Lecture #14

Final Exam Review & Career Discussions

SMA 2025

Title Slide

Final Exam Review & Career Discussion

Preparing for the Exam and Your Future in Security

Today's Agenda

- **Part 1: Exam Logistics & Format** - Dates, times, and structure.
- **Part 2: Comprehensive Review** - A high-speed recap of Lectures 1-12.
- **Part 3: Sample Questions** - What to expect on the test.
- **Part 4: Career Paths** - Jobs, salaries, and certifications.
- **Part 5: Final Q&A** - Open floor for any remaining questions.

Exam Logistics

- **Date:** February 2nd, 2026
- **Time:** 13:00
- **Room:** 335 FSEGA
- **Duration:** 1 Hours
- **Format:** Closed Book, Closed Notes.
- **Weight:** 40% of Final Grade.

Exam Structure

- **Section A: Multiple Choice (20 Questions / 20 Points)**
- Tests basic knowledge and definitions.
- Explain concepts (e.g., "How does Certificate Pinning prevent MitM?").
- "Here is a description of an insecure app. Identify 3 vulnerabilities and propose fixes."

Topic 1: OS Architecture (Lectures 1-3)

- **Key Concepts:**
  - **Sandboxing:** How Android (UIDs) and iOS (Containers) isolate apps.
  - **Permissions:** Install-time vs. Runtime. The *AndroidManifest.xml* and *Info.plist*.
  - **IPC:** Intents, Binder, URL Schemes.
- Know the difference between the Zygote (Android) and Launchd (iOS).
- Understand how a malicious app can exploit an exported Activity.

Topic 2: Data Storage & Privacy (Lectures 4-5)

- **Key Concepts:**
  - **Insecure Storage:** Storing tokens in *SharedPreferences* or *UserDefaults* (Plaintext).
  - **Secure Storage:** *EncryptedSharedPreferences* and the iOS *Keychain*.
  - **External Storage:** The risks of SD cards and public directories.
- Why is base64 encoding NOT encryption?
- How do you securely delete data?

Topic 3: Network Security (Lecture 6)

- **Key Concepts:**
  - **TLS/SSL:** The handshake process. Why we need it.
  - **Man-in-the-Middle (MitM):** How attackers intercept traffic (Proxies, Rogue APs).
  - **Certificate Pinning:** The defense against CA compromise.
- Draw a diagram of a MitM attack.
- Explain the pros and cons of pinning.

Topic 4: Cryptography (Lecture 10)

- **Key Concepts:**
  - **Symmetric vs. Asymmetric:** AES vs. RSA/ECC. Speed vs. Key Management.
  - **Hashing:** SHA-256 vs. MD5 (Broken). Salting passwords.
  - **Key Management:** Storing keys in the Hardware-Backed Keystore (TEE/Secure Enclave).
- Never roll your own crypto.
- Which algorithms are currently recommended (AES-GCM, SHA-256, ECDSA).

Topic 5: Enterprise Security (Lectures 8-9)

- **Key Concepts:**
  - **MDM vs. MAM:** Device control vs. App control.
  - **BYOD:** The privacy/security trade-off.
  - **Containerization:** Android Work Profile.
- How does an organization protect data on a device they don't own?
- What is a "Remote Wipe"?

Topic 6: IoT & Future Trends (Lectures 11-12)

- **Key Concepts:**
  - **The Mobile Control Plane:** The phone as the key to the physical world.
  - **IoT Protocols:** MQTT, BLE, Zigbee.
  - **5G & AI:** Network slicing, Deepfakes.
- Why is IoT security often weaker than mobile security?
- What is the "Post-Quantum" threat?

Sample Question: Multiple Choice

Question: Which of the following is the **safest** place to store an API Key on Android?

A) *strings.xml*

B) *SharedPreferences* (Plaintext)

C) *EncryptedSharedPreferences*

D) Hardcoded in Java source code

Sample Question: Multiple Choice

Question: Which of the following is the **safest** place to store an API Key on Android?

A) *strings.xml*

B) *SharedPreferences* (Plaintext)

C) *EncryptedSharedPreferences*

D) Hardcoded in Java source code

Answer: C) *EncryptedSharedPreferences*

Sample Question: Short Answer

Question: Explain the concept of "Certificate Pinning" and why an app developer might implement it. What is the primary risk of implementing it incorrectly?

Answer Key:

- **Definition:** Hardcoding the expected server certificate (or public key hash) in the app.
- **Why:** To prevent MitM attacks even if a Certificate Authority (CA) is compromised or if the user installs a malicious root cert.
- **Risk:** "Bricking" the app. If the server rotates its certificate and the app isn't updated, the app will stop connecting.

Sample Question: Scenario Analysis

Scenario: You are auditing a banking app. You find that it saves the user's password in a local SQLite database to enable "Auto-Login." The database is not encrypted.

Task:

- Identify the vulnerability.
- Explain the impact if the phone is stolen.
- Propose a secure solution for "Auto-Login."

Answer Key:

- **Vuln:** Insecure Data Storage (CWE-312).
- **Impact:** Attacker can extract the password and access the account from any device.
- **Fix:** Do NOT store the password. Use a **Biometric Token** stored in the Keystore/Keychain, or use an OAuth Refresh Token stored in EncryptedSharedPreferences.

Part 2: Career Paths in Mobile Security

Where do you go from here?

The Roles

- **Mobile Application Security Engineer (Blue Team):**
- **Role:** You work with developers to build secure apps. You review code, design crypto features, and run tools like MobSF.
- **Skills:** Kotlin, Swift, Java, Secure Coding standards (OWASP MASVS).
- **Role:** You are hired to break apps. You decompile, intercept traffic, and write exploits.
- **Skills:** Frida, Burp Suite, Reverse Engineering (Ghidra/JADX).
- **Role:** You design the big picture. How does the Mobile App talk to the Cloud? How do we handle Identity?
- **Skills:** Threat Modeling, Cloud Security, IAM (OAuth/OIDC).

Certifications to Consider

- **GMOB (GIAC Mobile Device Security Analyst):**
- **Focus:** Comprehensive mobile security (Android & iOS).
- **Verdict:** The "Gold Standard," but very expensive. Good for corporate training.
- **Focus:** Practical exploitation. You have to write a malicious app to pass.
- **Verdict:** Excellent value and very hands-on.
- **Focus:** General network pentesting.
- **Verdict:** Not mobile-specific, but the most respected cert in the industry. It proves you have the "Try Harder" mindset.

Building Your Portfolio

- **GitHub:**
- Upload the projects you built in this class (e.g., the Secure Notes App).
- Write a "Readme" explaining the security features you implemented.
- Sign up for HackerOne or Bugcrowd.
- Try to find bugs in real apps (that have safe harbor policies!).
- Even a "Duplicate" finding shows you know how to look.
- Start a blog. Write about a CTF challenge you solved or a vulnerability you studied.

The Community

- **OWASP (Open Web Application Security Project):**
- Contribute to the MSTG (Mobile Security Testing Guide).
- DefCon / BlackHat (Vegas).
- AppSec Global.
- BSides (Local, cheaper, often better for networking).

Final Advice

- **Stay Curious:** Technology changes every 6 months. You have to keep learning.
- **Ethics Matter:** You have powers now. You can steal data, track people, and break systems. **Don't.** Use your skills to protect.
- **Think Like an Attacker:** The best defenders know exactly how the attack works.

Q&A

Questions?

Thank You!

Good luck!