**Tại sao phải bảo mật hệ thống nhúng**

Tháng 9 năm 2007, máy bay phản lực của Israel đã ném bom một cơ sở hạt nhân ở phía đông bắc Syria. Trong số những bí ẩn bao quanh cuộc tấn công đó là sự thất bại của radar Syria, để cảnh báo quân đội Syria về cuộc tấn công sắp tới. Cũng không lâu trước khi các blogger quân đội và công nghệ kết luận rằng đây là một sự cố của tác chiến điện tử chứ không phải là một loại vụ án nào. Sau khi đăng bài người ta suy đoán rằng các bộ vi xử lý ngoài thị trường trong radar Syria có thể đã được chế tạo một cách có mục đích với "backdoor " để giấu bên trong. Bằng cách gửi mã được lập trình sẵn cho các chip đó, một đối tượng vô danh đã phá hỏng chức năng của các con Chip và tạm thời chặn radar.

Nguồn: IEEE spectrum, 2007.

* “backdoor” được giấu trong chip máy tính có thể cho phép tội phạm mạng có thể điều chỉnh và kiểm soát lại các hệ thống máy tính trên máy bay Boeing 787
* The Stuxnet worm có khả năng các phần mềm độc hại đầu tiên sẽ nhắm mục tiêu trực tiếp vào các hệ thống kiểm soát quy trình nhúng
* Stuxnet xâm nhập vào các hệ thống điều khiển quá trình của Siemens tại các nhà máy hạt nhân bằng cách phá hủy các nhà khai thác máy trạm MicrosoftWindows sử dụng để định cấu hình và giám sát hệ thống điều khiển nhúng
* Mạng SCADA được điều khiển bởi các PC thông thường

**Các kiểu tấn công hệ thống nhúng**

* Tấn công phần mềm nhúng
* Tấn công phần cứng nhúng

**Phần mềm nhúng là gì ?**

* Phần mềm nhúng là phần mềm máy tính, được viết trên điều khiển máy hoặc các thiết bị
* Các thành phần phần mềm nhúng:
* Firmware
* OS
* Program or Script

**So sánh Firmware vs OS**

* Firmware:
* Để mọi thiết bị (máy in, máy quét, máy ảnh kỹ thuật số, v.v.) bắt đầu chạy thì nó cần phải có một chương trình ban đầu để chạy khi được bật/khởi động. Nó còn được gọi là bootstrap program, BIOS và được gắn trên ROM.
* Firmware được xác định vị trí hệ điều hành Kenel và tải nó vào bộ nhớ chính (RAM) tại lúc khởi động assembly hoặc C / C ++.
* Operating System:
* Một ngăn xếp phần mềm hoàn chỉnh quản lý phần cứng của nhúng và thiết lập môi trường cho các ứng dụng chạy. Nói cách khác, một hệ điều hành thực hiện nhiệm vụ được chỉ định của thiết bị. Kernel ở dưới cùng của ngăn xếp phần mềm này và tiếp tục chạy miễn là thiết bị của bạn hoạt động. Khi tôi nói Hệ điều hành quản lý phần cứng, nó thực sự là Kernel quản lý mọi yêu cầu đối với tài nguyên phần cứng (CPU, bộ nhớ, đầu vào, đầu ra).

**Embedded OS**

* Có rất nhiều hệ điều hành nhúng
* Thường là hệ điều hành thời gian thực(RTOS)
* Các hệ điều hành LynxOS, VxWorks, BeRTOS, ThreadX, sẽ sang Windows CE hoặc Linux
* Các hệ điều hành khác: OpenWrt, PikeOS, eCos, Fusion RTOS, Nucleus RTOS,RTEMS, INTEGRITY, uC/OS, QNX, FreeBSD ,Tiny OS , và OSE.

**Các tấn công phần mềm nhúng**

* Điểm yếu ở phần mềm trong hệ thống nhúng chính là các lỗ hổng bảo mật.
* Tấn công lỗ hổng filmware hoặc hệ điều hành.
* Có 3 yếu tố gây thiệt hại bảo mật trong phần mềm là:
* Complexity
* Extensibility
* Connectivity
* Complexity
* Phần mềm phức tạp
* Thêm dòng mã để tăng khả năng lỗi và lỗ hổng bảo mật
* Ngôn ngữ lập trình không an toàn khi đang được sử dụng
* C và C ++ là phổ biến nhất
* Extensibility
* Updates
* Tiện ích mở rộng
* Các hệ thống phần mềm hiện đại được thiết kế mở rộng
* Nạp thiết bị mô-đun và drivers
* Connectivity
* Các hệ thống nhúng đang được kết nối với Internet
* Có thể xảy ra lỗi dẫn đến vi phạm an ninh
* Kẻ tấn công sẽ không cần truy cập vào các hệ thống mà sử dụng các cuộc tấn công tự động.