FIGI FINANCIAL INCLUSION GLOBAL INITIATIVE

FIGI Symposium
18 May - 24 June, 2021

DFS Security Lab: Assessing DFS Applications Vulnerabilities

Vijay Mauree, TSB, ITU

figi.itu.int
#financialinclusion

Organized by

Committee on Payments and Market Infrastructures | BIS | THE WORLD BANK IBRD • IDA | ITU

Overview

- FIGI Security, Infrastrcture and Trust WG
- DFS Security Lab
- Android Attack Vector
- DFS Security Tests
- Collaboration with DFS Regulators and Providers

FIGI Security Infrastructure & Trust Working Group

Security Workstream

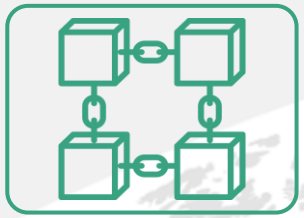
Address DFS application security, telecom infrastructure security issues, consumer authentication and cybersecurity risk management. Set up the DFS Security Lab.

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.

Outputs

- 16 Technical Reports
- DFS Security Lab
- Developer resources for FIDO

DFS Security Lab

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 against systemic vulnerabilities.

DFS Security Lab

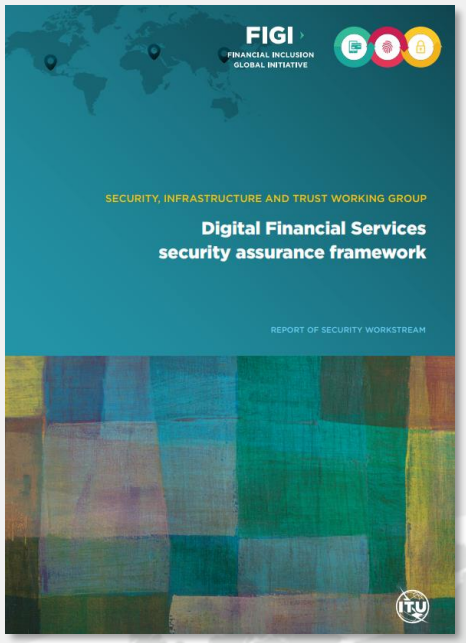
Systemic vulnerabilities include those that can impact integrity and confidentiality of the transactions, for instance:

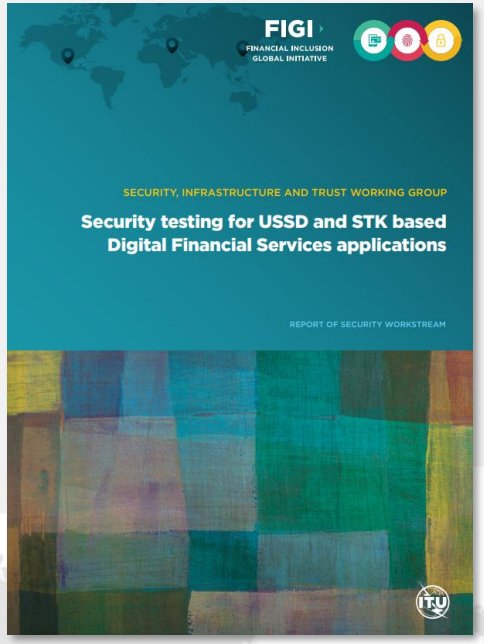
- ❑ The security communication protocols used (strength of ciphers).
- ❑ Secure user authentication
- ❑ Security checks on certificates
- ❑ Can it be run on rooted devices?
- ❑ Is consumer data privacy preserved?
- ❑ Is the source code properly obfuscated?

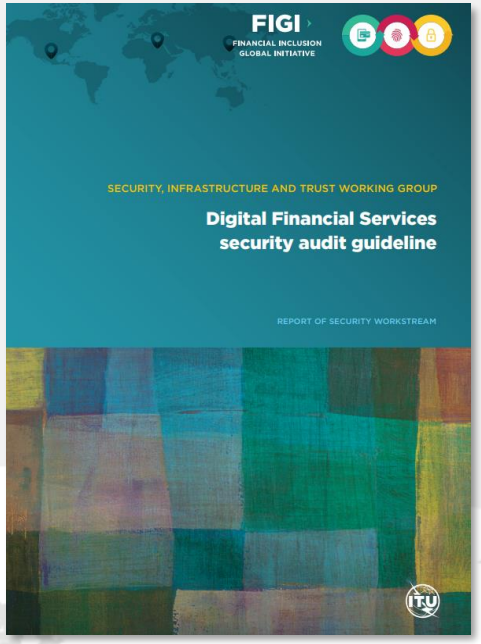
The DFS security lab provides a common methodology to conduct security audit for DFS applications and check for systemic vulnerabilities.

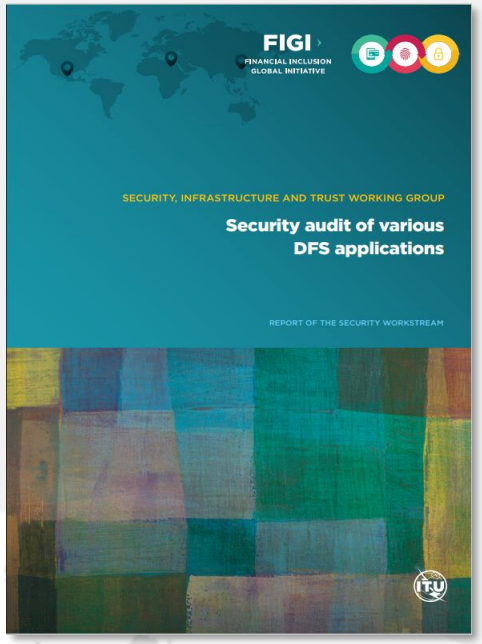
DFS Security Lab Objectives

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.









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 **FIDO**

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

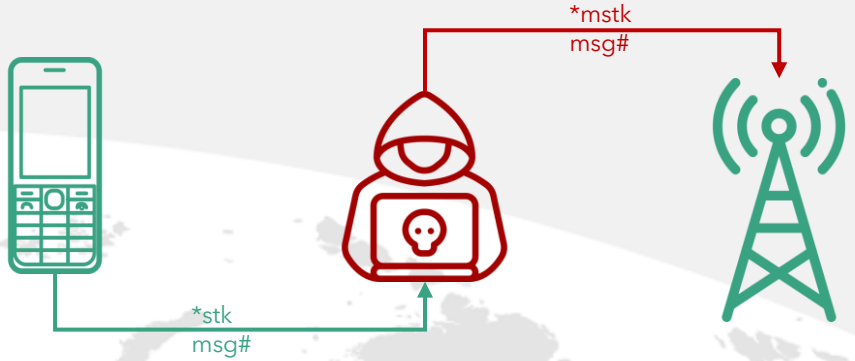
USSD & STK Security Tests

Covered on 17 June 2021 Session on Enhancing Security of DFS Applications in Emerging Economies

a. **SIM Swap** and **SIM clone** testing

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

c. Testing **remote USSD** execution attacks



d. Simulate **man-in-the-middle attacks**

FIDO Developer Resources

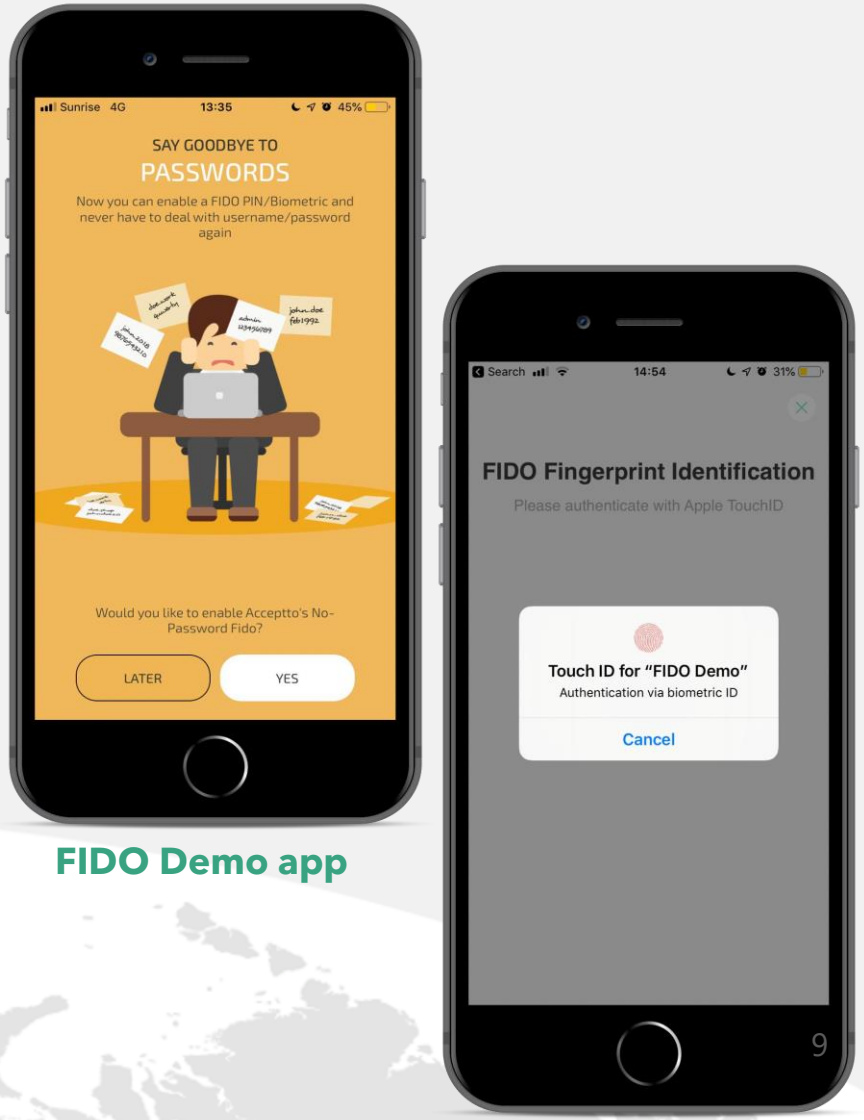
FIDO (Fast ID Online) is a set of technology-agnostic security specifications for strong authentication.

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.

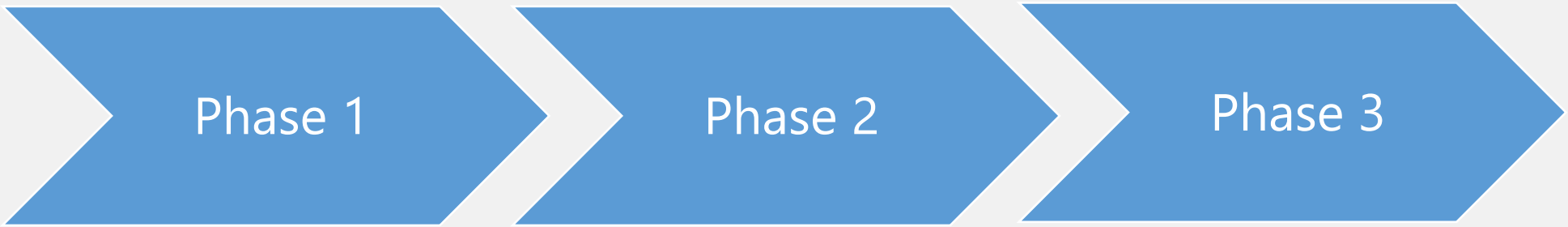


FIDO Demo app

Android Attack Vector

Attack Vector is a method that a hacker uses to gain access to another computing device or network in order to inject a “bad code” often called **payload**.

This helps hackers to exploit system vulnerabilities. Many of these attack vectors take advantage of the human element as it is the weakest point of this system.



- **Infect the device**

- **Install Backdoor**

- **Bypass containerization**
- **Exfiltrate information**

Android Attack Points

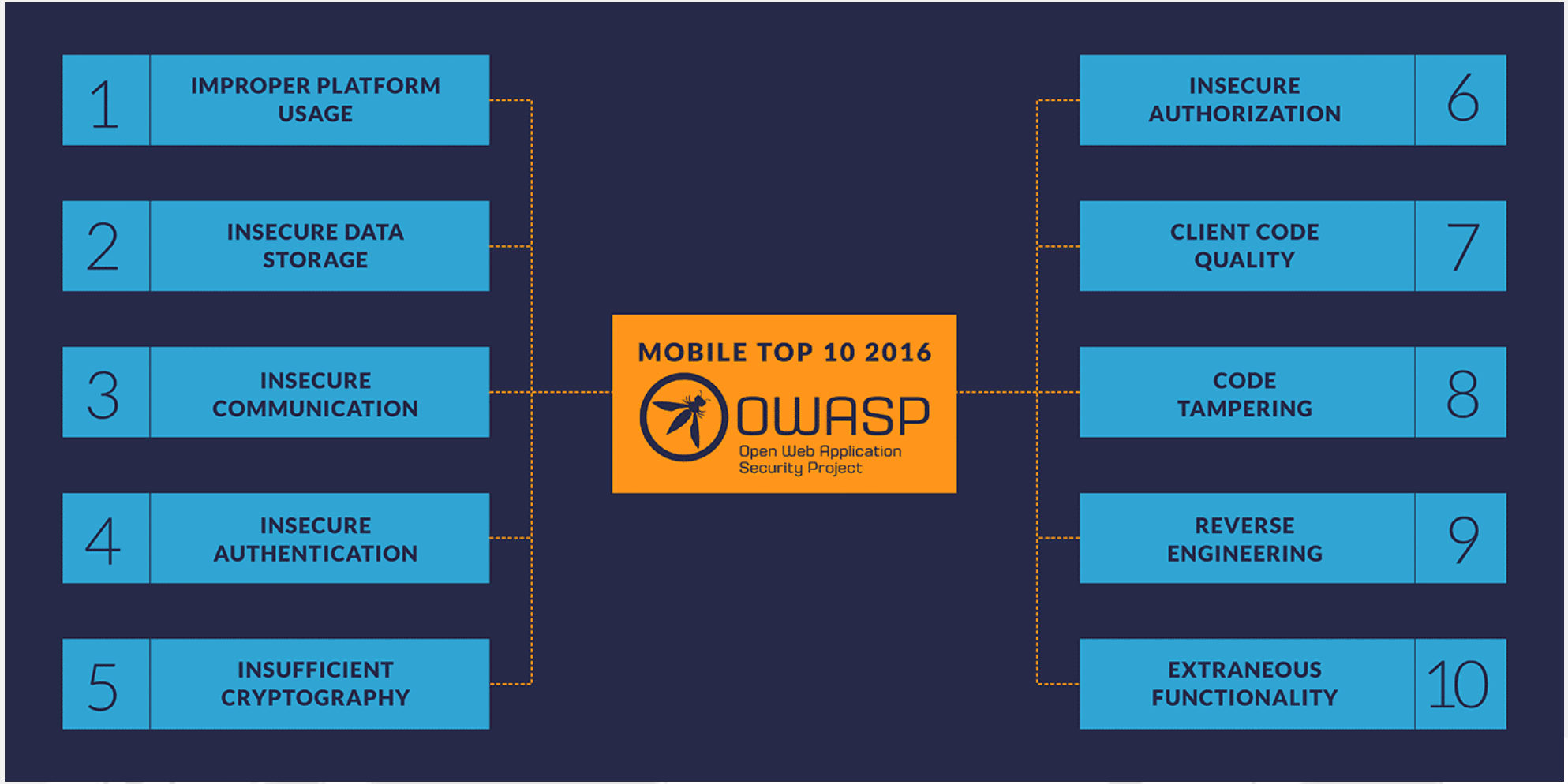
- Data Storage
  - Keystores
  - Application Filesystem
  - Application Database
  - Configuration files

- 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.

DFS security tests (based on the OWASP Mobile Top 10 Risks)



Source: OWASP

Android DFS security tests (based on the OWASP Mobile Top 10 Risks)

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

Areas of collaboration with DFS Regulators and Providers

1. DFS security assurance framework and audit guideline – implementation deep dive;
2. DFS application security audit and vulnerability assessment.
3. Collaboration on cyber preparedness
4. DFS Security awareness sessions/clinics/webinars on:
    a. Application security threats and vulnerabilities to USSD, STK, Android and QR code based DFS apps.
    b. DFS telecom infrastructure vulnerabilities (SS7 vulnerabilities and mitigation measures).
    c. Secure authentication technologies for DFS application

DFS Security Lab

Get in touch

dfssecuritylab@itu.int

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