IoT Cybersecurity Vulnerabilities and Practices

ECE 442/510 – Internet of Things and Cyber Physical Systems

David Arnold

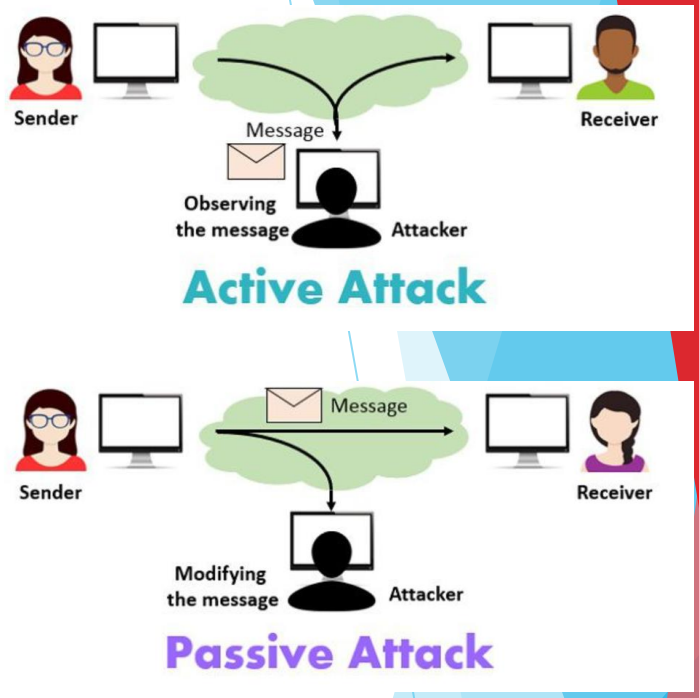
Discussion Outline

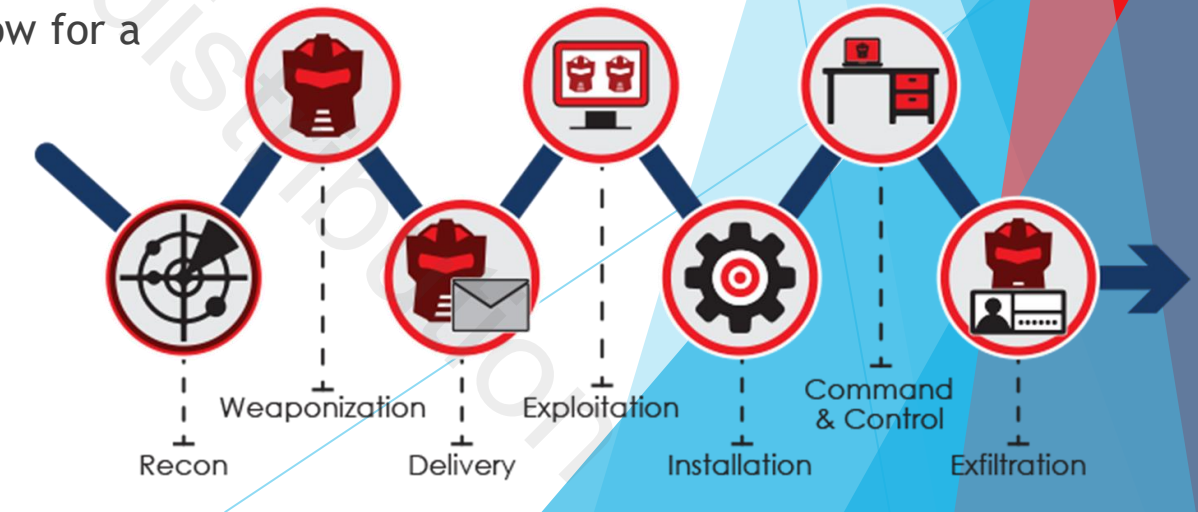
- General Considerations
  - Hackers and the Cyber Kill Chain
  - The CIA Triad
  - Communication Technologies
  - Physical/Hardware Weaknesses
  - Software/Application Weaknesses
  - Consumer Privacy
- Defensive Security Measures
  - Data Encryption
  - RSA Asymmetric Key Algorithm
  - Cloud Providers
- Common Attacks
  - OWASP Top 10 Security List
  - Wireless Traffic Sniffing
  - Weak Key Generation Protocols
  - Improper Input Validation
  - Man-in-the-Middle Attacks
  - Denial of Service Attacks
  - Side-Channel Attacks
- Advanced Security Concepts
  - Key Distribution Systems
  - Lightweight Encryption Accelerators

General Considerations

Hackers and the Cyber Kill Chain

- Types of Hackers
  - Active
    - Hacker modifies messages and/or device software
  - Passive
    - Hacker simply listens to messages between devices
- The Cyber Kill Chain
  - Generalized Attack Procedure that a hacker will follow for a successful attack
  - IoT Devices make good jumping-off points



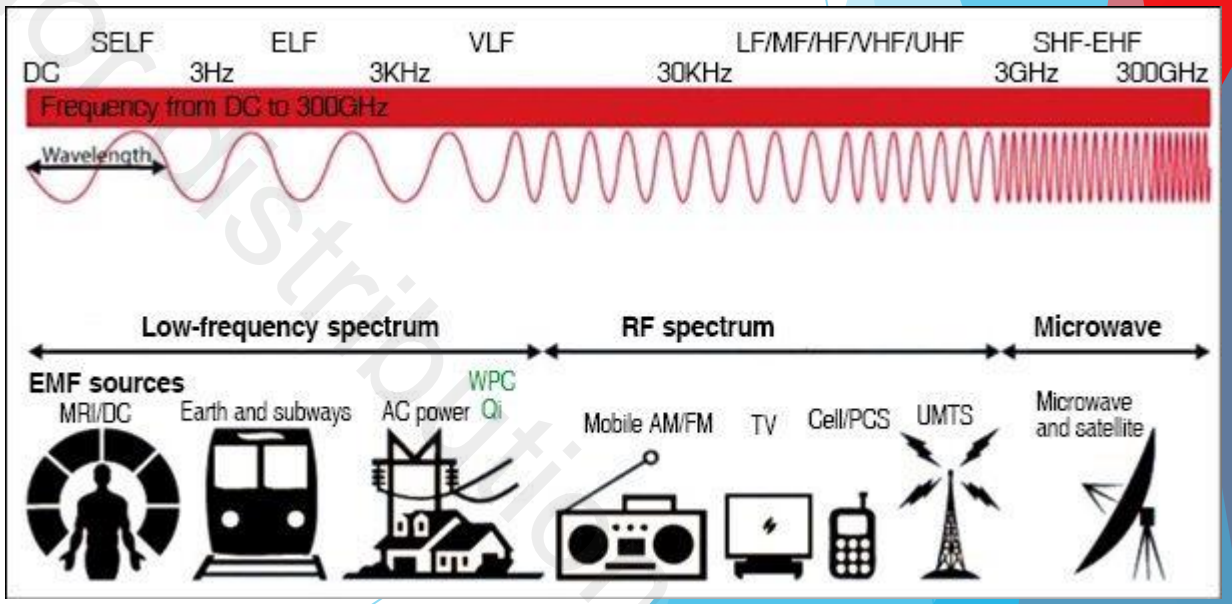


The CIA Triad
Information Security Metrics

- Confidentiality
  - Data is only readable by permitted parties
- Integrity
  - Data cannot be manipulated by outside parties
- Availability (Non-repudiation)
  - Data should be accessible by authorized parties
- How do these metrics change with different applications?
  - Smart Home Devices?
  - Industrial Components?
  - Medical Sensors?

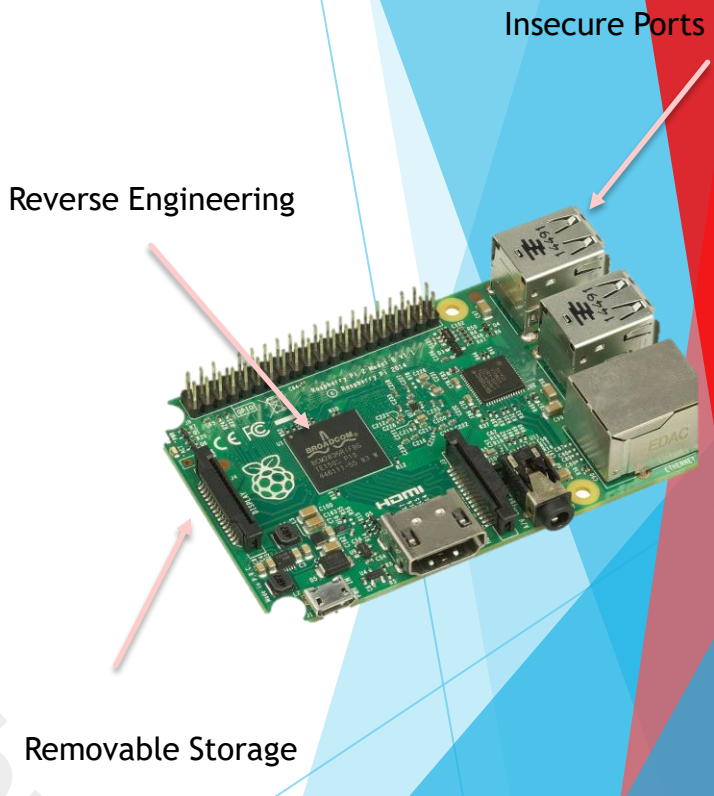
Communication Technologies
A Cybersecurity Perspective

- Devices that rely on RF Communication are required to specify their communication frequency with the FCC to legally operate
- Bluetooth
  - Operates at 2.4 GHz
- WiFi
  - Two Frequency Bands:
    - 2.4 GHz
    - 5 GHz
- Zigbee
  - General purpose 2.4 GHz
  - Long Range 868/900 MHz



Physical/Hardware Weaknesses

- How does having physical access to the device change how it can be manipulated?
- Insecure Access Points
  - Open USB ports provide an access point for installation of malicious software
- Removable/Easily Accessible Storage
  - Removal of storage devices may provide access to sensitive data and can interfere with data collection and/or function
- Reverse Engineering
  - Removal of core components (CPU and/or sensors) can be used to further explore the functionality/purpose of the device



Software/Application Weaknesses

- How is your data being handled on the front and back end?
- Databases
  - Username and Password Security
  - Access Control Mechanisms
- Web Servers
  - Interconnection with Database services
  - Data Presentation and Access Control
- Cloud Providers
  - Platform security functionality
  - Expanded service availability

Google Cloud

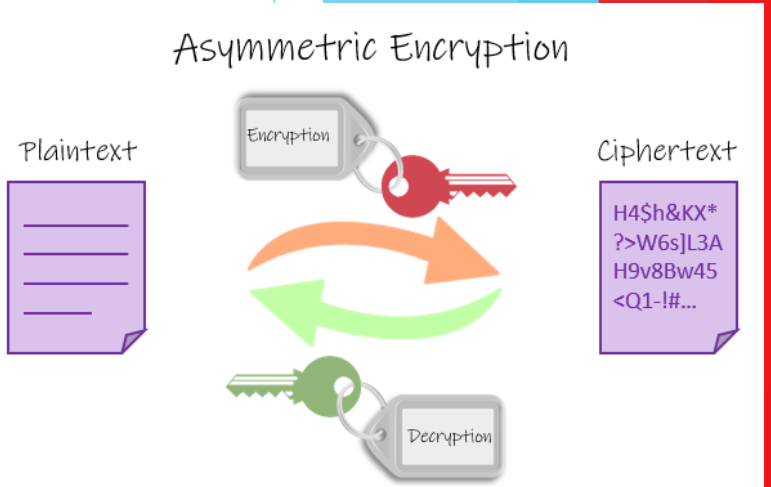
Consumer Privacy

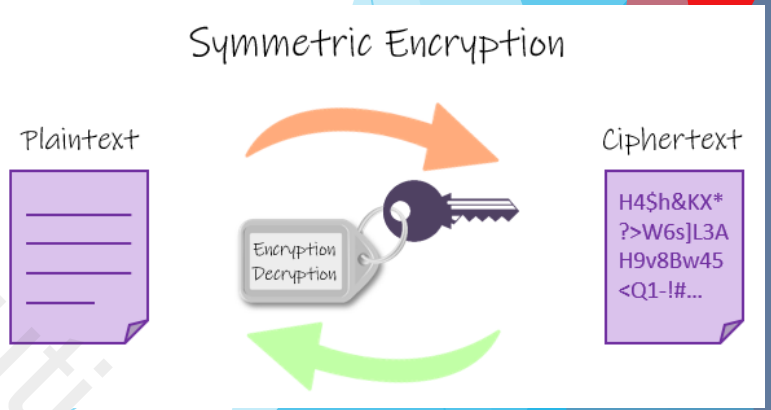
- Whenever an IoT device transmits to a remote database or cloud-based storage system, there is an inherent risk to user privacy
- Potential Concerns
  - Storage System Data Breaches/Improper Access
    - Is the data stored in an encrypted form?
    - What are the data breach notification requirements?
  - Corporate Use of Stored Data
    - How is user data used by the corporate entity and who is the data shared with?

Defensive Security Measures

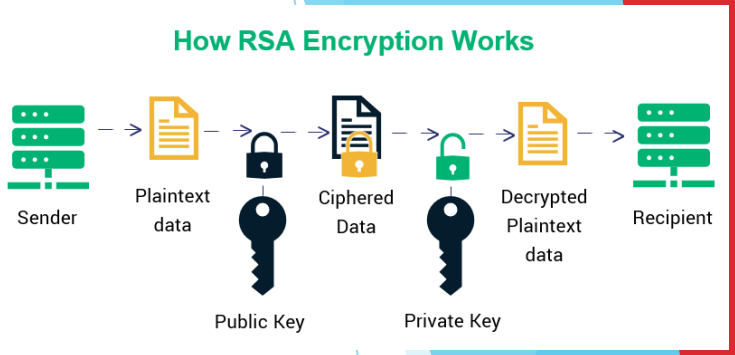
Data Encryption

- Asymmetric Vs. Symmetric Encryption
  - Asymmetric – public-private key pairs for encryption/decryption
    - Rivest-Shamir-Adleman (RSA) – 1024 bits
  - Symmetric - single, shared key for encryption/decryption
    - Advanced Encryption Standard (AES) – 256 bits
- Hashes
  - One-way, irreversible function for data integrity
- Data-at-Rest Vs. Data-in-Motion
  - Data-at-rest: data stored within your servers
  - Data-in-motion: data moving between your device and server





RSA Asymmetric Key Algorithm



- All users generate a public and private key. Public keys are posted in an accessible location for all users to pull from
- Data Confidentiality
  - Sender grabs the receiver's public key and encrypts their message
  - Receiver decrypts the message with their private key
- Sender Verification
  - Sender encrypts using their own private key and encrypts the message
  - Receiver decrypts using the sender's public key to verify their identity

Cloud Service Providers Security as a Service

- Many Cloud Service Providers offer additional options for IoT clients (for a price)
- AWS IoT Device Defender
  - Regular audits of IoT configurations for deviations from security policies
  - Device identity, authentication, and authorization services
- Google Cloud
  - End-to-end Asymmetric Key Authentication over TLS 1.2
    - CA-signed certificates
- Azure Sphere
  - Hardware, OS, and Cloud components for security from the ground up
  - Over-the-air (OTA) updates
  - Error reporting and security updates

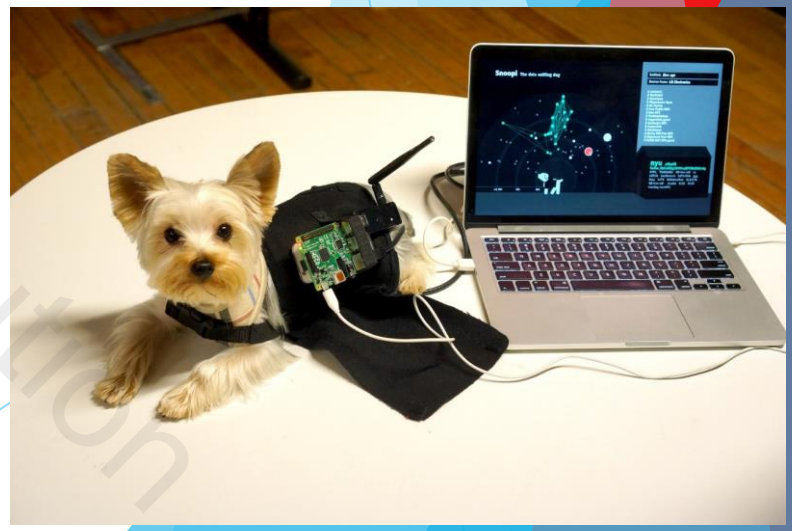
Common Attacks

OWASP Top 10 Security List
Open Web Application Security Project

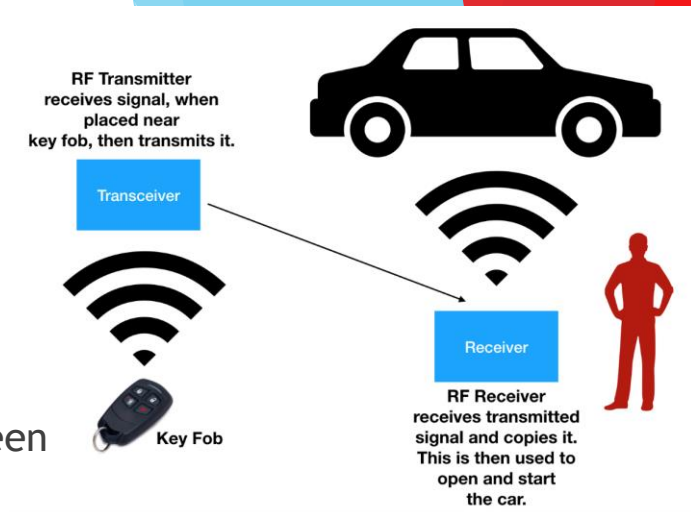
- OWASP regularly releases awareness documents regarding current cyber security threats.
- 2018 Top 10 IoT Security Checklist
  - Weak Guessable, or Hardcoded Passwords
  - Insecure Network Services
  - Insecure Ecosystem Interfaces
  - Lack of Secure Update Mechanism
  - Use of Insecure or Outdated Components
  - Insufficient Privacy Protection
  - Insecure Data Transfer and Storage
  - Lack of Device Management
  - Insecure Default Settings
  - Lack of Physical Hardening

Wireless Traffic Sniffing

- Radio Frequency (RF) transmissions are easy to detect and collect with cheap hardware and technology
- Due to FCC requirements, attackers can easily look up the operational frequency of any legitimate IoT device
- Replay Attack
  - Hacker collects valid transmissions and send them back to the receiver, hoping to achieve the same effect (such as opening and/or closing a garage door)
- Zigbee and Bluetooth devices DO NOT have encryption by default



Weak Key Generation Protocols Automotive Key Fob Hacks



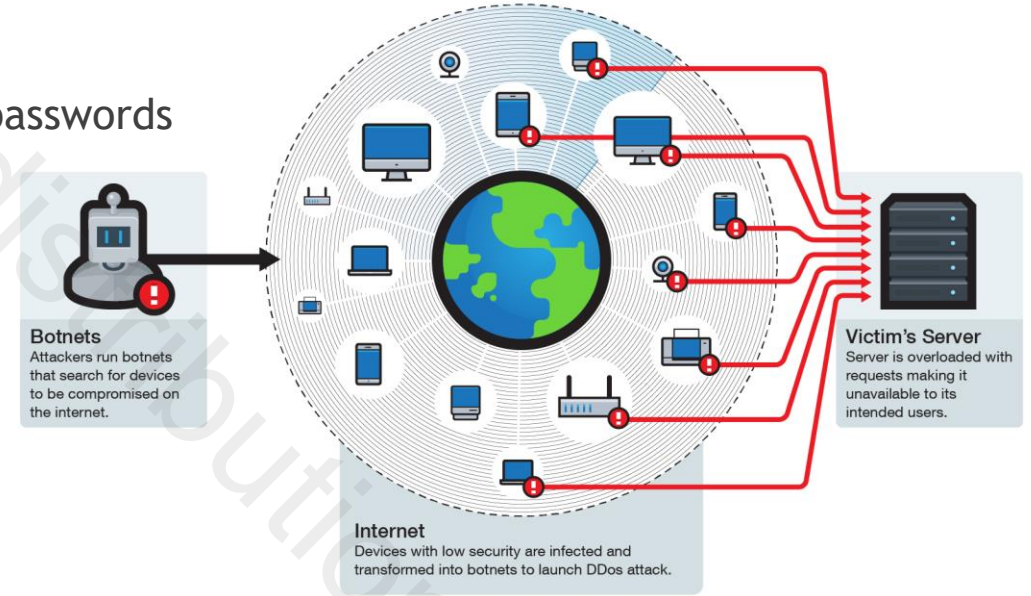
- Recently several high-profile hacks targeting remote unlock Key Fobs for vehicles have been discovered
- Key Fobs generate a shared symmetric encryption key every time you press the “lock” button
- Common Key Fob Hacks
  - Replay Attacks
    - Hacker records and sends back the key fob key generation signal
  - Encryption Keys Generated from Public Data
    - Keys derived from publicly readable information (transponder serial number)
  - Deprecated Key Strength
    - NIST recommends a minimum key length of 128 bits or longer for AES, some key fobs utilize 40 or 80 bit lengths
  - Rolling Code System – Predictable Key Generation
    - The Key Fob maintains a synchronization counter that is incremented with each push. It sends the counter to the receiver, which is checked against the transmitter’s serial number and the currently stored counter.

Improper Input Validation
Smart Spies

- Hackers may attempt to exploit database or feature functionality by providing tailored strings that result in improper operation
  - SQL Injection is a common attack against databases by passing valid SQL commands through prompts and receiving user data
  - Strings longer than expected can result in remote code execution
- In 2019, a vulnerability in Amazon's Alexa and Google's Google Home devices led to potential phishing and eavesdropping attacks
  - Unpronounceable text is replaced with a period of silence by the device, while still recording user interactions. This can be used to eavesdrop or to request user passwords and information.
  - Also displayed a weakness in the app verification process as designers can modify functionality after being greenlit by Amazon and Google

Denial of Service Attacks

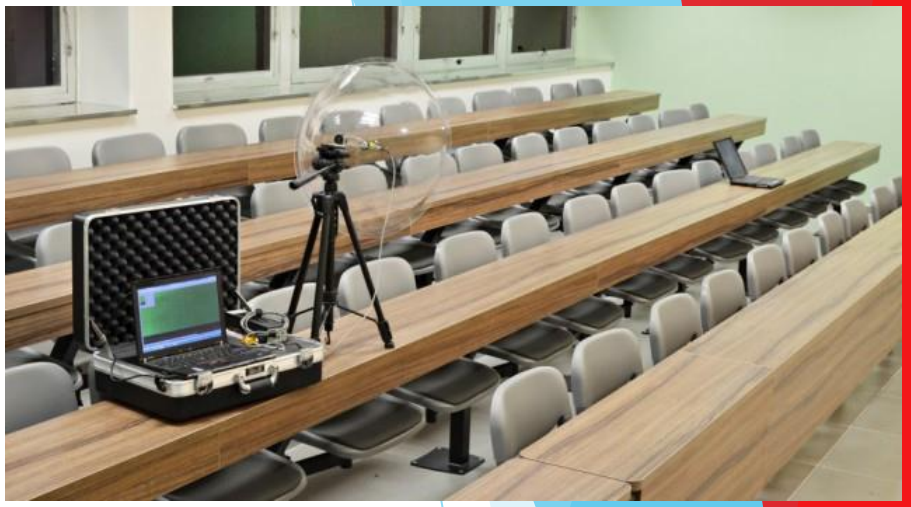
- Large amounts of incoming traffic can overwhelm target devices, rendering them unable to respond to valid requests.
- IoT devices are vulnerable to incoming Denial of Service (DoS) and at risk of being added to larger “botnets”
  - Low processing power with limited redundancy
  - Historically weak security, including default usernames and passwords



Man-in-the-Middle (MitM) Attacks

- Classical cyber security attack against asymmetric key protocols
  - The Hacker presents themselves as the desired device and generates separate shared key pairs between the victim and the device
  - Any messages sent between the target and the device will be decrypted by the Hacker before being sent to the proper destination
- ARP Spoofing/Poisoning
  - Attacker sends out fake ARP (Address Resolution Protocol) messages hoping to associate their MAC address with a target IP address in the network
  - Wireless networks can be compromised by ARP Spoofing the router

Side Channel Attacks

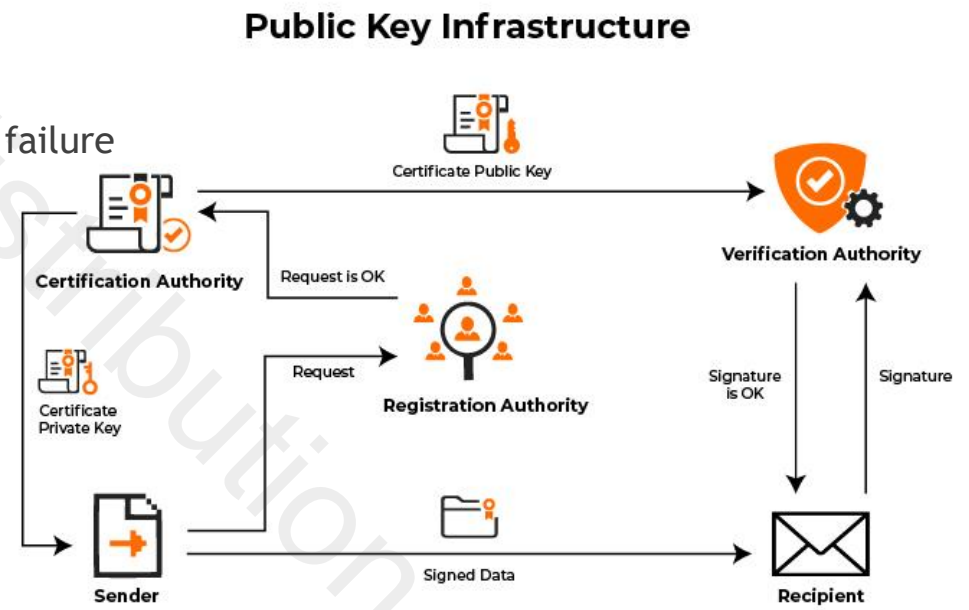


- Analysis of non-software/hardware device characteristics
  - Primarily completed locally, but can be completed remotely under the proper circumstances
- Common Characteristics for Side Channel Attacks
  - Timing
  - Power Consumption
  - Acoustic Performance
    - RSA Designers were able to successfully recover the RSA private key of a target computer by analyzing the acoustic performance of the target's CPU

Advanced Security Topics

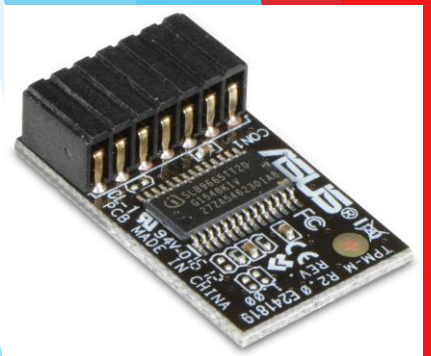
Key Distribution Systems

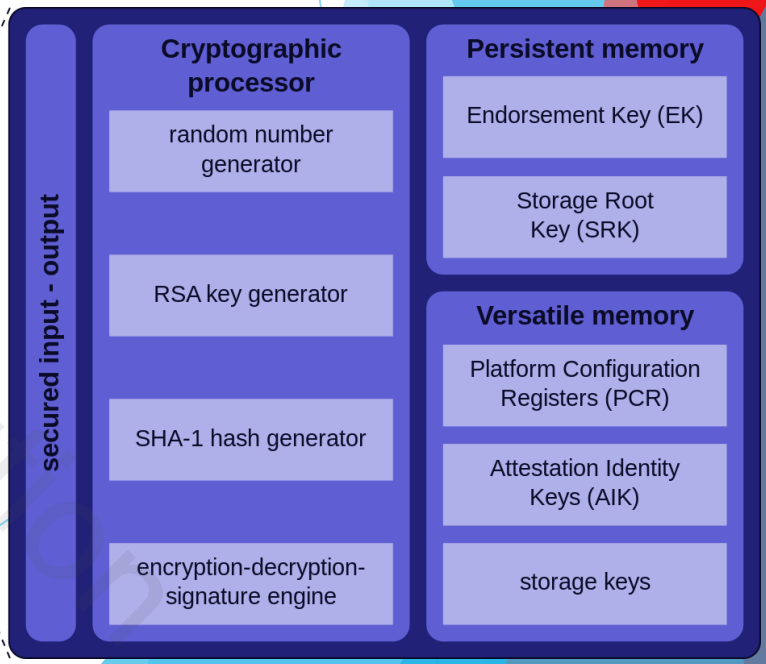
- Difficult to ensure secure transmission of critical symmetric and asymmetric keys
- Common Solution: Public Key Infrastructure
  - New devices register with a registration authority and receive a signed certificate that can be used to verify identity
  - Potential Problems:
    - Registration Authority and Certificate Authority are single points of failure
    - Costly to develop and maintain
  - Similar to Google Cloud RSA Key Generation services



Lightweight Encryption Accelerators

- The limited computational resources of common embedded devices drastically reduces the ability to use standard encryption practices, such as AES and RSA
- Add-on, external accelerators can offload the encryption requirements from the embedded device while maintaining a low per-unit cost
- Trusted Platform Modules
  - Encryption and key storage device commonly used by desktop computers
  - Can be adapted to use GPIO pinouts, like the ones on the Raspberry Pi
- However, connection points can be a vulnerability





Thank you!

Questions: darnold3@hawk.iit.edu