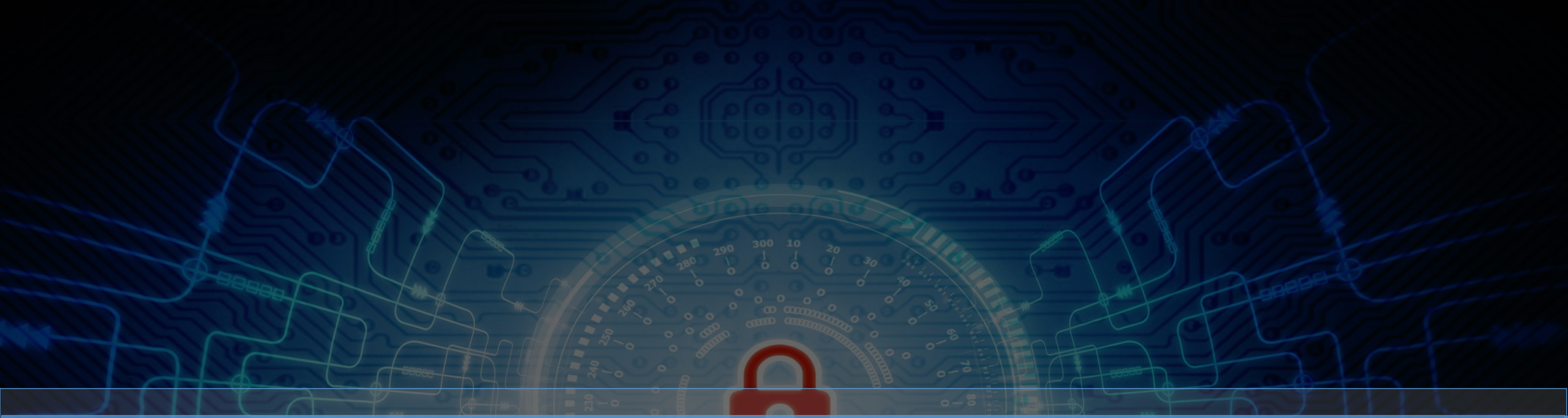
CHAPTER 7

Specialized and Fragile Systems



Episode 7.01 - Mobile Attacks

Objective 3.5 Explain common attacks and vulnerabilities against specialized systems

MOBILE ATTACKS

- Reverse engineering
  - Decomposing steps in a process to determine weaknesses
  - Attackers use it to find vulnerabilities
  - Can be used to select appropriate controls

MOBILE ATTACKS

- Sandbox analysis
  - Analyzing malware or exploit on isolated device or environment
  - Exploit is contained within the sandbox

MOBILE ATTACKS

- Spamming
  - Type of DoS attack
  - Flooding channel with useless traffic to reduce the usability of useful messages

MOBILE VULNERABILITIES

- Insecure storage
  - Unencrypted and easy for apps to access
- Passcode vulnerabilities
  - Weak and easy to guess
- Certificate pinning
  - Limiting certificates that devices or apps will accept
- Using known vulnerable components
  - Dependency vulnerabilities
    - Libraries or other included code
  - Patching fragmentation
    - Only patching part of a vulnerability or some systems/components

MOBILE VULNERABILITIES

- Execution of activities using root
  - Potential for attacker to elevate permissions by leveraging an escape vulnerability
- Over-reach permissions
  - Allowing apps to do more than is necessary
- Biometrics integrations
  - Any authentication method must be implemented securely and limited in its use
- Business logic vulnerabilities
  - Vulnerable software risks data disclosure, alteration, and availability

MOBILE TOOLS

- Burp Suite - https://portswigger.net/
- Drozer - https://labs.f-secure.com/tools/drozer/
- Needle - https://github.com/FSecureLABS/needle
- Mobile Security Framework (MobSF) - https://mobsf.github.io/Mobile-Security-Framework-MobSF/
- Postman - https://www.appdome.com/how-to/dev-sec-tools/app-sec-release-automation/test-cicd-postman-api-app-security-projects/
- Ettercap - https://www.ettercap-project.org/
- Frida - https://frida.re/
- Objection - https://github.com/sensepost/objection
- Android SDK Tools - https://developer.android.com/studio
- Androzer (deprecated) - https://github.com/az0mb13/Androzer
- ApkX - https://github.com/b-mueller/apkx
- APK Studio - https://vaibhavpandey.com/apkstudio/

QUICK REVIEW

- Mobile attacks include reverse engineering, sandbox analysis, and spamming
- Mobile vulnerabilities include insecure storage, passcode vulnerabilities, certificate pinning, vulnerable components, root activities, biometrics integrations, and business logic vulnerabilities

Episode 7.02 - IoT Attacks

Objective 3.5 Explain common attacks and vulnerabilities against specialized systems

IOT ATTACKS

- Bluetooth low energy (BLE)
  - Exploits depend on relaxed requirements for Bluetooth reconnection of paired devices

IOT SPECIAL CONSIDERATIONS

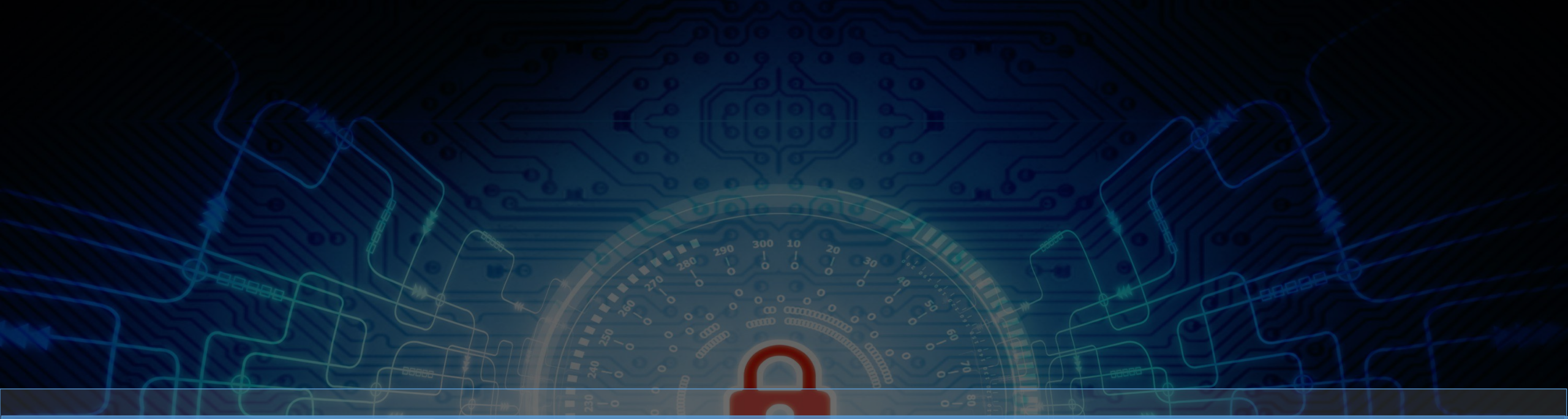
- Fragile environment
  - Low cost, low power devices
- Availability concerns
  - Interrupted availability could negatively affect larger system
  - Many IoT devices are expected to be unavailable at times
- Data corruption
  - Skew larger processes and analysis
- Data exfiltration
  - Easier access to raw and granular data

IOT VULNERABILITIES

- Insecure defaults
  - Easy install and operation often supersedes security
- Cleartext communication
  - Encryption requires setup, admin, and capable hardware/software
- Hard-coded configurations
  - Easy install and configuration
- Outdated firmware and hardware
  - Devices are often difficult to access and update
- Data leakage
  - Difficult to secure simple devices in the wild
- Use of insecure or outdated components
  - Hardware and software components in build may exhibit vulnerabilities over time

QUICK REVIEW

- A Bluetooth low energy (BLE) attack takes advantage of weaknesses in Bluetooth connection
- IoT security considerations include availability, data corruption, exfiltration, and leakage, insecure defaults, cleartext communication, hard-coded configurations, and outdated firmware and hardware



Episode 7.03 - Data Storage and Management Interface Attacks

Objective 3.5 Explain common attacks and vulnerabilities against specialized systems

DATA STORAGE SYSTEM VULNERABILITIES

- Misconfigurations
  - On-premises and cloud based
  - Default/blank username/password
  - Network exposure
- Lack of user input sanitization
  - Goal of software tends to be usability, not security
- Underlying software vulnerabilities
  - Same as with any hardware/software built using components

DATA STORAGE SYSTEM VULNERABILITIES

- Error messages and debug handling
  - Error messages can divulge too much architectural info
- Injection vulnerabilities
  - Single quote method

MANAGEMENT INTERFACE VULNERABILITIES

- Intelligent platform management interface (IPMI)
  - Secure, control, and manage servers remotely independent of the host's operating system
  - IPMI's elevated permission requirements makes the system vulnerable
  - Since IPMI is largely hardware-based, patches may not be available or applied
  - Hardware, software, and component vulnerabilities may pose problems

QUICK REVIEW

- Data storage system vulnerabilities include misconfigurations, lack of user input sanitization, underlying software, error messages and debug handling, and injections
- Intelligent platform management interface (IPMI) secures, controls, and manages servers remotely

Episode 7.04 -Virtual and Containerized Environment Attacks

Objective 3.5 Explain common attacks and vulnerabilities against specialized systems

VIRTUAL ENVIRONMENT VULNERABILITIES

- Virtual machine (VM) escape
  - Accessing resources outside a VM's boundary
    - Memory, storage, processing

VIRTUAL ENVIRONMENT VULNERABILITIES

- Hypervisor vulnerabilities
  - DoS
  - Code execution
  - Memory corruption
  - VM escape

VIRTUAL ENVIRONMENT VULNERABILITIES

- VM repository vulnerabilities
  - Altering trusted images with malicious ones
  - Potentially easy way to trick users into running malware

CONTAINERIZED ENVIRONMENT VULNERABILITIES

- Vulnerabilities related to containerized workloads
  - Workload remote access
  - Access to sensitive data and resources
  - Elevated privileges
  - Host escape

QUICK REVIEW

- Virtual machine (VM) escape is accessing resources outside a VM's boundary
- VM repositories can have trusted images replaced with malicious ones
- Containerized workloads vulnerabilities include remote access, access to sensitive data and resources, elevated privileges, and host escape

Episode 7.05 – Labtainers Lab (Industrial Control System)

Objective 3.5 Explain common attacks and vulnerabilities against specialized systems