**Động Lực**

**Tại sao bảo mật hệ thống nhúng lại quang trọng?**

* Critical Infrastructure (Nuclear power plant)
* Life Critical Systems (Pace Maker)
* Transportation systems (Flight control)
* Financial Infrastructure (Banking & Investing)
* Information systems (Patient MRI systems)
* Consumer Product (wireless routes)

**Điều gì có thể xảy ra nếu như đường bạn nhà bạn bị tấn công bởi Hacker?**

1. Hacker sẽ chiếm được quyền truy cấp cài đặt router.
2. Thay đổi cài đặt DNS trên routers
3. Router bây giờ sẽ thiết lập két nối tới hệ thống của hacker để phân tích địa chỉ tên miền
4. Tài khoản ngần hàng của bạn [www.yourbank.com](http://www.yourbank.com) sẽ được phân tích
5. Bạn nghĩ là bạn đang đăng nhập vào tài khoảng ngân hàng của chính bản thân bạn nhưng thực chất bạn đang đưa nó cho hacker
6. Pwn3d (hacker nói cho bạn biết ran82ng tài khoảng của bạn đã bị đánh cắp)

**Main takeaways**

**Tại sao bảo mạt hệ thống nhúng thì khó khăn?**

* Kinh tế / ngoại thương khuyến khích sản xuất sản phẩm có độ bảo mật kém: Thông thường người mua hàng (kể cả chuyên gia) thì không đủ khả năng phân biệt sự khác nhau về chất lượng giữa một sản phẩm bảo mật tốt và một vật vô dụng.
* Sự phực tạp phần mềm được gia tăng: sự phát triển tuyến tính trong nội dung phần cứng/phần mềm tạo ra sự phạt triển không tuyến tính ở sự phức tạp toàn bộ hệ thống . Sự phức tạp này gây ra sự thiếu sót.
* Bảo mật như một cách giải quyết muộn: Thông thường về mặt tài chính hoặc kỹ thuật điều đó là không thể trang bị thêm những sự tương tác bảo mật tới một hệ thống nhúng điều đó ngay từ đầu thì không được thiết kế.

**Làm sao chúng ta có thể giải quyết những khó khăn này?**

* Cân bằng các sự cân bằng: Tạo ra một sự cân bằng giữa sự bảo mật, hiệu suất, giá thành và sự thiêt kế
* Kiểm soát sự phức tạp: Tham vọng cho việc thêm vào một chút cung cấp giải pháp tối ưu nhất cho vấn đề này mà vẫn đảm bảo sự cân bằng. ( ví dụ như giá thành và thiết kế) được liệt ra ở trên.
* Thiết kế trong sự bảo mật từ quan niệm: Xây dựng một sự bảo mật từ lúc bắt đầu bằng cách tuân theo nguyên lý và kỹ thuật thiết kế bảo mật sản xuất tốt.

**Tổng quan an ninh mạng**

**Những thành phần của an ninh mạng:**

* Sự bảo mật: Phòng ngừa sự truy câp ko xác định rỏ nguồn gốc.
* Tính toàn vẹn: Ngăn ngừa sự biến đổi hay sự sai lệch của tài nguyên
* Khả năng truy cập: phòng ngừa những sự tấn công giữ cho một tài nguyên khỏi bị truy cập hay bị sử dụng tuân theo tính năng được mong đợi của nó.

**Những lĩnh vực liên quan bảo mật bao gồm:**

* Mã hóa (Cryptography)
* Thử nghiệm xâm nhập(Penetration testing)
* Kiểm tra và nhận dạng(Monitoring and detection)
* Kĩ năng xã hội (social engineering)
* Nhận thức tình huống mạng (cyber situational awareness)
* Thiết kế hệ thống bảo mật (security system design)

**Những nguyên tắc an ninh mạng:**

* Không có sự bảo an toàn vậy lý, không có sự bảo mật: Nếu hẹ thong vật ký bị thỏa hiệp,do vậy thì những thuộc tính khác của hệ thông mà nó tương tác trực tiếp hay gián tiếp với hệ thống vật lý.
* Một lần “root”, luôn luôn”root”: một lần một hệ thống đã bị thỏa hiệp, một hacker có thể cài đặt “backdoors” để truy cập hệ thống với root đặc quyền sau đó.
* Defense of depth: sự ngăn chặn hoàn toàn là bất khả thi. Những lớp đa hợp của phòng chống và kiểm định tla2 thật sự cần thiết để đạt điều kiện thuận lợi nhất cấp độ bảo vệ.
* Kerckhoffs ‘s principle: Giả sử như hacker biết được hệ thống. Kết quả: Bảo mật bằng sự mù tịch thì không đảm bảo.
* Nguyên tắc liên kết yếu nhất (Weakest link Priciple): lIên kết yếu nhất trong hệ thống thì hầu như là một phần của hệ thống bị tấn công đầu tiên bời vì nó dễ dành nhất.

**Thủ phạm chủ yếu cho lỗ hổng bảo mật dư thừa được tìm thấy trong hầu hết các sản phẩm chủ đạo là cái gì?**

* Sự thi hành yếu kém(poor implementation)
* Lỗ hỏng thiết kề (flawed design)

**Tại sao nó thì hợp lý để sản xuất các sản phẩm bảo mật thấp?**

**Thị trường cho các sản phẩm bảo mật kém**

* Giấy được viết bởi nhà kinh tế học George Akerlof vào nam 1970 để thảo luận sự bất đối xứng thông tin
* Sự bất đối xứng thôn tin: Một tổ chức có thông tin tốt hớn tổ chức khác
* Ý tưởng chủ chốt: Khi mà người mua hàng không có nhiều thông tin về chất lượng sản phẩm như người bán hàng có được, sẽ có vài áp lực giảm nghien trọng trên cả hai phần giá cả và chất lượng sản phẩm.

**Thị trường cho an ninh mạng “lemons”**

-Người mua(bao gồm cả chuyên gia bảo mật) thì thường không đủ khả năng đễ phân biệt một sản phẩm bảo mật tốt tư ột sản phẩm bảo mật kém.

-Sự khó khăn trong việc đánh giá một sản phẩm đòi hỏi khi source code và cấu trúc thiếc kế thì dcó thương hiệu và độc quyền.

-Số lượng tiền phát sinh cho một tổ chức độc lập thứ ba để đánh giá và kiểm định sự đòi hỏi sản phẩm

-Bottom line: Có thể là hợp lý cho những công ty sản xuất những sản phẩm bảo mật thường bời vì người dùng và các chuyên gia thì hầu như làm cho sự quyết đinh của họ dưa trên các thông số (ví dụ giá thành) họ có thể chấp nhận

Ngoại lệ hiếm (rare excepton): Secustick được vạch trần bởi Tweakers.net cho việc không mã hóa dữ liệu trên USB drives khi họ yêu cầu phải làm như vậy.

**Bảo mật nhúng: Hệt thống nhúng**

Định nghĩa: Một hệ thống nhúng là một sản phẩm điện tử bao gôm 1 hoặc nhiều vi sử lý và phần mềm để thi hành vài tính năng cấu thành với một thực thể lớn hơn

Key point: Hệ thống nhúng có thể được ràng buộc bởi giá thành, bộ nhớ, năng lượng, khối lượng và thể tích

Ví dụ:

* Smart meter
* Raspberry Pi
* Smart Phone
* Router

Tất cả các thiết bị nhúng có đặc điểm chung gì?

Lợi thế của hệ thống nhúng mạng lưới là gì?

Ban quản lý kiểm soát

* -Hiệu suất thẩm định của thiết bị triển khai trong một vùng
* -Sự cho phép cài đặt của những lỗ hỏng hay nâng cấp những phần mềm khác
* -Kích hoạt một số lượng lớn hơn cần thiết của nhiệm vụ quản lý

Gia tăng tuổi thọ, đội tin cậy, tiện lợi, và sự hài lòng của khách hàng trong khi giảm giá bảo trì và tổng giá thành của người sở hữu

Ví dụ của sự quản lý kiểm soát: Nhiệm vụ tìm đường sao hỏa (Mars pathfinder mission)

-Sự trục trặc được chuẩn đoán xuống một khuyết điểm phần mềm xuyên suốt nhiệm vụ

Vấn đề đảo ngược ưu tiên giữa nhiệm vụ giao tiếp (Ưu tiên trung), nhiệm vụ thời tiết (Ưu tiên thấp), bus liên kết thông tin( Ưu tiên cao)

Miêng vá để cung cấp phương pháp bằng cách thêm sự thừa kế ưu tiên được cài đặt thông qua kết nối vô tuyến từ Trái Đất

Quản lý kiểm soát (Remote management) cứu nhiệm vụ này khỏi thảm họa