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)

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 gây ra 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.

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)