Web and Mobile Application Security

Chapter 8 — Mobile Security

Mr Laïdi FOUGHALI

l.foughali@univ-skikda.dz

(Website ⇒ www.al-moualime.com)

University of Skikda — Computer Science Department

2nd Year Master in Information Security (IS)

Academic Year 2026-2027

Updated on 2026-09-22 at 23:41:52

Outline

Chapter objectives

By the end of this chapter, you will be able to

- Introduce mobile technologies and their ecosystem
- Understand the mobile platform security model
- Identify threats to applications, mobile networks, and privacy
- Know the role of encryption and best practices

8.1 — Mobile computing technologies

The mobile ecosystem

- Platforms: Android, iOS
- Native, hybrid, or Web applications
- Network evolution: 1G → 4G/LTE → 5G

4G architecture — two security domains

- **Access stratum** : between the device and the base station (eNB)
- **Non-access stratum** : between the device and the mobility management entity

All-IP and virtualization have broadened the attack surface.

8.2.1 — Mobile platform security model

Isolation and control

- Every application isolated in a **sandbox**
- Permission model
- Mandatory signing of applications distributed through stores

Android permissions

Normal (automatically granted) vs. **dangerous** (location, contacts, mic, camera, etc.) — explicit consent required.

8.2.2 — Threats to mobile applications

m-health study: alarming figures

- **95.63%** of applications pose a privacy risk
- **63.6%** send unencrypted data
- **55%** transmit the password, **45%** via a GET request
- **50%** transmit data to third parties

Source: Papageorgiou *et al.*, 2018

8.2.2 — The role of encryption

Common cryptographic weaknesses

- ECB mode, non-random IVs, static keys/salts
- Obsolete algorithms: DES, RC4, MD5, SHA-1
- GET requests instead of POST for sensitive data

Encryption protects

Data **at rest** (storage) and **in transit** (network) — if used correctly.

8.2.3 — Privacy and personal data

Failing privacy policies

10% of analyzed applications had no privacy policy reference at all; others were invalid or misleading.

Regulatory framework

Health data, location, contacts: regulated by the **GDPR** (consent, transparency, minimization, right to erasure) — often poorly met in practice.

8.2.4 — Threats to mobile networks

Classification by targeted property

- **Confidentiality** : interception, eavesdropping, identity tracking
- **Integrity** : message tampering
- **Availability** : denial of service, flooding
- **Authentication** : device/equipment impersonation

Entry points

Access network, core network, third-party networks (roaming, WLAN) — spoofing, MITM, eavesdropping, jamming.

8.2.5 — Automatically generated applications

"Citizen" development

Online Application Generators (OAGs) produce applications quickly with no security expertise.

Amplification effect

A single vulnerability in the generator **automatically** propagates to every application it produces — potentially thousands.

Source: Oltrogge *et al.*, 2018

8.2.6 — Countermeasures and best practices

To apply systematically

- Encrypt sensitive data (at rest and in transit)
- Principle of least privilege for permissions
- Properly configured TLS, validated certificates
- Valid privacy policy, limited sharing
- Official distribution, signing, updates
- Code audit, including auto-generated code

Key takeaways

The essentials of this chapter

- Sandbox, permissions, and signing isolate mobile applications
- Encryption is often absent or poorly implemented (ECB, fixed IVs, etc.)
- Privacy is threatened by undisclosed data sharing
- Mobile networks face 4 types of attacks (C/I/A/Auth)
- Application generators propagate vulnerabilities at scale

Questions and exercises

To practice

1. Describe Android's permission model (normal vs. dangerous).
2. Give three examples of cryptography misuse in mobile.
3. Classify four mobile network attacks by targeted security property.
4. How do application generators propagate vulnerabilities at scale?
5. Explain the role of encryption for data at rest and in transit.