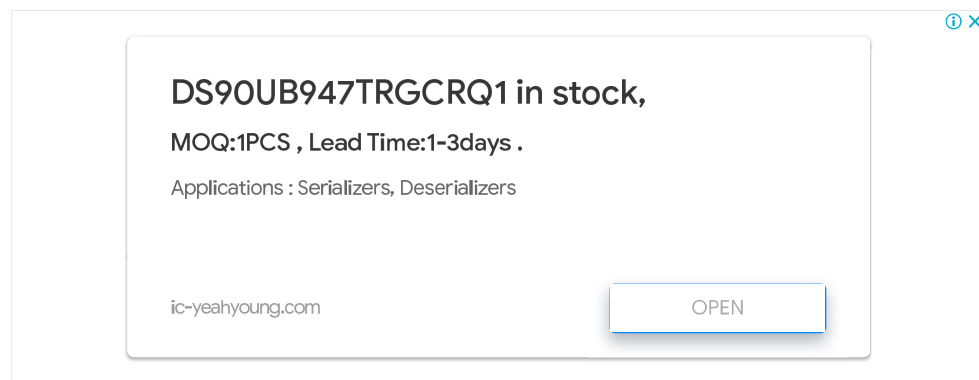


Đọc phần sụn STM32

Hầu hết mọi bộ vi điều khiển có bộ nhớ flash tích hợp đều có chức năng bảo vệ chống đọc phần sụn. Điều này được thực hiện để bảo vệ tài sản trí tuệ, khóa mật mã và thuật toán khỏi những kẻ xâm nhập. Các bộ vi điều khiển thuộc dòng STM32, đã trở nên phổ biến trong những năm gần đây, đặc biệt thường xuyên bị tấn công, tuy nhiên, không có kinh nghiệm thực tế hoặc thông tin nào liên quan đến việc bảo vệ STM32 khỏi các cuộc tấn công như vậy. Trong bài viết này, chúng tôi sẽ xem xét các hệ thống bảo vệ phần sụn sử dụng sê-ri STM32f0 làm ví dụ.

khái niệm bảo vệ

Flash Readout Protection (RDP) là thành phần bảo vệ chính có trong tất cả các dòng vi điều khiển. Nó bảo vệ phần sụn hệ thống được lưu trữ trong bộ nhớ flash bên trong không bị đọc ra ngoài. Tùy thuộc vào dòng sản phẩm, các cơ chế bổ sung như Bộ bảo vệ bộ nhớ (MPU) và các chế độ thực thi đặc quyền/không đặc quyền có thể được bao gồm. Cùng với nhau, các hệ thống này được thiết kế để tăng cường bảo mật.

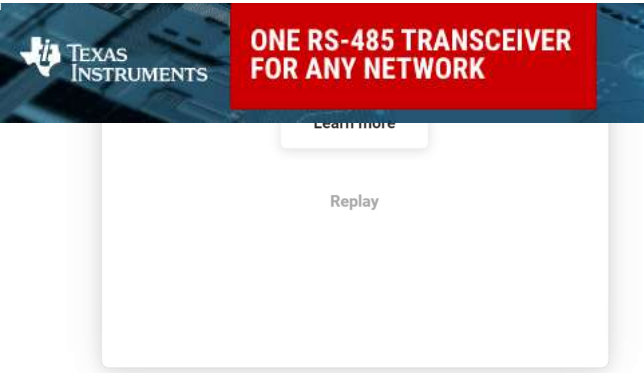


RDP có 3 cấp độ bảo vệ là RDP cấp 0, 1, 2. Độ bảo mật tăng dần theo số lượng.

RDP cấp 0: được cài đặt theo mặc định và không cung cấp tính năng bảo vệ. Sử dụng giao diện gỡ lỗi, bạn có thể có toàn quyền truy cập vào thiết bị.

PRD cấp 1: Giao diện gỡ lỗi vẫn hoạt động nhưng quyền truy cập vào flash bị hạn chế. Ngay khi giao diện gỡ lỗi được kết nối, bộ nhớ flash sẽ bị khóa. Nó không thể được đọc trực tiếp, thông qua DMA hoặc bằng cách thực hiện các hướng dẫn từ nó. Mức bảo vệ có thể được nâng lên 2 hoặc hạ xuống 0, với việc mất toàn bộ nội dung của bộ nhớ flash.

PRD cấp 2: giới hạn càng nhiều càng tốt và cung cấp mức độ bảo vệ tối đa. Giao diện gỡ lỗi bị vô hiệu hóa. Cấp độ không thể bị hạ cấp. Tuy nhiên, mặc dù mức độ bảo vệ cao nhất, mức độ 1 được sử dụng rộng rãi. Nhiều công ty chọn không chặn hoàn toàn thiết bị, giả sử khả năng sửa lỗi và trực trực, vì không thể gỡ lỗi ở cấp độ 2. Ngoài ra, dòng STM32f1 không hỗ trợ RDP cấp độ 2.



Thiết bị bảo mật RDP

Mức RDP là một phần của cấu hình hệ thống vi điều khiển, được lưu trữ trong phần byte tùy chọn chuyên dụng dưới dạng 16 bit của bộ nhớ cố định dưới dạng hai thanh ghi, RDP và nRDP. nRDP là bit bổ sung cho RDP. Dự phòng là cần thiết để bảo vệ chống lại sự thay đổi mức độ bằng cách hoán đổi một bit.

nRDP	RDP	Resulting protection
0x55	0xAA	RDP Level 0
Any other combination		RDP Level 1
0x33	0xCC	RDP Level 2

Thanh ghi cấu hình RDP

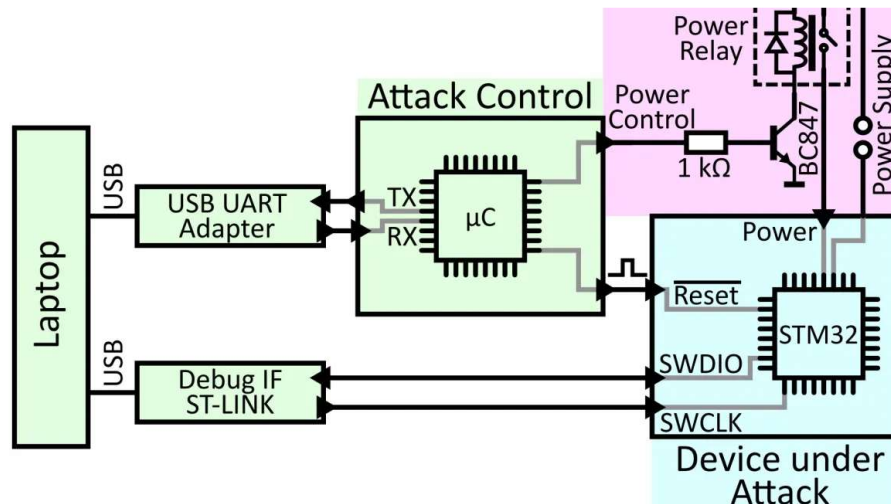
logic RDP

Theo biểu dữ liệu, có hai chế độ thực thi ở cấp độ RDP 1. Chế độ người dùng và chế độ gỡ lỗi. Ngay khi mk chuyển sang chế độ gỡ lỗi, quyền truy cập vào flash sẽ bị chặn. Đọc từ flash, theo nhà sản xuất, sẽ gây ra lỗi bus, sau đó là lỗi Hard Fault.

Cold-Boot bước tấn công

Ở chế độ RDP cấp 1, khi trình gỡ lỗi được kết nối, quyền truy cập vào bộ nhớ FLASH chỉ bị giới hạn, trong khi SRAM vẫn khả dụng. Chúng ta có thể thử trừ dữ liệu tại thời điểm nó được tải vào RAM. Các nhà phát triển thư viện mật mã đang vật lộn với lỗ hổng này. Các khóa mã hóa chỉ được lưu trữ trong SRAM trong quá trình sử dụng, tức là vài mili giây, điều này khiến cho một cuộc tấn công như vậy hầu như không thể thực hiện được, ngay cả khi chúng ta không biết về tổ chức bộ nhớ.

Để khắc phục hạn chế này, các tác giả của bài viết đã phát triển Cold-Boot Stepping (CBS), một phương pháp mà bạn có thể chụp nhanh chính xác RAM. Ý tưởng của phương pháp là đếm chính xác thời gian từ một sự kiện, chẳng hạn như RESET, và theo chu kỳ với một bước của vài chu kỳ xung nhịp để tạo ảnh chụp nhanh nội dung SRAM. Cuộc tấn công bao gồm các bước sau:



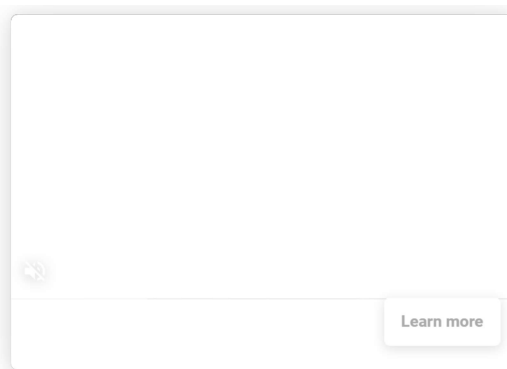
Sơ đồ cài đặt cho một cuộc tấn công CBS

1. Đặt hệ thống về trạng thái ban đầu

1. Tắt nguồn. Điều cần thiết là mk có thể đọc lại từ bộ nhớ flash.
2. Cài đặt RESET trước khi bật nguồn. Cho phép bạn khởi động hệ thống mà không cần bắt đầu thực thi mã
3. Nguồn điện được thiết lập RESET

2. Khởi chạy hệ thống theo N bước.

1. Bắt đầu thực thi mã bằng cách xóa RESET
2. Đợi cho đến khi phần sụn thực thi đạt đến vị trí đã đặt
3. Cài đặt Reset. Dừng thực thi, nhưng dữ liệu trong SRAM vẫn còn nguyên.



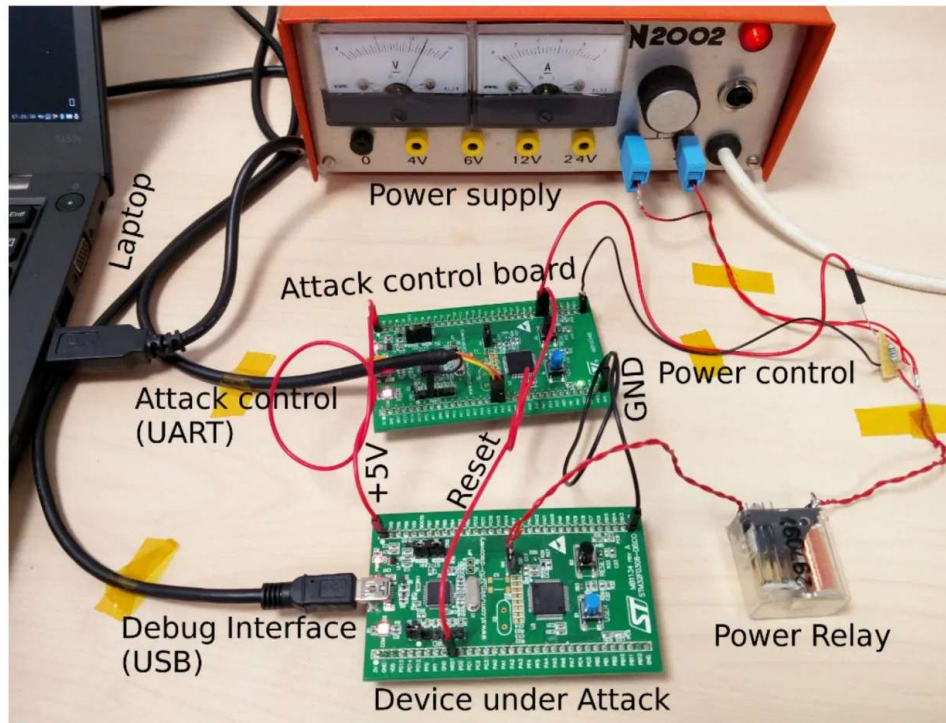
① ×

3. Đọc nội dung SRAM vào tệp

1. Kết nối trình gỡ lỗi với mk
2. Loại bỏ tín hiệu đặt lại. MK không bắt đầu thực thi mã vì nó ở trạng thái tạm dừng do trình gỡ lỗi đặt.
3. Trừ SRAM

Bằng cách lặp lại thuật toán này bao nhiêu lần tùy ý, chúng ta có thể nhận được thông tin về bối cảnh thực hiện chương trình. Để thực hiện cuộc tấn công này, cần phải kiểm soát chính xác thời

Phát triển phương pháp được mô tả, có thể tạo phương pháp trích xuất phần sụn hoàn chỉnh. Trong nhiều sản phẩm, các nhà sản xuất sử dụng bộ tải khởi động, thuật toán xác minh phần sụn dựa trên việc tính toán số lượng kiểm tra, ví dụ: CRC32, được triển khai trong một số dòng MK. Sử dụng CBS (Bước khởi động lạnh) ở giai đoạn hoạt động của bộ tải khởi động, bạn hoàn toàn có thể khôi phục phần sụn bằng cách phân tích các thanh ghi kiểm tra phần cứng về số lượng hoặc triển khai phần mềm của nó, bởi vì tại một bước nhất định, nó lưu trữ các byte của phần của phần sụn mà chúng tôi quan tâm.



Cài đặt cho một cuộc tấn công CBS

Ảnh hiển thị một bản cài đặt độc lập để giải nén phần sụn. Máy tính xách tay tự động điều chỉnh bước dựa trên thành công của bước trước đó. Đối với mk có dung lượng bộ nhớ nhỏ, ví dụ STM32F051R8T6 với tốc độ 64kb thì việc giải nén sẽ mất vài ngày.

Nó chỉ ra rằng mặc dù RDP cấp 1 cung cấp khả năng bảo vệ đọc SRAM nhưng nó vẫn có thể bị xâm phạm.

Sử dụng RDP cấp 2 cho phép bạn bảo vệ thiết bị khỏi các cuộc tấn công như vậy, một nhà sản xuất thường sử dụng RDP cấp 1. Ví dụ: trong phần mềm gỡ lỗi phổ biến, OpenOCD, chỉ cung cấp lệnh "Khóa" để bảo vệ bộ nhớ flash của thiết bị. Tuy nhiên, lệnh chỉ hỗ trợ RDP cấp 1.

Hạ cấp bảo vệ

Bây giờ chúng ta hãy xem các phương pháp hạ cấp RDP. Nhà sản xuất tuyên bố rằng cài đặt RDP cấp 2 là không thể đảo ngược. Lý tưởng nhất là chúng ta cần hạ mức 2 xuống 0, nhưng sự dư thừa của các thanh ghi RDP yêu cầu thay thế 8 bit. Để downgrade 2->1 chỉ cần thay đổi 1 bit.

00	01	0000	0000	0000	0001	
...	
33	CB	0011	0011	1100	1011	
33	CC	0011	0011	1100	1100	0
33	CD	0011	0011	1100	1101	1
...	
55	A9	0101	0101	1010	1001	
55	AA	0101	0101	1010	1010	
55	AB	0101	0101	1010	1011	
...	
FF	FE	1111	1111	1111	1110	
FF	FF	1111	1111	1111	1111	

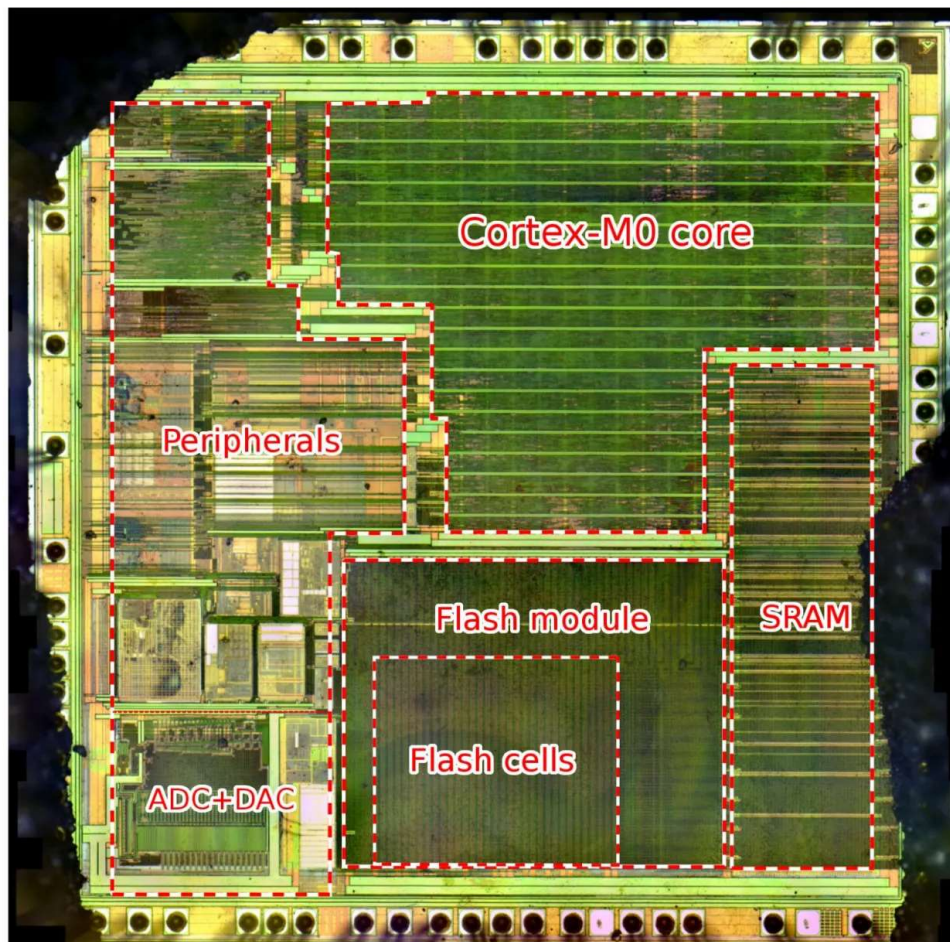
Level 2

Level 1

Level 0

Bảng ánh xạ trạng thái RDP

Bằng cách phơi sáng quang học UV-C, bit có thể được thay đổi từ "0" thành "1". Khi bức xạ 254nm chiếu vào cổng, các electron được đưa vào và trạng thái của ô logic chuyển từ 0 (đã tích điện) sang 1 (không tích điện). Trước tiên, bạn phải làm sạch tinh thể bằng phương pháp ăn mòn hóa học.



Tuy nhiên, cần phải bản địa hóa vùng của tinh thể nơi đặt các byte RDP. Nhà sản xuất không ghi lại cấu trúc bên trong của tinh thể. Hãy viết một chương trình sẽ đọc các vùng bộ nhớ và xác định xem

thêm các bit bị thay đổi nhầm.

Bảo vệ chống lại bảo vệ dưới cấp

Không có biện pháp bảo vệ chống lại việc hạ cấp RDP, nhưng bạn có thể viết chương trình của mình để trong giai đoạn khởi tạo, nó kiểm tra giá trị của các bit RDP và FLASH_OBR, lưu trữ mức bảo vệ hiện tại càng sớm càng tốt và dừng thực thi, tạo ra CBS phương pháp chiết xuất vô dụng.

Hack giao diện gỡ lỗi

Bộ vi điều khiển từ nhà sản xuất ST giả sử gỡ lỗi thông qua giao diện SWD [2]... Khi trình gỡ lỗi kết nối với MCU bằng RDP cấp 1, tính năng bảo vệ flash sẽ hạn chế quyền truy cập. Cơ chế sửa lỗi được ghi chép kém đặt ra nhiều câu hỏi và khuyến khích học hỏi.

Các tác giả của bài báo đã tạo triển khai giao diện SWD của riêng họ để nghiên cứu cách hoạt động của tính năng bảo vệ. Hóa ra, tính năng bảo vệ chỉ được kích hoạt nếu trình gỡ lỗi tương tác với bus AHB-Lite [1]... Chỉ truy cập các thanh ghi SWD, tính năng bảo vệ không được kích hoạt, nhưng ngay khi yêu cầu quyền truy cập vào các thiết bị ngoại vi, SRAM hoặc Flash mk chuyển sang chế độ gỡ lỗi và bộ nhớ flash bị chặn.

Để xác định logic của hoạt động bảo vệ, các tác giả đã giảm số lượng yêu cầu SWD xuống mức tối thiểu cần thiết để khởi tạo thành công. Trong quá trình khởi tạo, bảo vệ không được kích hoạt.

Theo tài liệu Cortex-M0 [3] hướng dẫn bộ xử lý được ưu tiên hơn giao diện gỡ lỗi. Hóa ra trình gỡ lỗi cần đợi một chu kỳ trống trên xe buýt để thực hiện yêu cầu của nó. Nếu trình gỡ lỗi giành được quyền truy cập vào bus trước khi bảo vệ bộ nhớ flash, nó sẽ có thể đọc dữ liệu từ bộ nhớ không bị khóa.

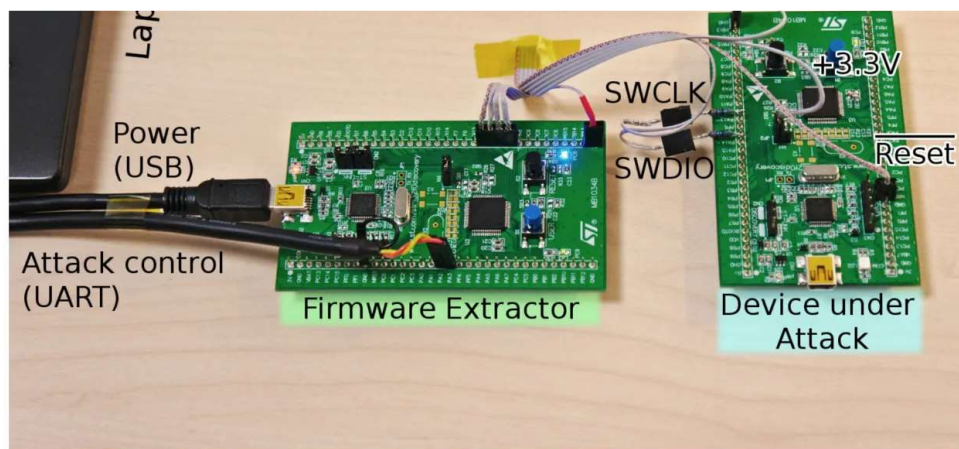
Các tác giả của bài báo đã nghiên cứu công việc bảo vệ với phần sụn mô phỏng tải trên xe buýt, bao gồm các hoạt động đọc và NOP chuyên sâu. Nếu không có hoạt động như vậy trong phần sụn, thì bộ nhớ được trình gỡ lỗi đọc sẽ mất 2 chu kỳ: phân giải địa chỉ và đọc trực tiếp. Nếu bạn thêm một thao tác NOP, thì một trong ba yêu cầu đọc sẽ không thành công. Sự phụ thuộc của xác suất đọc thành công vào số lượng thao tác NOP có thể được biểu thị bằng công thức

$$P_s = 1 - \frac{w}{2+w} = \frac{2}{2+2}$$

Sử dụng các thao tác STR làm tải sẽ cho thấy rằng chính bộ nhớ flash kiểm soát quyền truy cập. Phần sụn cũng nhấp nháy rất nhanh với đèn LED và thời điểm nó ngừng nhấp nháy cho biết bộ nhớ đã bị khóa và quá trình thực thi mã đã dừng.

Một trong những lời giải thích cho lỗi hổng này có thể là do việc triển khai phối hợp nguồn đồng hồ và phần còn lại của logic không chính xác.

Các tác giả đã trình bày một triển khai hoạt động của việc trích xuất mã bằng cách sử dụng hai STM32F0 Discovery. Dữ liệu được gửi đến PC thông qua giao diện UART và SWD được triển khai trên một trong các STM.



Cuộc tấn công bao gồm các bước sau:

1. Khởi động lại hệ thống bằng cách ngắt kết nối và cấp nguồn để thiết lập lại bảo vệ flash.
2. Khởi tạo giao diện gỡ lỗi.
3. Đặt độ dài từ gỡ lỗi thành 32 bit
4. Đặt địa chỉ đọc từ flash
5. Cố gắng đọc từ bộ nhớ
6. Đọc dữ liệu qua SWD
7. Lặp lại cho đến khi chúng tôi đọc toàn bộ bộ nhớ bằng cách tăng địa chỉ

Tốc độ đọc trung bình là khoảng 45 byte mỗi giây, giúp bạn có thể đọc được "hòn đá" dung lượng lớn nhất là 256kb trong 2 giờ. Tuy nhiên, các thử nghiệm chỉ được thực hiện trên dòng STM32F0 và người ta cho rằng do trạng thái bên trong giống nhau nên tất cả các dòng mic đều dễ bị tấn công giống nhau. Các giai đoạn khác có thể không bị ảnh hưởng.

Có thể tránh được cuộc tấn công này bằng cách sử dụng cấp độ thứ hai của RDP, nhưng như đã trình bày trước đó, cấp độ bảo vệ có thể được thay đổi. Mặc dù phương pháp CBS yêu cầu khả năng hoạt động của mã chương trình, nhưng lỗi hỏng trong trình gỡ lỗi có thể hoạt động trong trường hợp phần sụn bị hỏng khi mức RDP bị hạ xuống.

kết luận

Sê-ri MK STM32F0 chứa một số lỗ hổng cho phép phòng thí nghiệm với thiết bị cơ bản tạo bản cài đặt để đọc phần sụn. Các phương pháp có thể được kết hợp để đạt được kết quả tốt nhất hoặc chúng có thể được chạy ở mức RDP 2.

Tất cả các tài liệu cần thiết, mã nguồn và các ví dụ được cung cấp công khai bởi các tác giả của bài báo theo giấy phép MIT <https://science.obermaier-johannes.de/> ...

Bài viết gốc: [Làm sáng tỏ quá nhiều về Bảo vệ Phần sụn của Vi điều khiển | SỬ DỤNG](#)

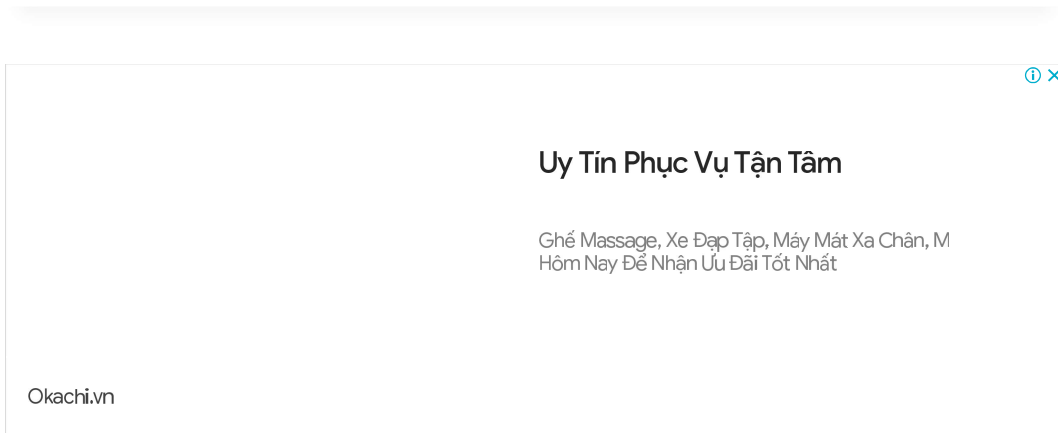
[1] CÔNG TY TNHH CÁNH TAY. Đặc tả giao thức AMBA 3 AHB-Lite v1.0, 2006.

[2] CÔNG TY TNHH CÁNH TAY. Sổ tay tham khảo kỹ thuật các thành phần CoreSight, 2009.

[3] CÔNG TY TNHH CÁNH TAY. Sổ tay Tham khảo Kỹ thuật Cortex-M0, 2009.

Shrink RS-485 designs

Ad Texas Instruments



Uy Tín Phục Vụ Tận Tâm

Ghế Massage, Xe Đạp Tập, Máy Massage Chân, Máy Massage Mặt
Hôm Nay Để Nhận Ưu Đãi Tốt Nhất

Okachi.vn

← TRƯỚC

Quảng cáo Dendy chúng tôi xứng đáng



KẾ TIẾP →

những nàng thơ mới. dụng cụ tự làm

bài viết tương tự

và sau đó quyết định tiếp
cận từ quan điểm sinh lý học
thần kinh và học cách trở
thành một huấn luyện viên

quen tự tin

Uy Tín Phục Vụ
Tận Tâm

Okachi.vn

Để lại một câu trả lời

Enter your comment here...

