

Uganda Communications Commission

Digital Financial Services Security

Testing Laboratory



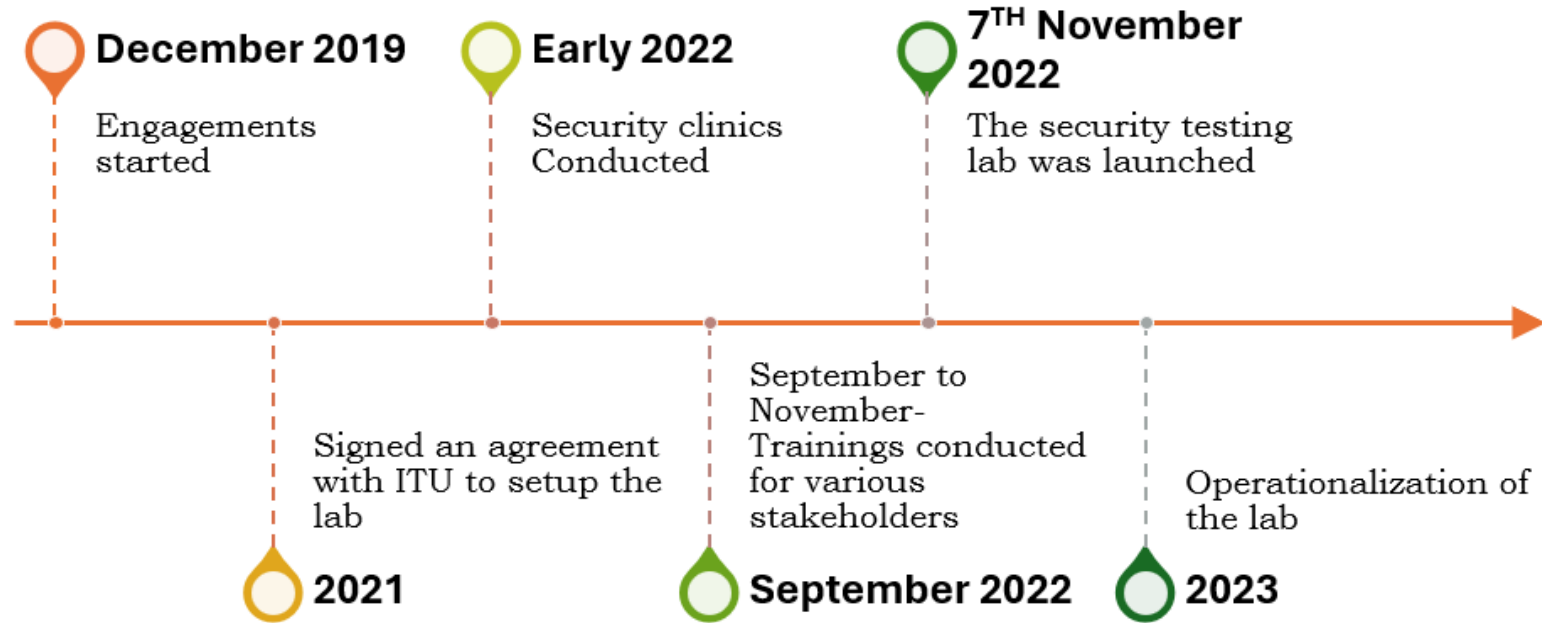
UGANDA
COMMUNICATIONS
COMMISSION

Agenda

- Uganda's lab establishment journey
- Engagement model
- Type of tests done
- Common vulnerabilities & remediation approach
- Road ahead
- Q & A



DFS Laboratory journey



Engagement model

Uganda's scenario:

- ❖ Bank of Uganda, the country's central bank, is mandated with licensing and regulating payment services and operators.
- ❖ Uganda Communication Commission is mandated with licensing and regulating communication services.

How do the regulators work?

Short answer, co-regulate via an agreed on and approved memorandum of understanding that:

- ❖ Stipulates the scope of co-operation
- ❖ Defines roles and responsibilities
- ❖ Information sharing
- ❖ Defines the format of information requests
- ❖ Confidentiality and use of information
- ❖ Establishes technical working groups to spear head this corporation



Types of tests done

- ❖ USSD and STK security testing:-
 - Testing susceptibility to binary over the air attacks
 - Man in the middle attacks
 - Testing remote USSD execution attacks
 - SIM cloning.

- ❖ Android & iOS security testing:-
 - Improper credential usage
 - Insecure authentication/authorization
 - Insufficient input/output validation
 - Insecure communication
 - E.t.c.....



Common vulnerabilities

❖ USSD & STK vulnerabilities:

- Man in the middle attack on STK application providing geo-location data:

```
1:48:27.300669613 127.0.0.1 127.0.0.1 GSM SIM 88 ISO/IEC 7816-4 unless stated otherwise TERMINAL RES
Linux cooked capture
Internet Protocol Version 4, Src: 127.0.0.1, Dst: 127.0.0.1
User Datagram Protocol, Src Port: 45105, Dst Port: 4729
GSM SIM 11.11
  1010 .... = Class Coding: ISO/IEC 7816-4 unless stated otherwise (0xa)
  .... 00.. = Secure Messaging Indication: No SM used between terminal and card (0x0)
  .... ..00 = Logical Channel number: 0
  Instruction: TERMINAL RESPONSE (0x14)
  Card Application Toolkit ETSI TS 102.223
    Command details: 012600
      Command Number: 0x01
      Command Type: PROVIDE LOCAL INFORMATION (0x26)
      Command Qualifier: Location Information (MCC, MNC, LAC/TAC, Cell Identity and Extended Cell Identity) (0x00)
    Device identity: 8281
      Source Device ID: Terminal (Card Reader) (0x82)
      Destination Device ID: SIM / USIM / UICC (0x81)
    Result: 00
      Result: Command performed successfully (0x00)
  Location Information: 46f11103ee3014
    Mobile Country Code (MCC): Uganda (641)
    Mobile Network Code (MNC): [REDACTED] ( )
    Location Area Code / Tracking Area Code: 0x03ee
    Cell ID: 0x3014
Status Word: 9141 Normal ending of command with info from proactive SIM
```



Common vulnerabilities

❖ Android & iOS application vulnerabilities:

- Improper credential usage:

```
blueline:/ # cat /data/data/[REDACTED]/shared_prefs/FlutterSharedPreferences.xml | grep pin  
<string name="flutter.pinCode">9[REDACTED]</string>
```

- Insecure authentication & authorization:

<pre>POST [REDACTED] HTTP/1.1 user-agent: Dart/3.4 (dart:io) accept: */* Accept-Encoding: gzip, deflate, br Content-Length: 41 host: [REDACTED] auth: [REDACTED] content-type: application/x-www-form-urlencoded; charset=utf-8 bearer: [REDACTED] signature: [REDACTED] Connection: keep-alive accountNumber=256[REDACTED]&page=0&perPage=9</pre>	<pre>1 HTTP/1.1 200 OK 2 Server: [REDACTED] 3 Date: Thu, 17 Apr 2025 12:34:44 GMT 4 Content-Type: application/json; charset=utf-8 5 Content-Length: 182 6 Connection: keep-alive 7 X-Powered-By: [REDACTED] 8 request-id: 9 [REDACTED] 10 Vary: Origin, Accept-Encoding 11 Access-Control-Allow-Credentials: true 12 ETag: [REDACTED] 13 { "success":true, "statusCode":200, "message":"[REDACTED] transactions retrieved successfully", "data": [], "meta":{ "total":0, "lastPage":0,</pre>
---	---



Common vulnerabilities & remediation approach

❖ Android & iOS application vulnerabilities:

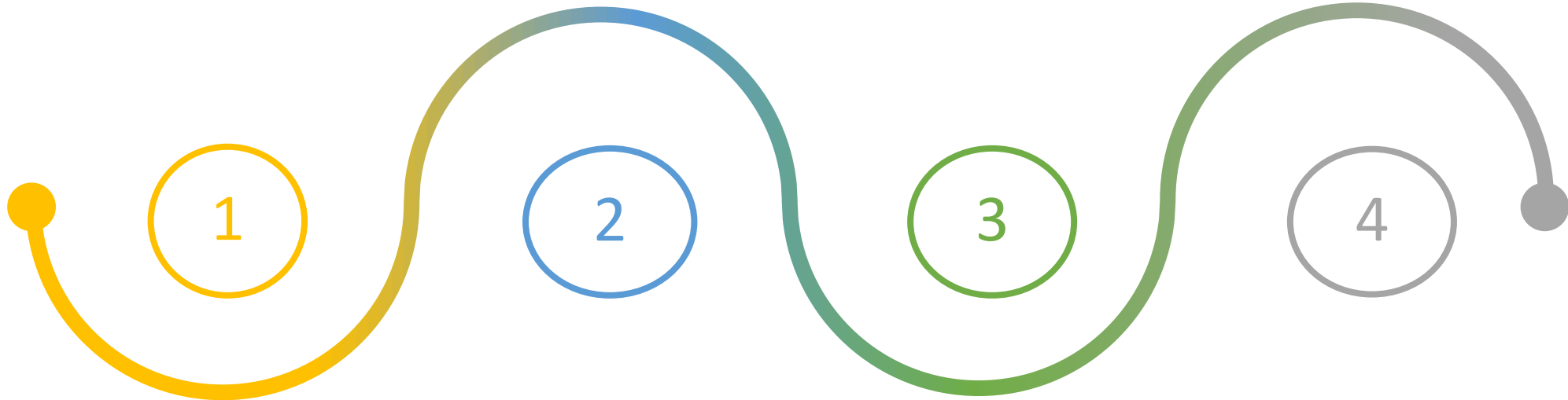
- Insufficient binary protections: E.g No code obfuscation



❖ Remediation approach: 2-step process

- Walk-through with the technical team on the proposed remediations
- Under-take a re-test of the application

Road ahead



DEVELOPMENT OF DFS CYBERSECURITY GUIDELINES

Guidelines to define minimum cybersecurity requirements for the DFS ecosystem. E.g
Minimum cybersec guidelines,
Mobile AppDev guidelines

LAB RESOURCING

Enhance laboratory hardware, software and staffing resourcing

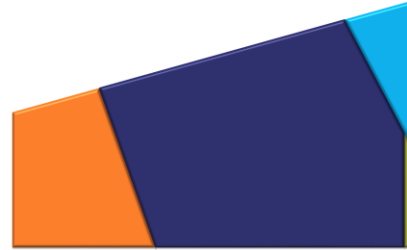
EXPAND SECURITY TESTING SCOPE

Security testing to include MNO, DFS providers and bank applications and infrastructure. E.g
3G/4G/5G test bed

ENHANCE SECTOR COLLABORATION

Partner with other regulators, DFS providers, experts and academia. E.g
AFC working group

Thank you!



UGANDA
COMMUNITY
COMMISSION

