ITMC411

Security in mobile computing

LECTURE 5

Mobile Application (In)security

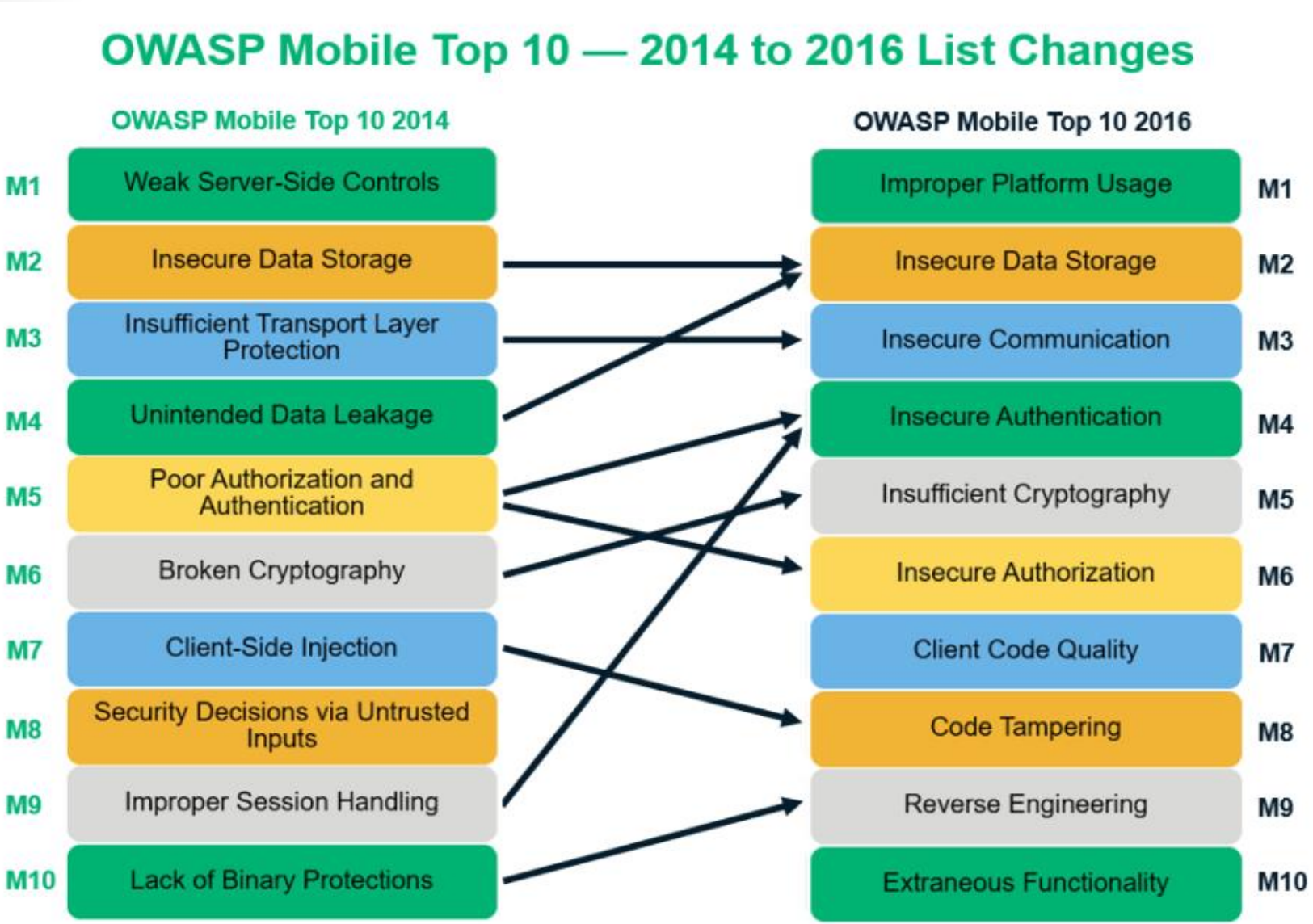
Attack Surface

- **Network communications**
  - Often public Wi-Fi
- **Device theft**
  - Locally stored data
- **Malicious apps on the phone**
  - Often from Google Play
- **Other input sources**
  - NFC, Bluetooth, camera, microphone, SMS, USB, QR codes

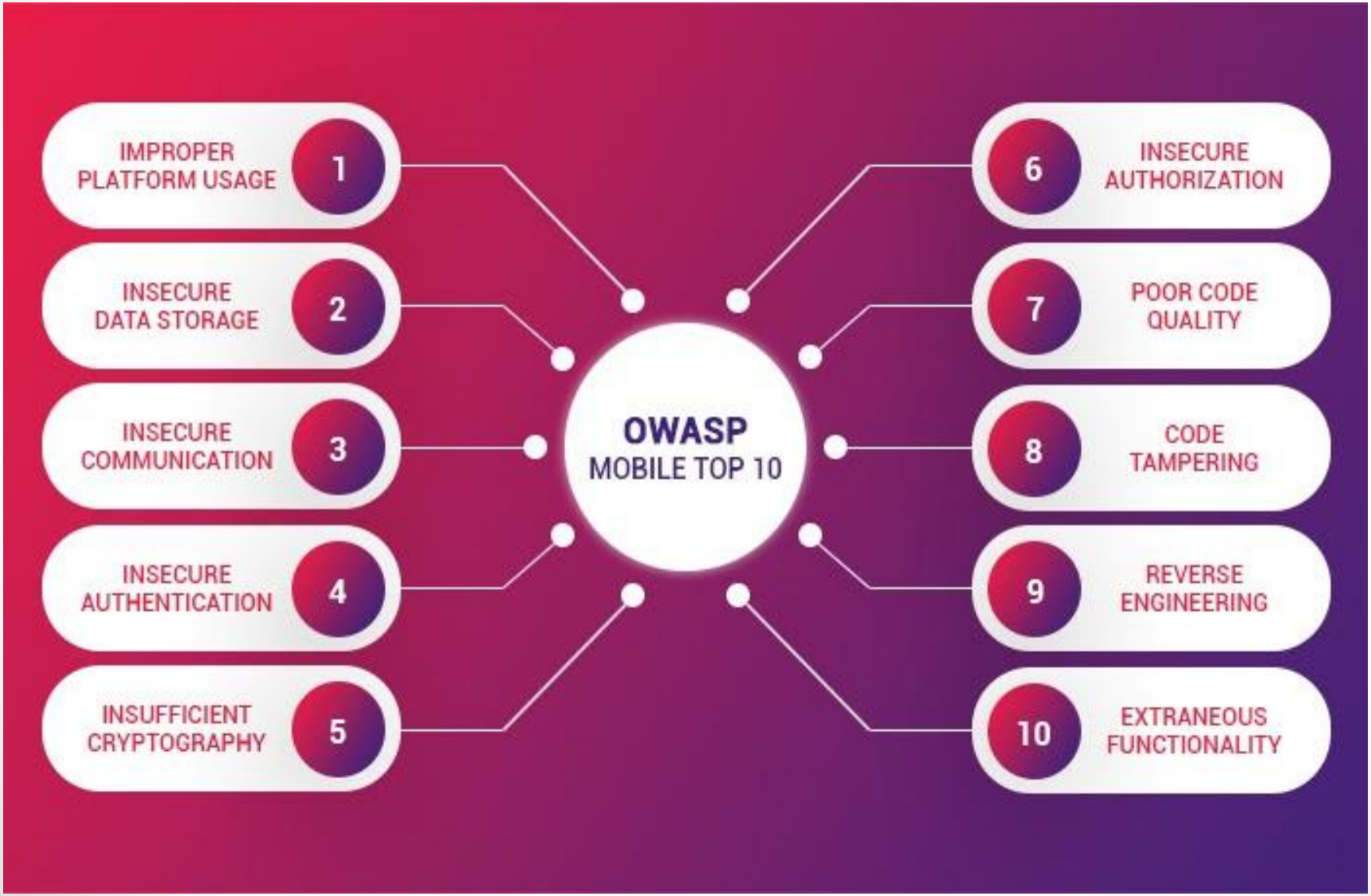
Key Problem Factors

- **Underdeveloped security awareness**
  - By developers
- **Ever-changing attack surface**
- **Custom development**
  - **In-house code** mixed with **libraries** from many sources

OWASP Top Ten



OWASP Top Ten-2016



OWASP Top Ten

- **M1: Improper Platform Usage**
  - Violation of published guidelines.
  - Violation of convention or common practice
  - Unintentional Misuse
- **M2: Insecure Data Storage**
  - Plaintext or obfuscated

OWASP Top Ten

- **M3: Insecure Communication**
  - Failure to validate **TLS certificates**

- **M4: Insecure Authentication**
  - App is able to anonymously **execute** a **backend API service** request without providing an **access token**.
  - App stores any **passwords** or shared secrets **locally**.
  - App uses a **weak password** policy
  - App uses a feature like **TouchID**

OWASP Top Ten

- **M5: Insufficient Cryptography**
  - **Poor** Key Management Processes
  - Creation and Use of **Custom Encryption Protocols**
  - Use of **Insecure** and/or **Deprecated Algorithms**

- **M6: Insecure Authorization**
  - Presence of **Insecure Direct Object Reference** (**IDOR**).
  - Hidden Endpoints
  - User **Role** or **Permission** Transmissions

OWASP Top Ten

- **M7: Poor Code Quality**
  - **Format-string** vulnerabilities,
  - **Buffer overflows**,
  - Integration with insecure **third-party libraries**,
  - Remote Code Execution (**Code Injection**)
- **M8: Code Tampering**
  - Make **direct binary changes** to the application package's **core binary**
  - Make **direct binary changes** to the resources within the **application's package**
  - **Redirect** or **replace** system **APIs** to intercept and execute foreign code that is malicious

OWASP Top Ten

- **M9: Reverse Engineering**
  - understand the contents of a **binary's string table**
  - perform **cross-functional analysis**
  - Derive a reasonably **accurate recreation** of the source code from the binary.

M10: Extraneous Functionality

- The defining characteristic of this risk is **leaving functionality enabled** in the app that **was not** intended to be **released**.

OWASP Mobile Security Tools

- **iMAS**
  - Framework to develop secure **iOS apps**
- **GoatDroid, iGoat, DV iOS**
  - Deliberately insecure apps **for practice**
- **MobiSec**
  - Mobile pentesting distribution, like Kali
- **Androick**
  - For Android forensics

References

Top 10 Mobile Risks - Final List 2016

- https://owasp.org/www-project-mobile-top-10/

OWASP Mobile Top 10: A Comprehensive Guide For Mobile Developers To Counter Risks

- https://www.appsealing.com/owasp-mobile-top-10-a-comprehensive-guide-for-mobile-developers-to-counter-risks/

OWASP Mobile Top 10 Vulnerabilities & Mitigation Strategies

- https://sectigostore.com/blog/owasp-mobile-top-10/