Uganda Communications Commission

Digital Financial Services Security

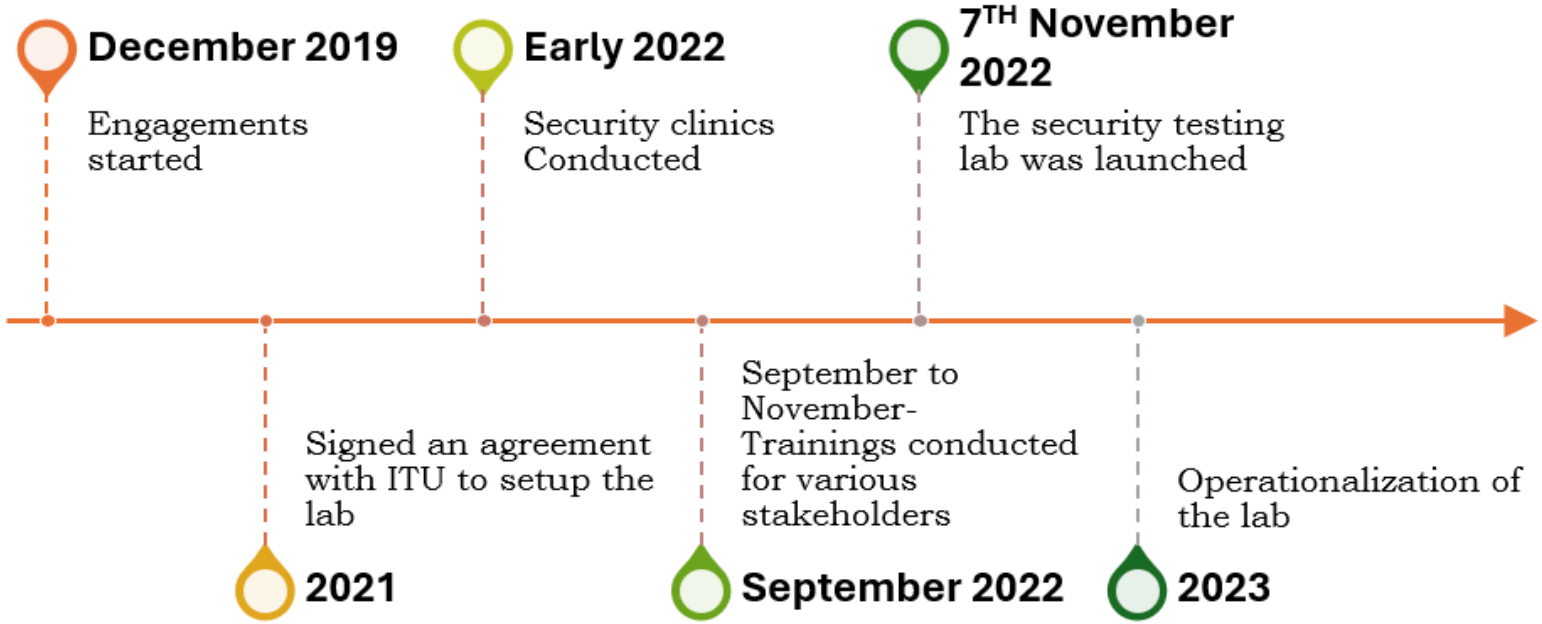
Testing Laboratory

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

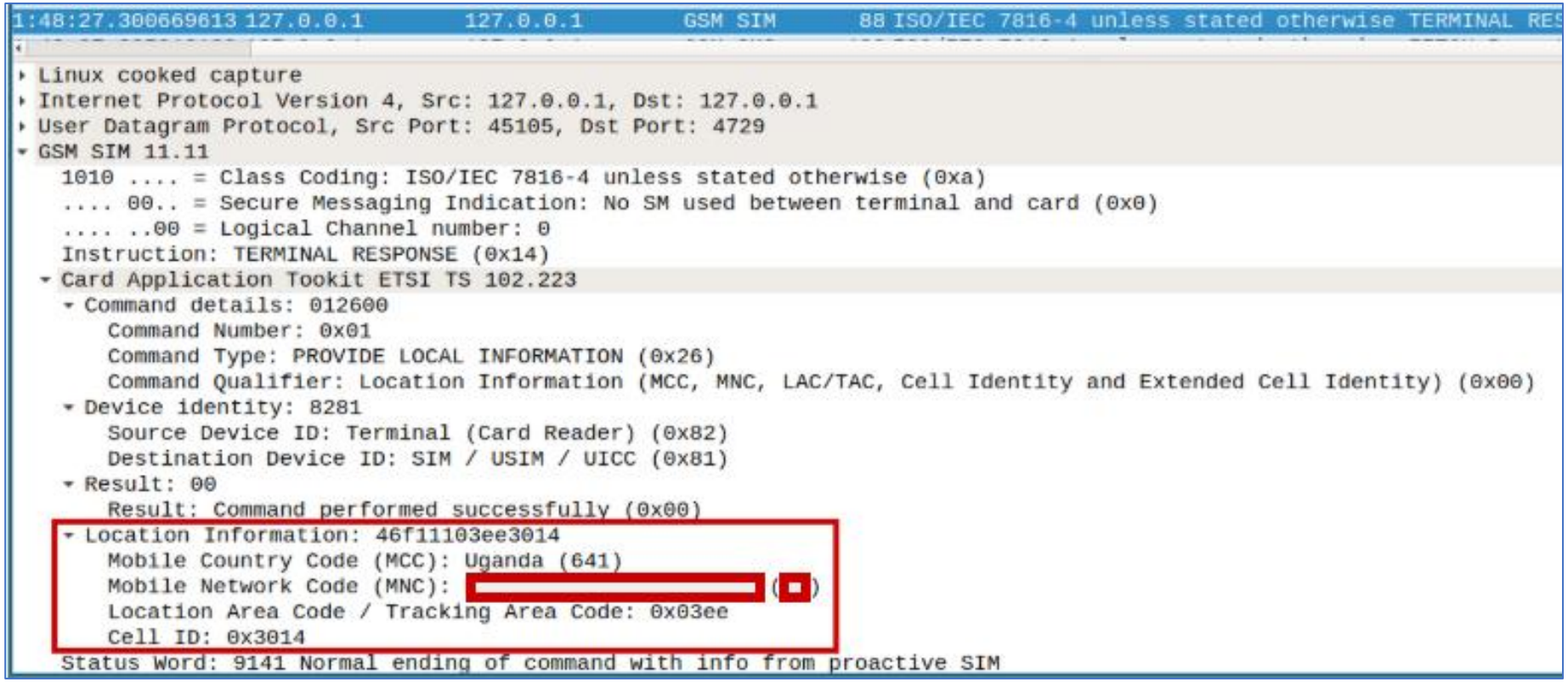
Types of tests done

- 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:



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:

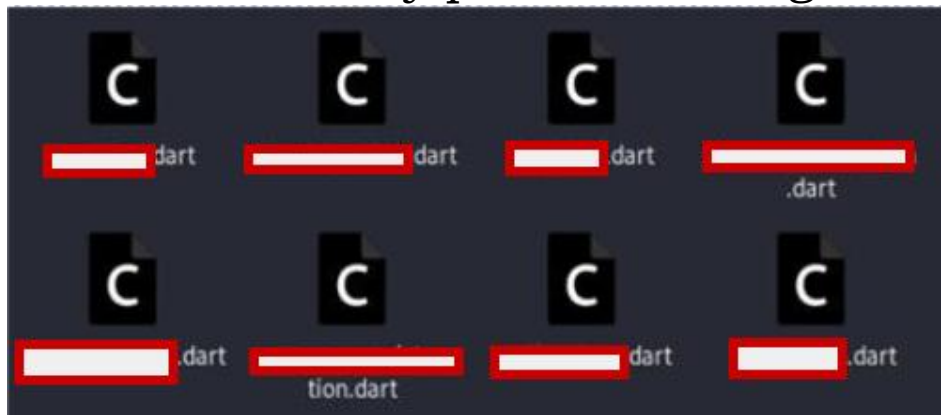
```
POST [redacted] HTTP/1.1
user-agent: Dart/3.4 (dart:io)
accept: */*
Accept-Encoding: gzip, deflate, br
Content-Length: 41
host: [redacted]
auth: [redacted]
content-type: application/x-www-form-urlencoded;
charset=utf-8
bearer: [redacted]
signature: [redacted]
Connection: keep-alive

accountNumber=2564[redacted]&page=0&perPage=9
```

```
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: [redacted]
9  Vary: Origin, Accept-Encoding
10 Access-Control-Allow-Credentials: true
11 ETag: [redacted]
12
13 {
       "success":true,
       "statusCode":200,
       "message":"[redacted] transactions retrieved successfully",
       "data":[
       ],
       "meta":{
           "total":0,
           "lastPage":0,
```

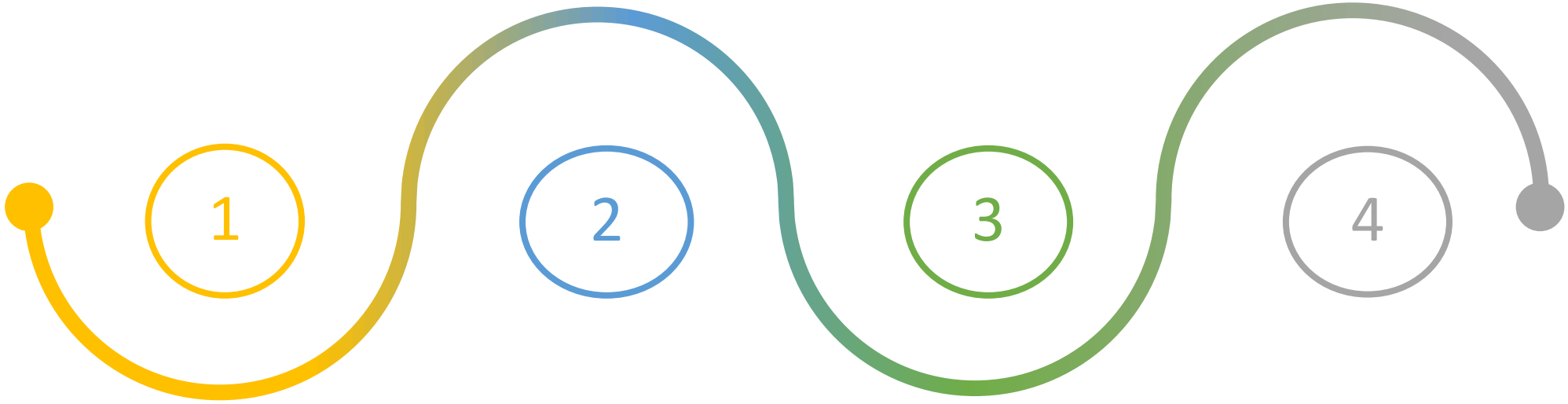
Common vulnerabilities & remediation approach

- 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

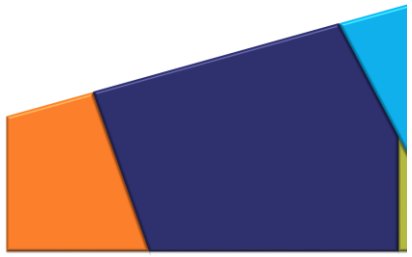
Enhance laboratory hardware, software and staffing resourcing

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!