Ali Bouanane & Zine eddine Tabbech

# MOBILE APP FORENSICS:

## INVESTIGATING SUSPICIOUS ACTIVITIES THROUGH STATIC AND DYNAMIC ANALYSIS

# Introduction to Mobile App Forensics

Mobile app forensics involves extracting, preserving, and analyzing data from mobile applications.

It examines both static data (code, configuration, resources) and dynamic data (runtime behavior, network interactions).

# Ethical & Legal Boundaries in Mobile App Development (GDPR & CCPA Compliance)

## OVERVIEW

Mobile applications must comply with strict privacy laws and ethical standards to protect users. Regulations like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) set clear guidelines on what app developers can and cannot do.

# Examples of Rules That Shouldn't Be Broken

1. **Unauthorized Data Collection** & Data Exfiltration
2. Spying on Users Recording audio, taking pictures ...
3. Weak or No Encryption for Sensitive Data
4. Excessive or Unjustified Permissions
5. Malicious Behavior (Backdoors, Keylogging, etc.)
6. Privacy Violations via Third-Party SDKs(game app sending user behavior data to an ad company)

## Pentesting Focus 🔍→🛡️

**What it does:** Finds app weaknesses **before** hackers can exploit them.

**Example:** Tracing weaknesses to improve app security ,e.g: encryption or insecure API calls.

## Forensic Utility 🕵️→🔎

**What it does:** Investigate security incidents and collect evidence **after** attack

**Example:** Spoting Illegal activities , e.g: Analyzes network traffic and API calls to see how data was stolen

## Key Difference: ⏰ Timing

🛡️ Before an Attack

🔍 After an Attack

**Forensics** is about investigation, while **penetration** testing is about prevention.

# what is MOBSF?

Mobile Security Framework (MobSF) is an open-source tool for automated static and dynamic analysis of mobile applications (APK/IPA).

# When & How MobSF Transitions to Forensic Analysis

**MobSF** primarily focuses on penetration testing, but it is also considered forensic tool in scenarios when there is no physical evidence or when an app exhibits suspicious activity, violating compliance or legal licenses. In such cases, traditional forensic tools like **Autopsy**, **Cellebrite**, and **Magnet AXIOM** won't help, leaving **MobSF** as the only option to uncover every detail about the app.

# Deep Dive into Static Analysis with MobSF

**Static analysis examines an app's package (APK/IPA) without executing it, revealing its structure, permissions, and vulnerabilities**

## How MobSF Performs Static Analysis:

- ✅ App Decompilation: Extracts source code and resources for analysis.
- ✅ Manifest & Permissions Analysis: Flags dangerous permissions and components.
- ✅ Code & API Analysis: Identifies insecure coding practices and API calls.
- ✅ Hardcoded Secrets Detection: Finds embedded credentials, API keys, and secrets.
- ✅ Obfuscation & Encryption Analysis: Detects obfuscation techniques and weak encryption methods.
- ✅ File & Binary Analysis: Checks for suspicious executables, libraries, and embedded files.

# Deep Dive into Dynamic Analysis with MobSF

**dynamic analysis observes an app's behavior in real time by executing it in a controlled environment**

## How MobSF Performs Dynamic Analysis:

- ✅ Sandbox Execution: Runs the app in an emulator to monitor runtime behavior.
- ✅ API Call Monitoring: Logs API interactions to detect unauthorized access.
- ✅ Network Traffic Inspection: Captures outbound/inbound traffic to detect data leaks.
- ✅ Behavioral Analysis: Flags suspicious activity like background tracking or hidden communications.
- ✅ Memory Dump & Hooking: Extracts volatile data and intercepts app functions.

# Real world examples

🔄 Unauthorized Data Transfer:
Uber was fined £245M for transferring drivers' personal data to U.S. servers without proper safeguards.

🔒 Lack of Data Security & Breach:
LinkedIn faced a fine of €310M for processing and storing user data without adequate security measures.

🍪 Cookie Consent Violations:
Amazon was fined €746M for not obtaining proper user consent before storing and using cookies for data tracking.

👤 Excessive Data Collection via Third Parties:
Clearview AI was fined €30.5M for scraping social media images without consent to build a biometric database.

🔐 Data Breach from Weak Security Measures:
Meta (Facebook) received a €251M fine for a data breach that exposed millions of user records due to insufficient security protocols.

# THANK YOU FOR LISTENING!