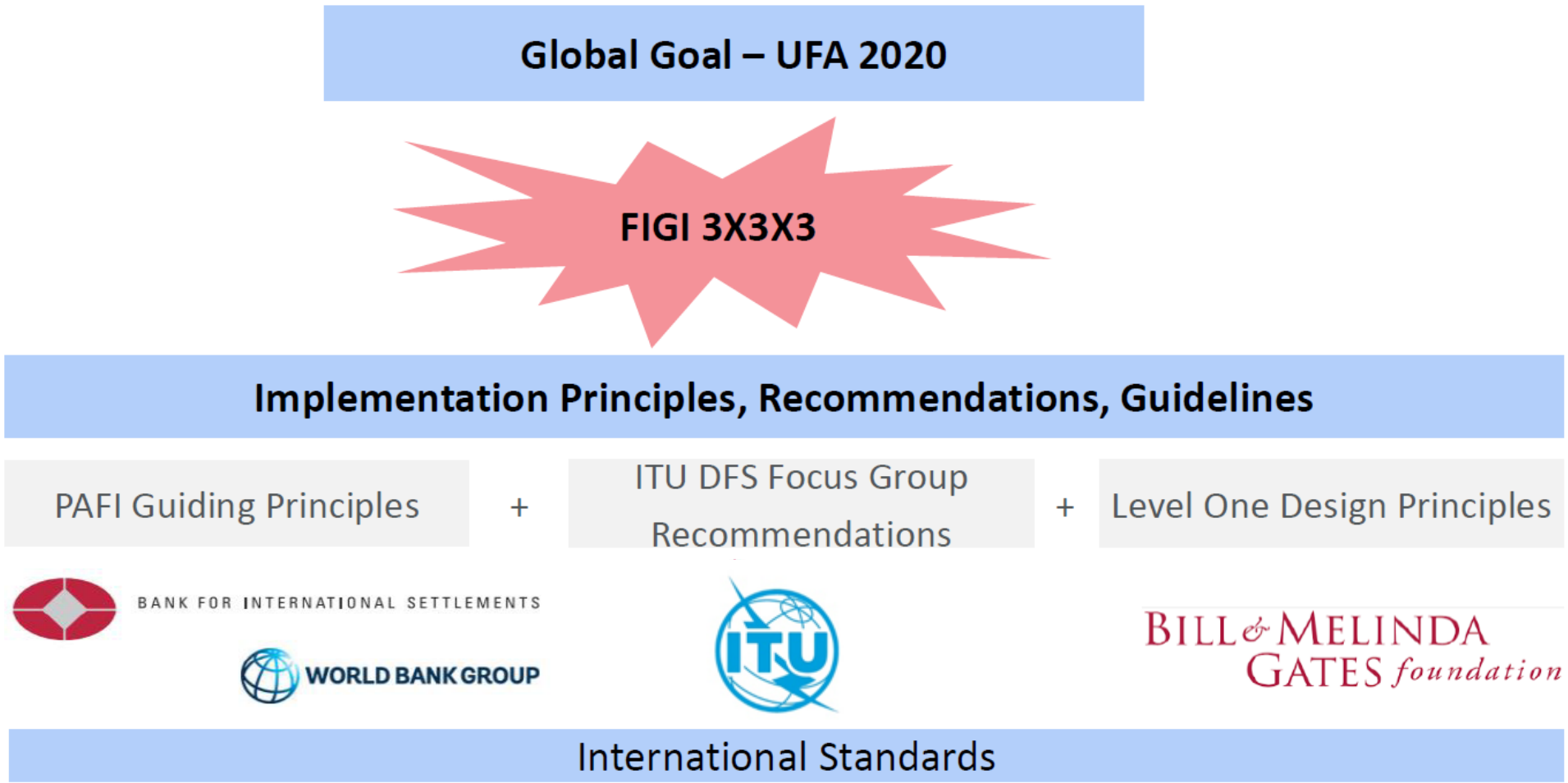
ITU DFS Security Lab

Vijay Mauree, Programme Coordinator, ITU

28 October 2021

Financial Inclusion Global Initiative (FIGI)



www.figi.itu.int/figi-resources/dfs-security-lab/

FIGI Security Infrastructure & Trust Working Group

Security, Infrastructure & Trust Working Group workstreams

Working Group Reports

Security Workstream

Address DFS application security, telecom infrastructure security issues, consumer authentication and cybersecurity risk management.

Trust Workstream

Address unlicensed digital investment schemes, digital skills for users, and innovations and risks that AI and big data pose when used in financial inclusion.

Quality of Service Workstream

Develop methodology for measurement of key performance indicators (KPIs) for QoS and QoE for DFS

Distributed Ledger Technologies Workstream

Use of distributed ledger technology to secure digital financial services transactions.

www.figi.itu.int/figi-resources/dfs-security-lab/

Problem statement

There is not a common approach for regulators, developers and DFS providers to test DFS mobile apps in a complex mobile ecosystem in order to provide/verify the level of assurance on security.

DFS Security Lab

Systemic vulnerabilities include those that can impact integrity and confidentiality of the transactions, for instance:

- The security communication protocols used (strength of ciphers).
- Secure user authentication
- Security checks on certificates
- Can the application be executed on rooted devices?
- Is consumer data privacy preserved?
- Is the source code properly obfuscated?

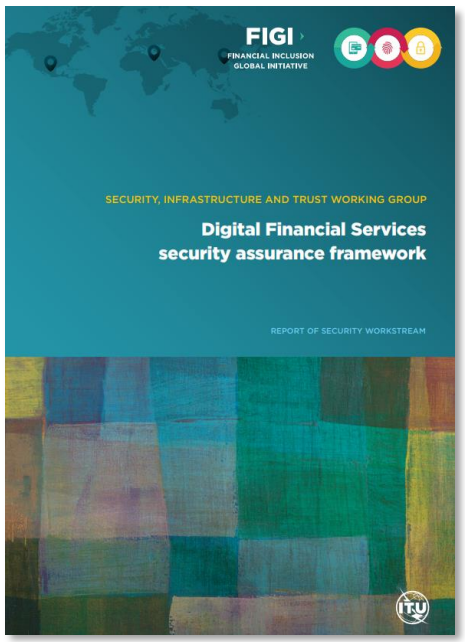
The DFS security lab provides a common methodology to conduct security audit for mobile DFS apps and address systemic vulnerabilities.

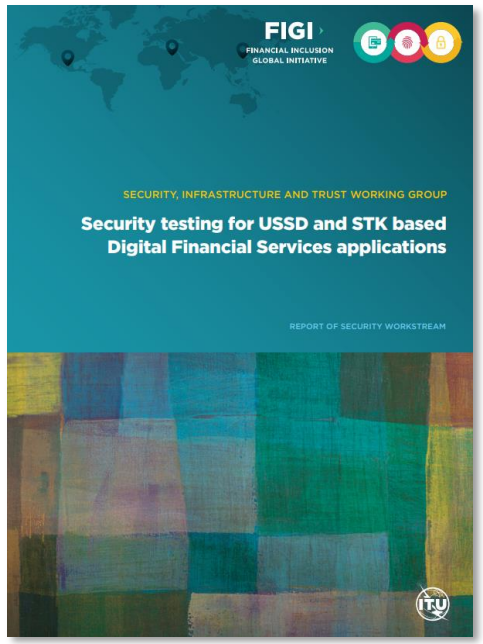
2019 Mobile App Vulnerabilities Study – Positive Technologies

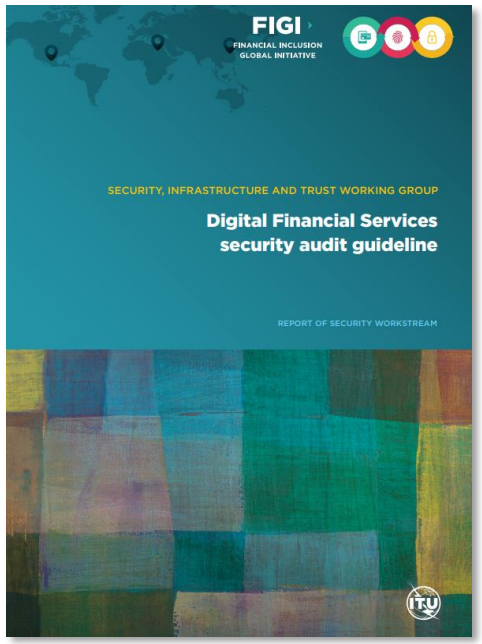
- High-risk vulnerabilities – 38% of mobile apps for iOS and in 43% of Android apps.
- Insecure data storage is the most common issue, found in 76% of mobile applications. Passwords, financial data and are at risk.
- Hackers seldom need physical access to a smartphone to steal data: 89 percent of vulnerabilities can be exploited using malware.
- 56% of vulnerabilities can be exploited without administrator rights (jailbreak or root)
- Most cases are caused by weaknesses in security mechanisms (74% and 57% for iOS and Android apps, respectively, and 42% for server-side components).
- Because such vulnerabilities creep in during the design stage, fixing them requires significant changes to code.
- Risks do not necessarily result from any one particular vulnerability on the client or server side. In many cases, they are the product of several seemingly small deficiencies in various parts of the mobile application.

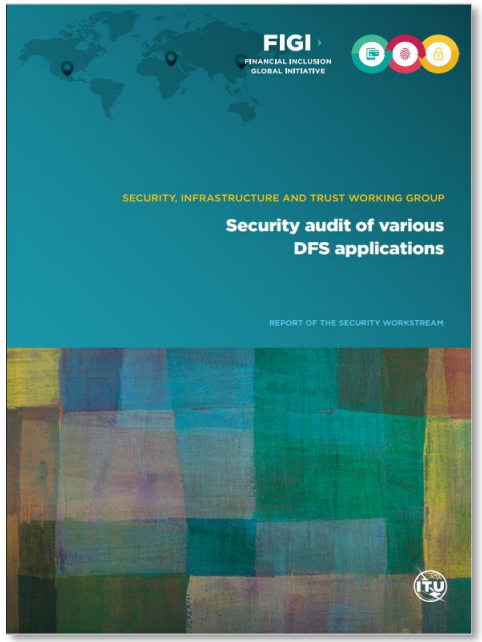
DFS Security Lab Objectives

Collaborate with DFS regulators and DFS providers to enhance the cybersecurity strategy for DFS and security assurance of the DFS ecosystem by implementing the recommendations in the DFS Security Assurance Framework, methodology for testing of USSD, STK and Android apps and DFS Security Audit Guidelines.









See *https://figi.itu.int/figi-resources/working-groups/*

DFS Security Lab Objectives

Collaboration with DFS regulators on security

Perform DFS **security audits** of DFS Apps

Encourage adoption of **international standards on DFS security**

Organise **security clinics**

Assist DFS regulators to evaluate the **cyber preparedness** for DFS ecosystem

Knowledge sharing on threats to security of DFS apps

DFS Security Lab Components

Security testing for **USSD** and **STK**

Developer resources for strong authentication using **Fast Identity Online** (**FIDO)**

Security audit of **Android** DFS apps using **OWASP** Mobile Top 10 Risks.

FIDO Developer Resources

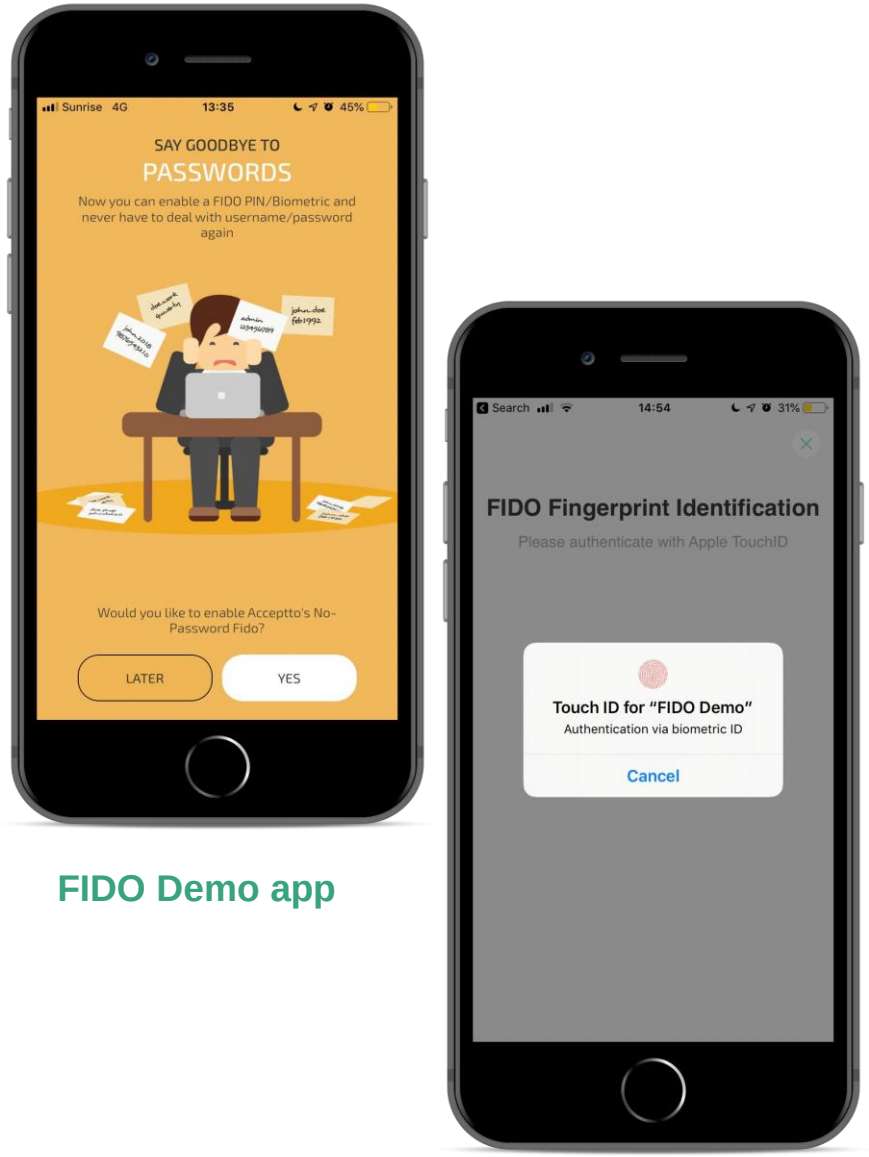
FIDO (Fast ID Online) is a set of technology-agnostic security specifications for strong authentication (passwordless authentication).

ITU Resources for developers

i. Step-by-step guide for deploying FIDO UAF on a native app

ii. FIDO UAF compliant server to test FIDO UAF authentication

iii. Sample Android and iOS FIDO demo client app to show user registration, deregistration, and transaction authentication.

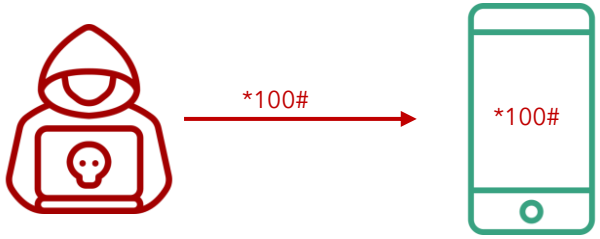


FIDO Demo app

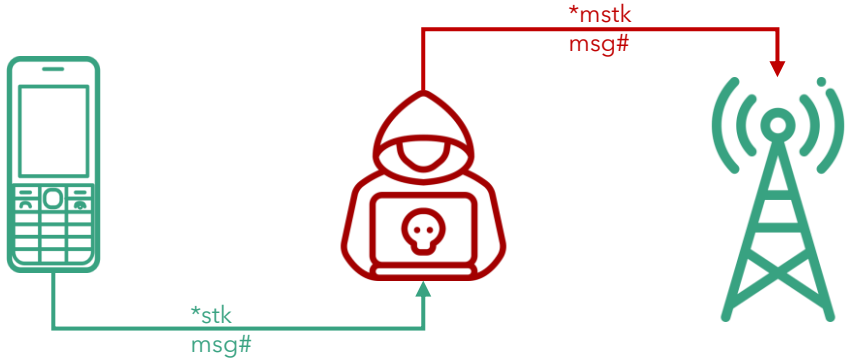
USSD & STK tests

a. **SIM Swap** and **SIM cloning**

b. susceptibility to **binary OTA attacks** (SIM jacker, WIB attacks)



c. **remote USSD** execution attacks

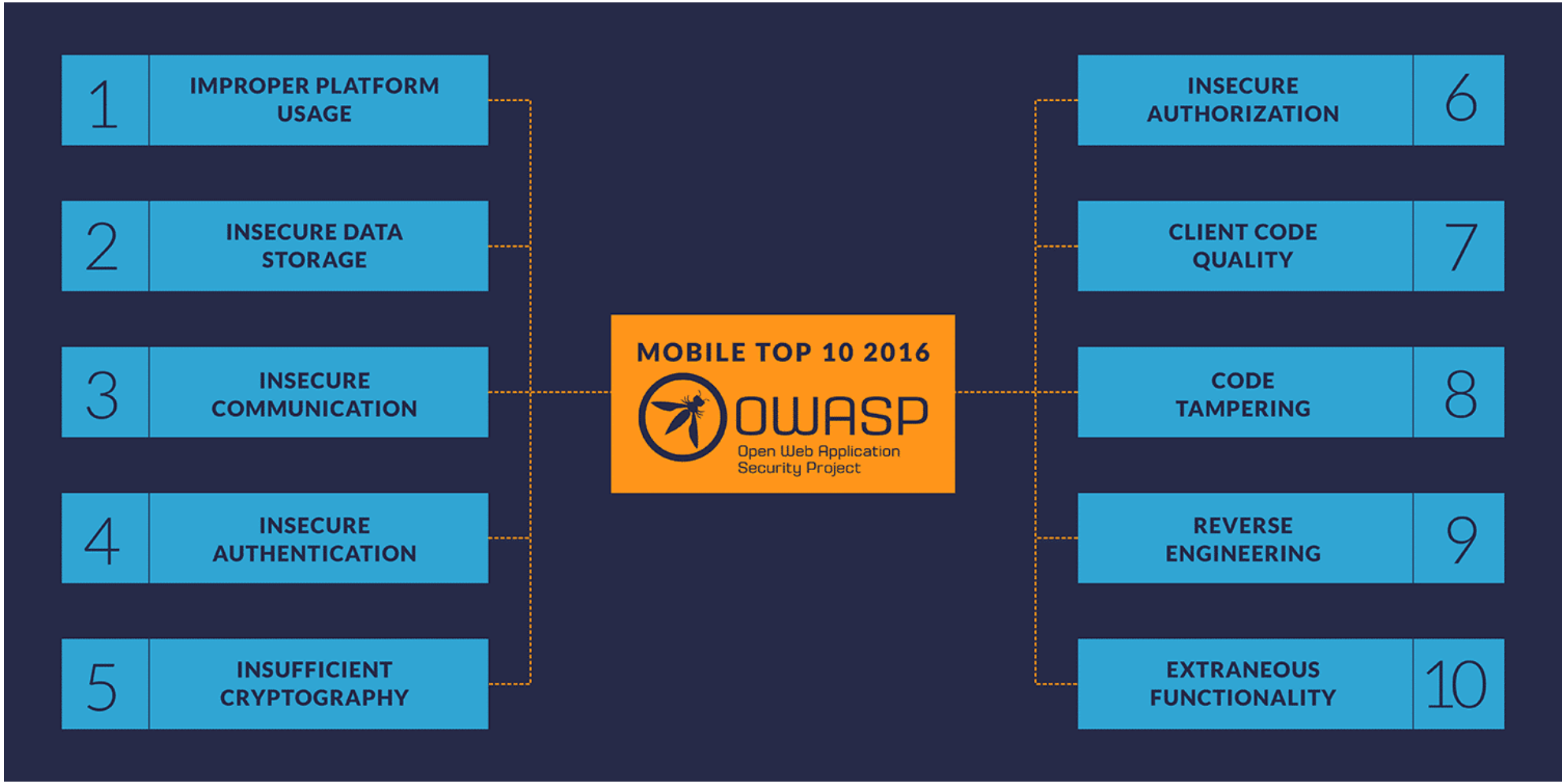


d. **man-in-the-middle attacks** on STK based DFS applications

Android Attack Points

- Data Storage
  - Keystores
  - Application Filesystem
  - Application Database
  - Configuration files
- Binary source code
  - Reverse engineering
  - Look for vulnerabilities in source code
  - Embedded credentials
  - Key generation routines
- Platform
  - Malware installation
  - Mobile botnets
- Data storage, source code and platform are interrelated
  - A weakness in one can lead to exploitation in another.

OWASP Mobile Top 10 Security Risks



Source: OWASP

Android app security tests

Risks	Security test
M1 Improper Platform Usage	Check misuse of platform features or failing to use platform security controls provided
M2 Insecure Data Storage	Check that malware and other apps do not have access to DFS sensitive information
M3 Insecure Communication	Check that communication channels are encrypted
M4 Insecure Authentication	Authentication cannot easily be bypassed
M5 Insufficient Cryptography	Check crypto algorithms used
M8 Code Tampering	Check whether it is possible to modify the code
M9 Reverse engineering	Decompile source code

Summary

1. DFS security lab provides a methodology to conduct security audit for mobile DFS applications
2. Collaborate with telecom regulators, Central Banks and DFS providers in emerging economies
3. Provide guidance on implementation of FIGI Security recommendations for DFS
    - Managing security risks to DFS from an application, infrastructure and incident response perspective
    - Security audits of mobile payment applications
    - Encourage adoption of security best practices and international standards for DFS
    - Enhance knowledge sharing on security threats and vulnerabilities regarding DFS among regulators at a regional and global level.

DFS Security Lab

Get in touch

dfssecuritylab@itu.int

https://figi.itu.int/figi-resources/dfs-security-lab/

www.itu.int