**EMBEDDED SYSTEM SECURITY**

1. **Giới thiệu:**

* Bảo mật hệ thống nhúng (Embedded system security) là làm giảm các lỗ hổng bảo mật và bảo vệ thiết bị chống lại các mối đe dọa của phần mềm chạy trên các hệ thống nhúng.
* Trước đây, số lượng các hệ điều hành nhúng bị tấn công từ bên ngoài không nhiều, do chúng ít có giao tiếp Internet và giao tiếp giữa các thiết bị với nhau.
* Tuy nhiên, xu hướng ngày nay, các hệ thống nhúng đã gia tăng đáng kể giao tiếp machine to machine (M2M), Internet of Things và các hệ thống công nghiệp điều khiển từ xa đã tăng số lượng thiết bị được kết nối. Do đó các thiết bị này sẽ trở thành mục tiêu của các cuộc tấn công qua mạng.
* Việc cập nhật firmware cho hệ điều hành nhúng kèm theo số lượng các điểm giao tiếp của các thiết bị tăng lên kéo theo sự gia tăng bề mặt tấn công.
* Một điểm giao tiếp là một điểm xâm nhập tiềm tàng cho tin tặc.
* Phần mềm nhúng (firmware) của một thiết bị có thể bị hacker theo dõi và kiểm soát mọi thứ từ Internet, các điểm truy cập không dây, USB, camera…

1. **Bảo mật hệ thống nhúng trên các thiết bị di động:**

Các thiết bị di động luôn phải đối mặt với nguy cơ bị khai thác các lỗ hổng bảo mật rất cao.

Việc kết hợp nhiều thiết bị lại với nhau thông qua một hệ thống mạng là một thách thức đối với các nhà bảo mật trong việc đề phòng tin tặc và các cuộc tấn công mạng.

Một số cách mà các công nghệ nhúng giúp các chuyên gia giải quyết vấn đề bảo mật trên thiết bị di động:

* Tăng tốc độ mã hóa: Bao gồm mã hóa tự động full – disk, không ảnh hưởng đến trải nghiệm của người dùng trên thiết bị. Công nghệ **Intel AES New Instructions** có thể mã hóa dữ liệu nhanh hơn gấp 4 lần mà không ảnh hưởng tới tốc độ của thiết bị. **Intel Secure Key** giúp bảo vệ dữ liệu tốt hơn bằng cách tạo ra những con số ngẫu nhiên.
* Tăng cường phòng chống các mối đe dọa: Chống lại sự xâm nhập của rootkit, phần mềm độc hại bên dưới hệ điều hành, nó rất khó tấn công khi người dùng làm việc trong môi trường đám mây hoặc môi trường ảo.
* Cải tiến công cụ quản lý nhận dạng.
* Tăng cường giám sát, khắc phục sự cố thiết bị.