



@WIST



Cyber security Basics



Mobile Application Security

Importance of Mobile Application Security

- To ensure mobile applications are developed with security in mind.
- To be able to spot a malicious application.
- To ensure you comply with mobile security standards e.g. OWASP
- To ensure the user's data is secured and confidentiality is maintained.
- To protect the application and the service from malicious attackers.
- To be able to build well secured mobile applications.

Mobile security contd...

Mobile Threats – OWASP top 10

- M1 – Improper platform usage : Misuse of a platform feature or failure to use platform security controls e.g. platform permissions.
- M2 – Insecure data storage : Insecure data storage and unintended data leakage.
- M3 – Insecure communication : Incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.
- M4 – Insecure authentication : Failing to identify the user at all when that should be required or failure to maintain the user's identity when it is required, etc.

Mobile security contd...

- M5 – Insufficient cryptography : The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way.
- M6 – Insecure authorization : This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.).
- M7 – Client code quality : This would be the catch-all for code-level implementation problems in the mobile client e.g. buffer overflows - an anomaly where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory locations.

Mobile security contd...

- M8 – Code tampering : This covers dynamic memory modification, method hooking etc. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.
- M9 – Reverse engineering : This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets.
- M10 – Extraneous functionality : Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. e.g . a developer disabling of 2-factor authentication during testing.

WEB Application Security

Basic understanding of how the web works:

When you visit a website, your computer sends a message to the website's server requesting the contents of the website. The server responds in a format called HTML, which your browser renders to display the webpage. In this case, your request to the server is known as a "GET" request, because you are requesting to get information from the server. This is in contrast to other methods such as a "POST" request, which takes actions or modifies information. The request to get information from

Digital Forensics

Scope:

1. Definition
2. Areas Applicable
3. Methods and Techniques
4. Digital Forensics Process
5. Case Study



1. Definition

Digital Forensics is the science of collecting, preserving, analysing and reporting the content of digital evidence.

1.b Branches:

-Computer forensics

-Cloud forensics

-Network Forensics

-Web attack investigation

-Mobile Forensics

-Malware

-Database forensics

-Email Investigation

-OS Forensics

2. Areas Applicable

- Criminal and civil investigations

b. Ways in which computers can be used in a crime

- Commission of a crime
- Store evidence of a crime
- Means to commit a crime
- Collaborate existing evidence
- Recovery of files

Q: What happens when a file is deleted?



Cont...

- Reconstructing information from damaged equipment

Q. What causes damage to digital devices?


- Test for changes to devices
- Malware and botnet research when trying to determine impacts

Live forensics	Definition: Live forensics, otherwise known as Live Response, attempts to discover, control, and eliminate threats in a live, running system environment.
Data Recovery	Data recovery is the restoration of data that has been damaged, deleted, or lost.
Password Recovery	Definition: It refers to the recovery of password-protected files that are rendered useless if the passwords are lost.
File Carving	A forensics technique that uses file contents, rather than file metadata, to find or recover said file.
Known File Filtering	Known file filtering is a common forensics technique used to locate only relevant files by filtering out irrelevant artifacts.
String and Keyword Searching	In digital forensics, string and keyword searching is exploited, which can help identify pertinent data, as well as the source of potential threats.
Header Analysis	Header analysis enables investigators to analyze email headers, which can point to the IP address of the source email, as well as fix delays in email delivery.
Time line analysis	The analysis of events in chronological order that either led to, or followed the main event under investigation.

3. Tools and Techniques

- EnCase
 - FTK
 - Autopsy
 - Oxygen Forensics
 - Cellebrite
 - .XRY
 - Nuix
- Relativity

4.Digital Forensic Investigation Process

Acquiring 	The process of capturing original digital media from a source, using forensic tools that create a bit by bit copy of the suspect's media drive. Employs write protect precautions to avoid corruption. Involves file hashing to authenticate integrity.
Preserving	Involves protecting physical media as well as preserving a paper trail of the media
Analysis	Analysis of digital data using forensic tools and techniques. Documents, pictures, deleted files are subjected to analysis.
Reporting	Making of conclusions and presentation of findings.

Reverse Engineering

DEFINITION:

Process of taking something apart such as a device, an electronic component or software and analysing it in detail to see how it works.

Why reverse engineer?

- Identify system components and their interrelations
- Find security flaws
- Cloning purposes

Reverse engineering contd....

REVERSE ENGINEERING TOOLS

- Disassemblers and debuggers
- Prior programming knowledge

APPROACHES

Black-box testing

Examine the functionality of a software depending on its specifications and without peering into its internal workings or structures.

Reverse engineering contd....

White box testing

Test the internal workings or structures of a software as opposed to functionality.

DISCLAIMER!!

Patents and copyrights

SOC Analysis

SOC(Security Operation Center) is a centralized command center for network security event monitoring and incident response.(24x7/365 days)

Uses SIEM - Security Information Event Management is a software which aggregates and correlates security events data from different data sources. E.g. QRadar, Splunk, LogRhythm, ArcSight, SolarWinds, AlienVault

Data Sources: laptops, servers, routers, switches, firewall, IPS, Antivirus, users, cloud, applications, IOT, Threat Intelligence feeds etc

Roles in a SOC: SOC Analyst L1, L2, L3

SOC Analysis Cont...

SOC Analyst Role:

- Continuously monitors the alert queue
- Triage security events - Objective is to identify who, what, when, where, why, how of a security incident.
- Monitors the health of the security sensors and endpoints
- Consolidates data required for deep investigation by a SOC L2/L3 analyst

SOC Analysis Cont...

Incident Response Process:

1. Preparation
2. Identification
3. Containment
4. Eradication
5. Recovery
6. Lessons Learned



Introduction to Hardware Security



Hardware Security

- **What is hardware security?**

- It is the analysis of hardware components or physical devices rather than software in order to identify exploitable vulnerabilities that may affect Confidentiality, Integrity and Availability (CIA)
- It is also the future of security as most software based vulnerabilities can be fixed or prevented by implementing hardware controls.

- **Why is hardware security a current target?**

- Any technology based device requires a hardware component
 - Targeted Devices
 - Biometric systems
 - Mobile devices, Computers, Networking devices, laptops etc.
 - Home appliances
 - IOT based devices

Hardware Security

- **How do hackers assess hardware based vulnerabilities?**

- Analyzing hardware components by using:
 - Hardware manuals that can be retrieved online
 - China can clone any device --> **Easy access to a test model**
 - Easy access to tools that can read and decode hardware device signals

- **Examples of hardware hacking?**

- **The Spectre and Meltdown bug** - Hardware vulnerability existing in Intel, AMD and ARM processors which can be exploited by malicious programs to extract data from memory.
- **Miura M010 card readers** - Hardware vulnerability that allows an attacker to intercept transaction data via bluetooth and also downgrade software.
- Bloomberg alleges that china embeds spy-chips as a means of infiltrating USA - **Rejected Theory**

Hardware Security - Skills Required

- **What skills do you need?**

- Understanding electronic components and building electronic circuits
 - Tools: Arduino / Raspberry PI
- Experiment with broken down devices
- Sniff signals or data transmitted by the target device
- Learn how to read and recreate schematic diagrams

Hardware Security - **Assessment Categories**

- **What are the categories of hardware security assessment?**
 - **Modifying and/or Extending hardware modules**
 - **Example:** Attaching a USB cable to a computer (USBHarpooning)
 - **Firmware Modification:** Modifying hardware or software to manipulate how data or signals are transmitted or encrypted.
 - **Firmware Exploitation:** Exploiting vulnerabilities existing on the firmware
 - **Exploits:** Eavesdropping, Man-in-the-Middle attacks

Hardware Security - Categories of Attacks

- Hardware Modification
- Firmware Modification
- Remote Firmware Attack
- Attack Persistence
- Traffic Sniffing
- Surveillance
- Data Tampering / Spoofing
- Information Access

- Malfunctions
- Denial of Service
- Modification of Services
- Property Losses
- Destruction of Hardware
- Loss of Compliance
- Waste of Resources

Hardware Security - Module Categories

AUTHENTICATION

- Passwords
- Biometric Information
- Multi-factor authentication details
- Encryption keys

HARDWARE

- Internal Interfaces
 - PCMCIA, Memory/SD Cards, Display interfaces, NIC and cabling, Power supply and charger, eSATA etc.
- External Interfaces
 - USB, Audio, Battery, Debugging ports, SATA/IDE/SCSI etc.

FIRMWARE

- CPU and Baseband Processor
- Battery
- Hard drive
- USB Media
- Smart Chargers
- Memory/SD Cards
- Network Interface Cards
- Co-processors/SIM/HSMs
- Main Board Controller/Bios

LOGICAL OPERATIONS

- Update Functions
- Monitoring & Diagnostics
- Authentication Processes

PHYSICAL OPERATIONS

- Energy
- Access
- Cooling
- Heating
- Monitoring

USER INFORMATION & PRIVACY

- Behavioural data
- Biometric Information
- Availability Information
- Personal/Location/Health data
- Configuration Device Information

Hardware Security - Threat Landscape

	Malicious Abuse	Intercepting Dat
Threat	<ul style="list-style-type: none">• Exploiting firmware vulnerabilities• Abusing update functionality• Abusing binary firmware loading mechanisms• Memory Corruption Vulnerabilities• Logical Flaws• Backdoor Functionality• Remote management functionality	<ul style="list-style-type: none">• Traffic Sniffing: Network Level, Internal Bus Level and Memory Level• Surveillance: Location, Audio, Visual data Behaviour• Data Tampering/Spoofing: Location, Behaviour e.t.c.
Potential Effects	<ul style="list-style-type: none">• Information integrity• Information confidentiality• Information destruction• Software asset integrity• Service availability• Service functionality• Outage	<ul style="list-style-type: none">• Information integrity• Information confidentiality• Information destruction
Asset Types	<ul style="list-style-type: none">• Logical Operations• Physical Operations• Hardware• Firmware	<ul style="list-style-type: none">• User information and privacy

Hardware Security - Threat Landscape

	Physical Attacks	Damage
Threat	<ul style="list-style-type: none">• Hardware Modification• External and Internal Hardware Trojan• Temporary hardware access for system modification• Property Losses:<ul style="list-style-type: none">◦ Access control bypass◦ Disabling of monitoring/alerting	<ul style="list-style-type: none">• Destruction of Hardware: Overheating, Explosion, Bricking, Disabling of interfaces• Waste/destruction of Resources: Excessive Heating/use of heat, Excessive energy consumption, Excessive use of resources
Potential Effects	<ul style="list-style-type: none">• Information integrity• Information confidentiality• Software asset integrity• Service functionality• Property availability• Property destruction	<ul style="list-style-type: none">• Property availability• Property destruction• Environment harm• User harm
Asset Types	<ul style="list-style-type: none">• Logical Operations• Physical Operations• Hardware• Firmware• User Property	<ul style="list-style-type: none">• User Property• Physical Operations• User Health• Physical Operations• Hardware

Hardware Security - Threat Landscape

	Failures and Malfunctions	Outages
Threat	<ul style="list-style-type: none">• Failure of devices• Overheating/explosion of batteries• Failure of access systems• Failure of alarm systems• Wrong device usage• Outage or False negative reporting by alarm/monitoring systems	<ul style="list-style-type: none">• Denial-of-Service<ul style="list-style-type: none">◦ Flooding/volumetric attack◦ Software bug/exploit◦ Logical flaw
Potential Effects	<ul style="list-style-type: none">• Property availability• User harm	<ul style="list-style-type: none">• Service availability• Outage• User harm
Asset Types	<ul style="list-style-type: none">• User Property, Health, Information and Privacy• Logical and Physical Operations• Hardware• Firmware	<ul style="list-style-type: none">• User Property and Health• Logical and Physical Operations

Hardware Security - Threat Landscape

	Legal
Threat	<ul style="list-style-type: none">• Loss of Compliance• Avoidance of certification/validation approvals• Violation of contractual requirements• Violation of internal/external compliance requirements• Violation of data protection laws
Potential Effects	<ul style="list-style-type: none">• Software asset integrity• Service availability• Reputation damage
Asset Types	<ul style="list-style-type: none">• Logical Operations• Physical Operations

References: www.enisa.europa.eu

Publication: Hardware Threat Landscape



Introduction to Malware Analysis