SNS COLLEGE OF TECHNOLOGY

An Autonomous Institution

Coimbatore-35

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A++' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF ELECTRONICS & COMMUNICATION ENGINEERING

19ITT204 - MICROCONTROLLER AND EMBEDDED SYSTEMS

II YEAR/ IV SEMESTER

UNIT V EMBEDDED SYSTEM DEVELOPMENT

TOPIC – Security Issues in Embedded Systems

EMBEDDED SYSTEM SECURITY

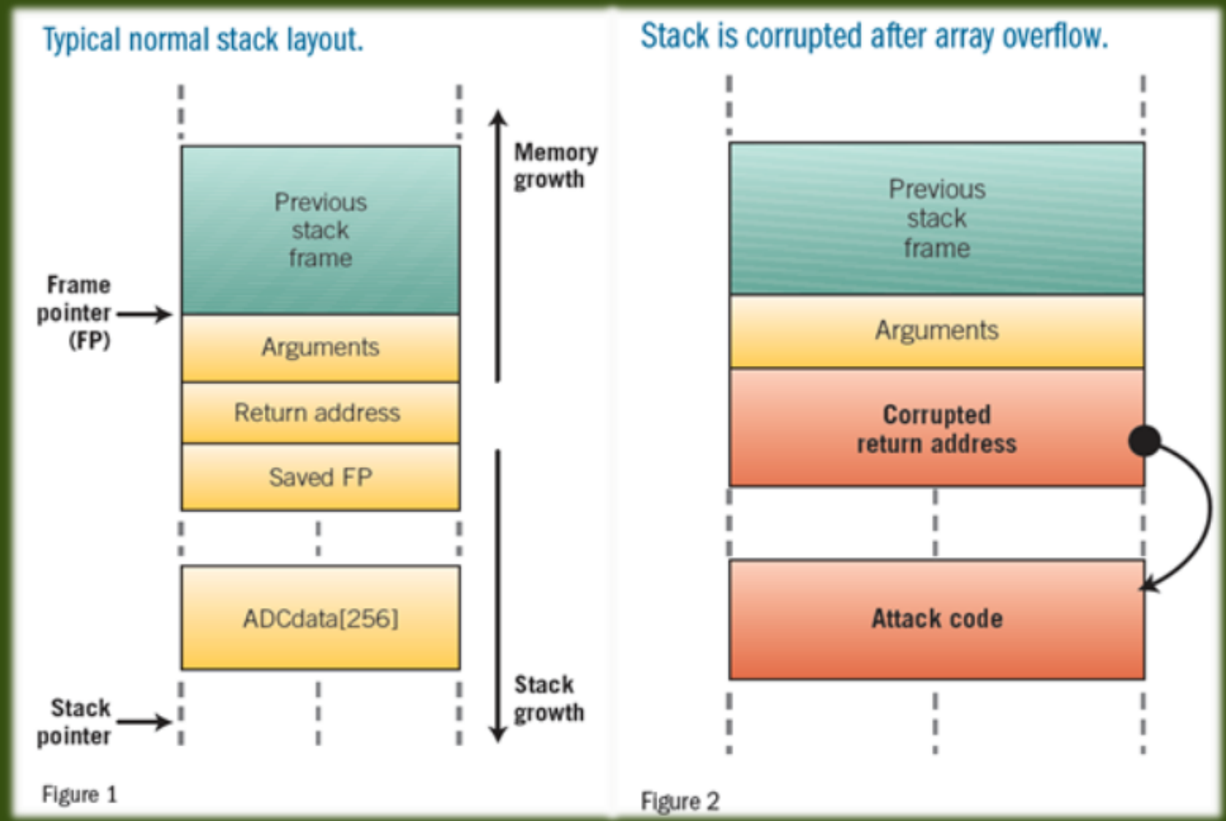
- Sorts of embedded security issues
  - Software security
  - Hardware security
  - Network security

OUTLINE

SOFTWARE SECURITY

- Most attacks are via software
- Cryptographic attacks
- Code injection attacks
  - **Stack-based buffer overflows**
  - Heap-based buffer overflows
  - Etc.

SOFTWARE SECURITY ▸ Example - Stack-based buffer overflows



SOFTWARE SECURITY

- Possible security strategies
  - No unknown source program in execution space
    - Non-executable stack
    - Read-only memory
  - Strong data privacy and encryption
  - Hardware-assisted protection

NETWORK SECURITY

- What is network security
- Sources of network attack
- Ways to manage risk

NETWORK SECURITY

How to Hack Into a Boeing 787

Published February 20, 2008 · FoxNews.com 0 0

- Federal Aviation Administration warned Boeing that its new Dreamliner aircraft Boeing 787 had design problem. Hackers could hack the aircraft from passengers' Wi-Fi network.
- Navigation system or control system could be hijacked

NETWORK SECURITY

- Activities designed to protect your network
- Give reliability, usability, integrity and safety to network

NETWORK SECURITY

- Attack categories:
  - Passive attack
  - Active attack

- Threat sources:
  - Wiretapping: a third party monitoring your network
  - Port scanner: probes the host to find the current service
  - Idle scan: send garbage to the host to find available service
  - DoS (Denial of Service Attack): service rejects the legal user
  - **Man in the middle: attacker cheat the server and client**

NETWORK SECURITY

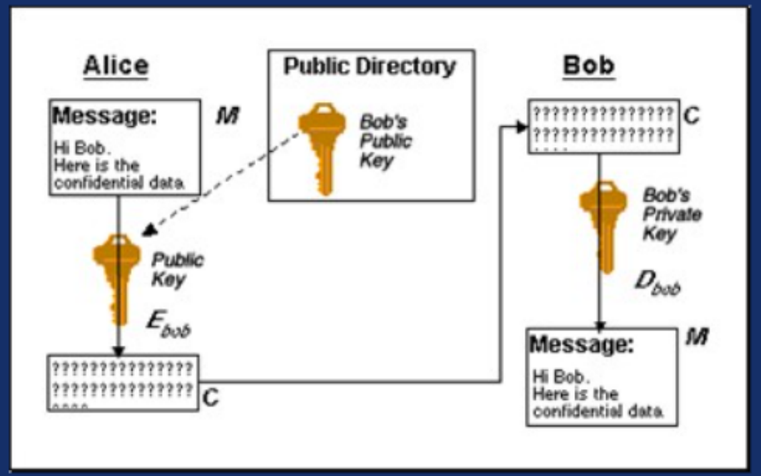
- Man in the middle
  - Third party relays or possibly alter the message
  - Server and client believe they are talking directly to each other
  - Secret message getting stolen might lead to severe outcome to the country

NETWORK SECURITY

- Method to improve network security
  - Anti virus and anti spyware
  - Firewall
  - Intrusion prevention system
  - Virtual private network
  - **Key authentication**

NETWORK SECURITY

- Key authentication
  - Public key: A public key encrypts a message. Public key is publicly known.
  - Private key: A private key decrypts a message. Private key is only known by owner.
  - Needham-Schroeder protocol
- Public key encryption
  - An encryption mechanism where two keys are used. A public key is used to encrypt the message and a secret private key to decrypt the message.
- Advanced encryption algorithm
  - Diffi-Hellman key exchange
  - Needham-Schroeder protocol



HARDWARE SECURITY

Credit card skimmer found at Ann Arbor gas station

- Credit Card Skimmer
  - Malicious card reader that grabs data off the magetic stripe.
  - Create cloned cards, and steal money

Credit Card Skimmer

HARDWARE SECURITY

$60 DIY car hacking device is an inexpensive and easy way to hack cars

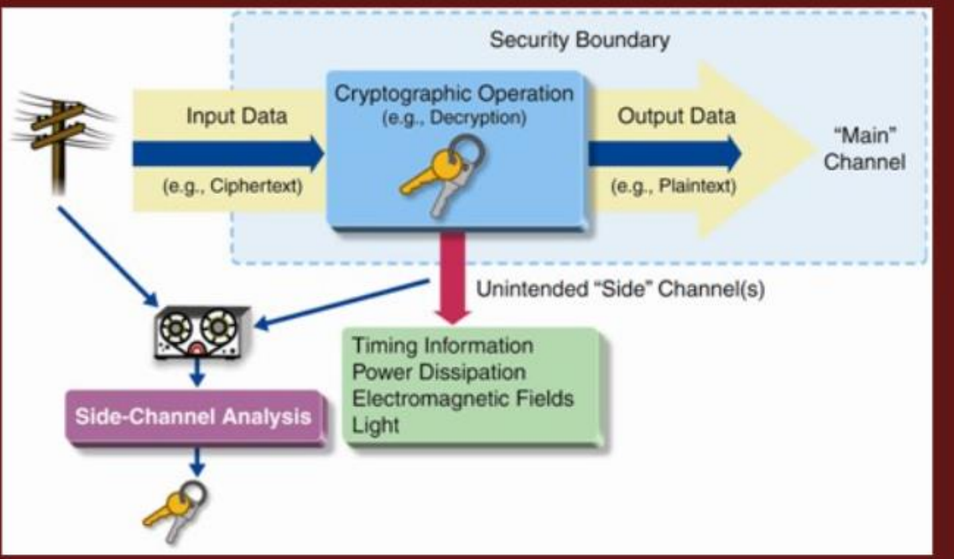
- Credit Card Skimmer
  - Malicious card reader that grabs data off the magetic stripe.
  - Create cloned cards, and steal money
- Things can get worse ..
  - Use the CAN bus in the car
  - Take control of braking, acceleraion ...

HARDWARE SECURITY

- Pyramid of Trust
  - Each layer can rely on the effective security of its underlying layer without being able to verify it directly
  - A perfect software security solution will be useless with a weak hardware protection
- Lots of Methods of Hardware Hacking ...
  - https://diy.org/skills/hardwarehacker

HARDWARE SECURITY

- Side-Channel Analysis
  - Definition - any **attack** based on information gained from the **physical implementation** of a cryptosystem
- Types
  - Timing Analysis - timing due to program branches
  - Simple Power Analysis (SPA) - Power supply currents
  - Electromagnetic Analyses (EMA) - Electromagnetic Radiation

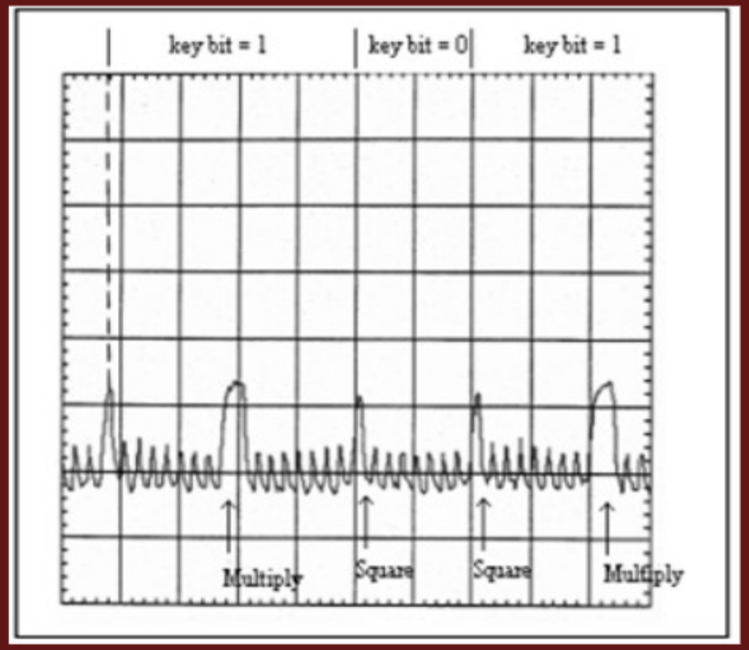


HARDWARE SECURITY

- SPA analysis on RSA
  - IC power consumption depends on activity of transistors
  - Variations in **power** consumption occur as the device performs different operations
- RSA

Decryption $c^d \equiv (m^e)^d \equiv m \mod n$

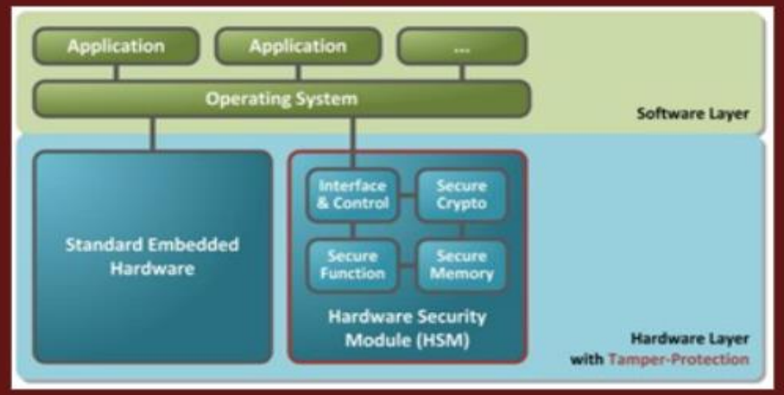
  - If a bit of the binary private key is $d_i = 1$, we square + multiply
  - If the bit is 0, we just square
  - **Power consumption of Multiplication and Square are different**



HARDWARE SECURITY

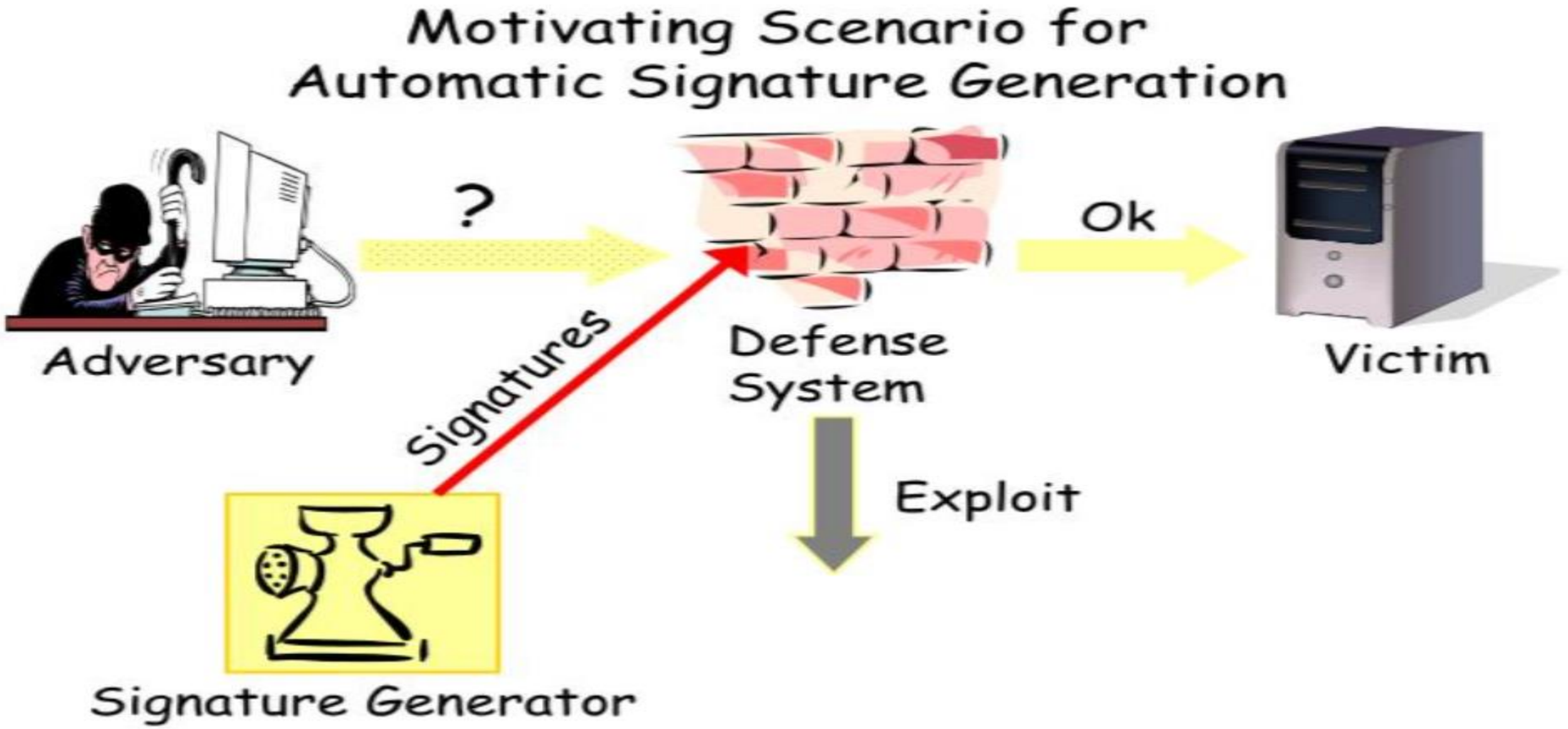
- Solution
  - Hardware Security Modules (HSM)
    - Payment Card Industry (PCI) HSM
  - Physical Isolation
  - Etc.

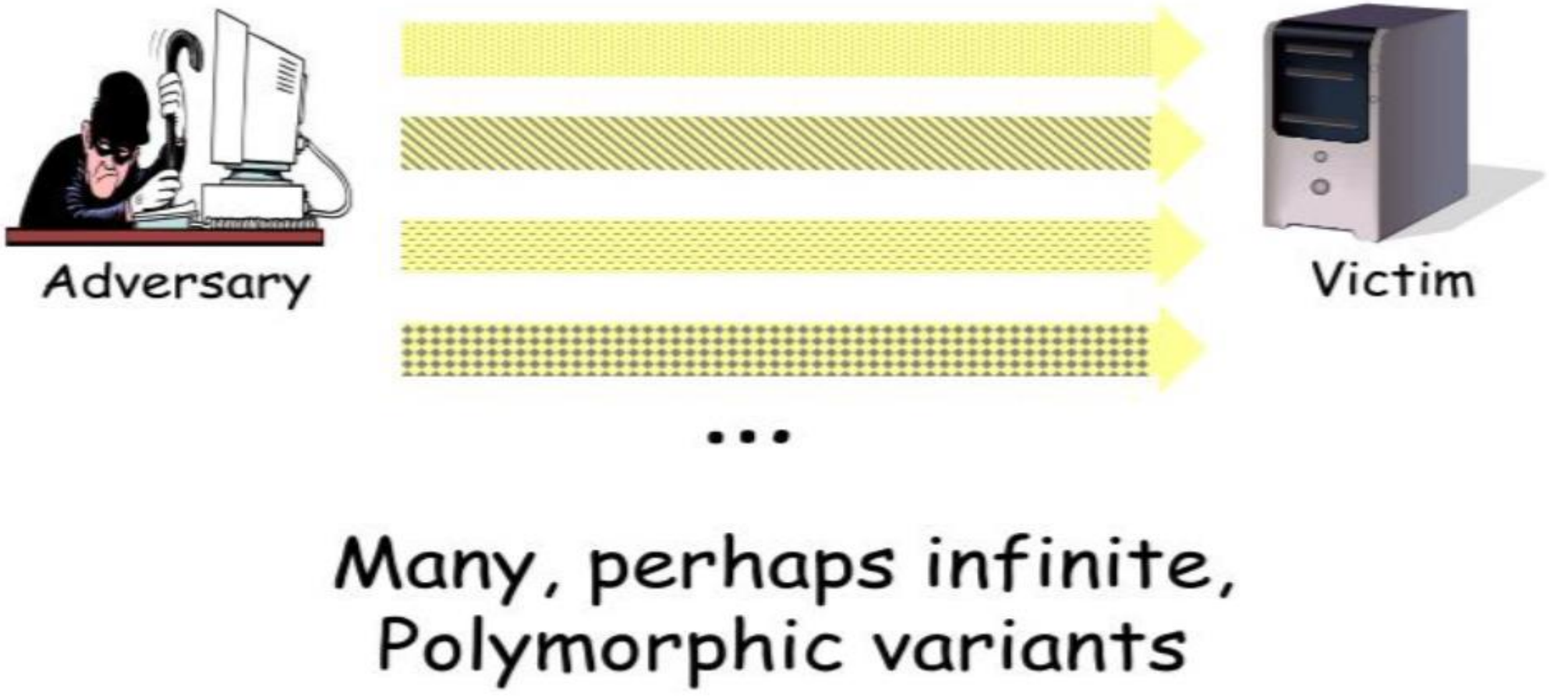
SafeNet PCIe HSM



Dynamic and Configurable Environment

- Embedded systems are highly configurable
  - They have to work in many different scenarios
- Environment is highly dynamic
  - Think about embedded systems in a battlefield
  - Embedded system in a vehicle


Motivating Scenario for
Automatic Signature Generation
?
Ok
Adversary
Signatures
Defense
System
Victim
Exploit
Signature Generator


Adversary
Victim
...
Many, perhaps infinite,
Polymorphic variants

What is security in an embedded system

Embedded System Security Is a Strategic approach to protecting software running on **Embedded** Systems from attack. An **Embedded System** is a programmable hardware component with a minimal operating system and software.

Embedded Systems are designed to perform a dedicated function or functions. Found in Consumer Electronics, Process Control Systems, Aircraft, In-car systems and many other applications, Embedded systems need to be extremely reliable. Because of their small size and limited compute resources, However, They can present security challenges for designers and developers.

Why do we require security in an embedded system

- The most common examples of embedded system exploits are Hacks Of Consumer Electronics such as GPS Devices, Video Cards, Wi-Fi Routers, and Gaming devices. These hacks are usually possible because manufacturers don't protect their firmware. As a result, Almost anyone with a little technical knowledge can gain access to premium features or Overclock A device. It was originally published On Https://Www.Apriorit.Com/.
- In 2018, Ethical hackers found Meltdown And Spectre Hardware Vulnerabilities that affect all Intel X86 and Some AMD Processors. Both Vulnerabilities mess up isolation between user Applications, Giving applications access to sensitive data and expanding the attack surface. Both Linux and Windows developers have issued patches for their operating systems that partially protect devices from Meltdown and Spectre. However, Lots of devices (Especially Old Ones) Running on Vulnerable Processors are still unprotected. It was originally published On Https://Www.Apriorit.Com/.
- Military Equipment also can suffer From attacks on embedded systems. For example, Hackers could Shut Down the trusted aircraft information download station on the F-15 Fighter Jet. This Embedded device collects data from video cameras and sensors during the flight, Giving Pilots navigation Data. It was originally published on Https://Www.Apriorit.Com/.

Attack taxonomy in an embedded system

Five Dimensions are defined along Which Attack Against Embedded Systems Can Be Classified

1. Preconditions
2. Vulnerability
3. Target
4. Attack Method
5. Effect Of The Attack

1. Precondition

Internet Facing Device.

Local Or Remote Access Device.

Direct Physical Access To The Device.

Physically Proximity Of The Attacker.

2. Vulnerabilities

Programming Errors.

Web Based Vulnerability.

Weak Access Control Or Authentication.

Improper Use Of Cryptography.

3. Target

Hardware

Firmware/Os

Application

Device Itself

4. Attack method

Control Hijacking Attacks.

- Reverse Engineering.
- Malware.
- Injection Crafted Packets Or Code Injection.
- Eavesdropping.
- Brute-force Search Attacks.

5. Effect of attack

Denial - Of - Service.
Code Execution.
Integrity Evolution.
Information Leakage.
Illegitimate Access.
Financial Loses.

THANK YOU