Digital Financial Services Security Clinic

Addressing security risks to digital finance ecosystem

Recommendations to mitigate SS7 and SIM swaps

Arnold Kibuuka
Project Officer, ITU

Recommendations

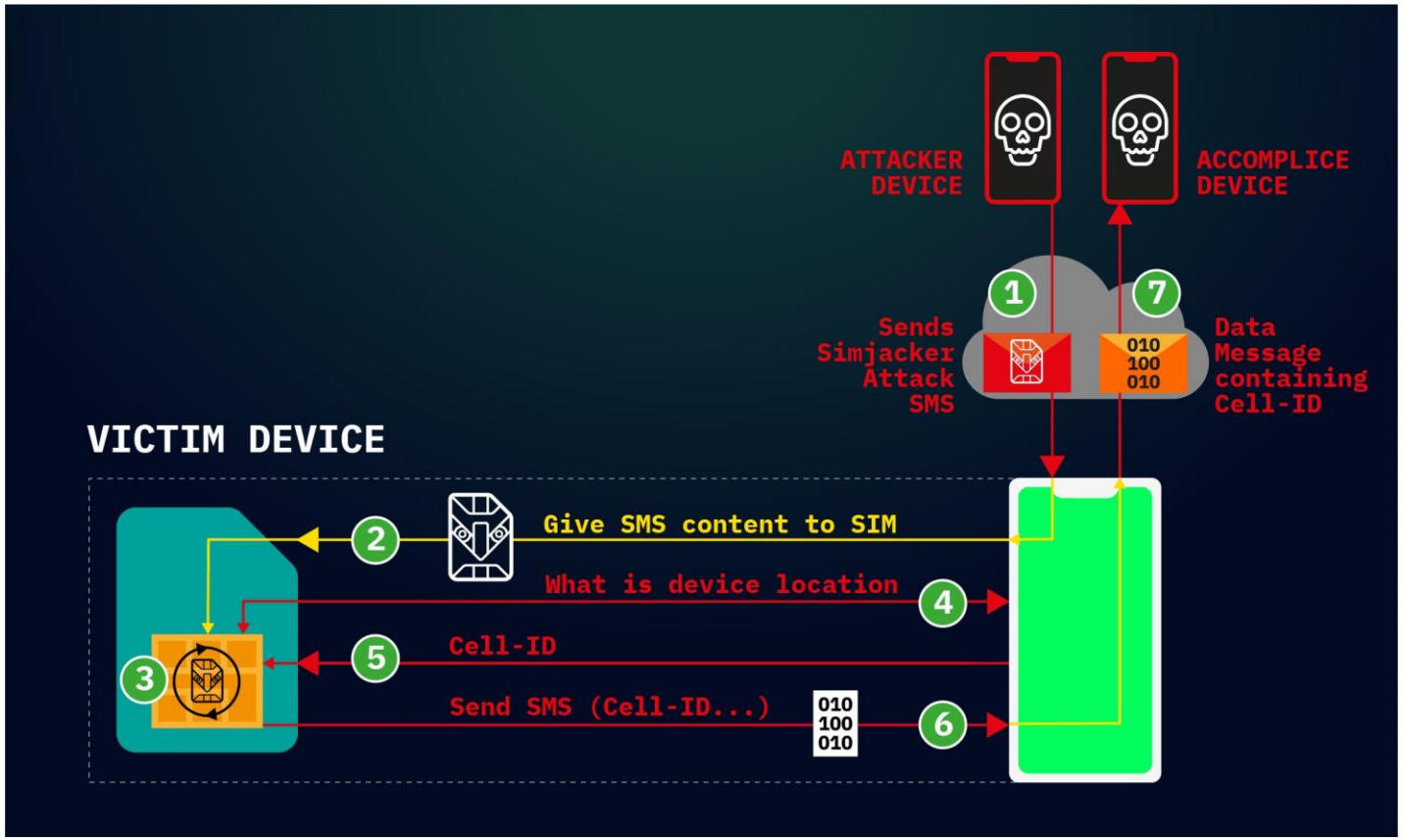
1. Security recommendations to protect against DFS SIM related risks like SIM swap fraud and SIM recycling
2. Recommendations to mitigate SS7 vulnerabilities
3. Template for a Model MOU between a Telecommunications Regulator and Central Bank related to DFS Security
4. Mobile Application Security Best practices

Regulatory Guidance to mitigate SIM risks

Related report:
Security testing for USSD and STK based DFS applications

SIM risks

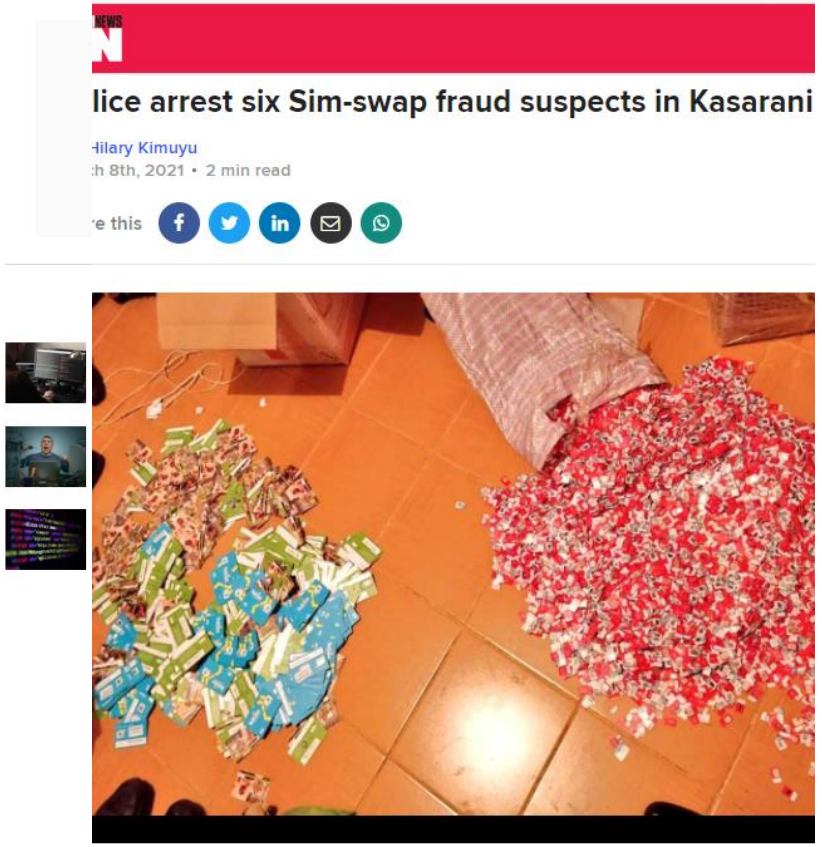
1. SIM Cloning
2. SIM Swaps
3. SIM Recycling
4. Binary over the air attacks (Sim jacker and WIB browser attacks)



Source: adaptive mobile

Examples of DFS attacks

Source: znet



Source: Nairobi News

- March 2021, Times Of India, **2 duped of Rs 82k in SIM swap fraud**
- March 2021, Nairobi News: **Police arrest six Sim-swap fraud suspects in Kasarani**
- The Daily Monitor: **Thieves use 2,000 SIM cards to rob banks**
- Ghana Chamber of Telecommunications: **Mobile Money Fraudsters Now Target Bank Accounts Linked To MoMo Accounts**
- February 2021, CNN: **Police arrest eight after celebrities hit by SIM-swapping attacks**

Regulatory Guidance to mitigate SIM risks

a. Regulatory coordination between telco and DFS regulator on SIM vulnerabilities.

   - e.g. An MOU between the DFS regulator and Telco regulator

b. Standardization by regulators of SIM swap rules amongst MNOs/MVNOs

   - including SIM swaps leading to porting of numbers to other MNOs/MVNOs

c. Recommending security measures for MNOs on SIM risks.

Regulatory Guidance to mitigate SIM risks

a. **An MOU between the DFS and MNO that includes:**

   i. Areas of cooperation and cooperation strategies general provisions

   ii. National Telecommunications Regulator - Designated roles

      - Continuous controls monitoring of DFS entities

   iii. Central Bank-designated roles

MNO controls on SIM swaps

a. Where SIM replacement is carried out by proxy, the MNO/MVNO or its agents must capture a biometric, facial image of the proxy which must be kept for a specified period.

b. MNOs should notify DFS providers on swapped SIMs, ported and recycled numbers.

c. Biometric SIM swap verification

d. Multifactor user validation before SIM swap

e. Information sharing with DFS provider on SIM swaps and SIM recycling:

f. SIM swap notifications to users

g. Secure SIM data protection

h. Holding time before activation of a swapped SIM

i. Customer support representatives training

DFS operators controls to mitigate SIM swaps

- Real time IMSI/ICCID detection
- Real time device change detection
- Encourage use of secure DFS access

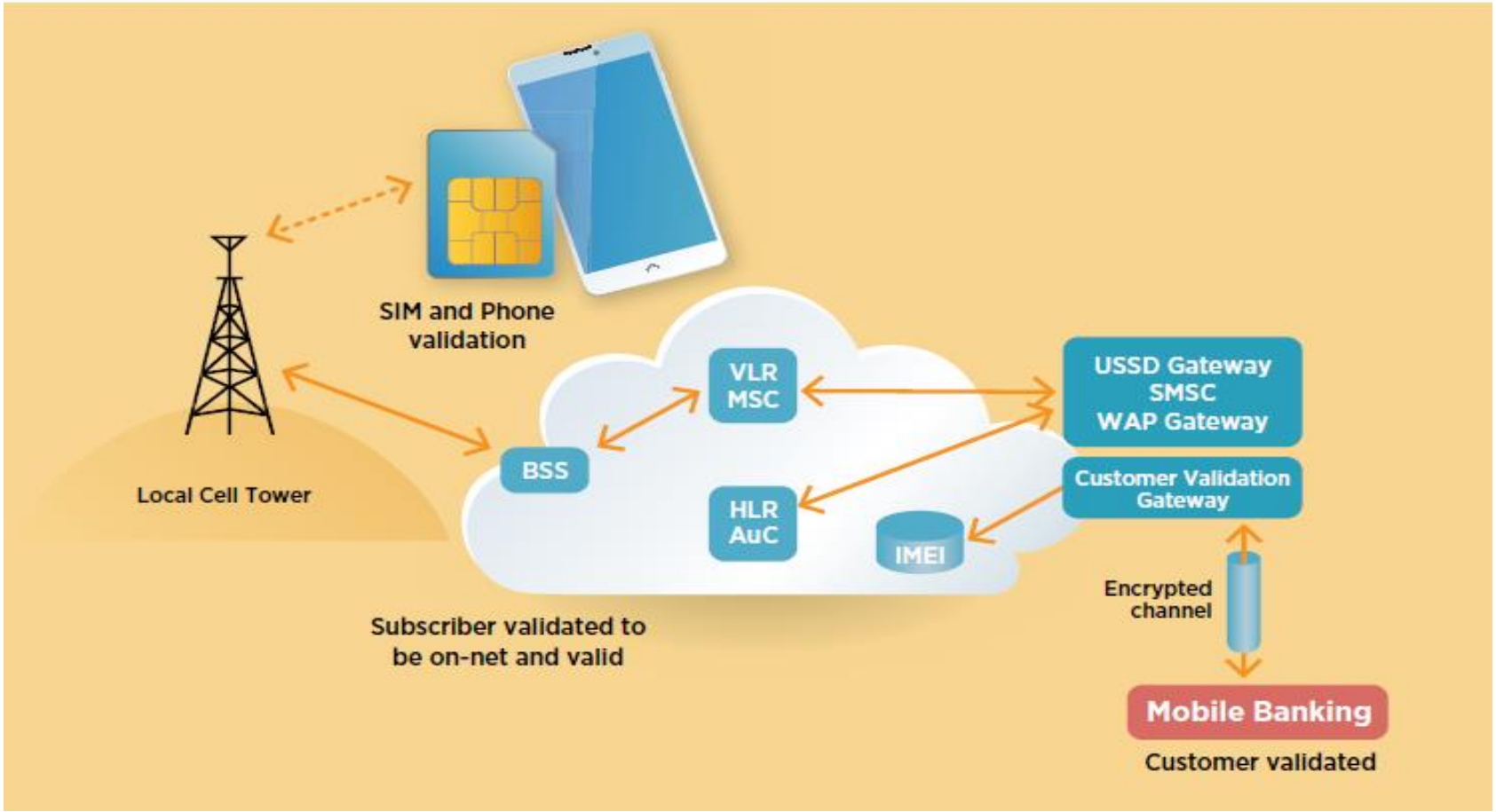
Guidance to mitigate SS7 threats

Related report:
Security testing for USSD and STK based DFS applications

Regulatory Guidance to mitigate SS7 risks

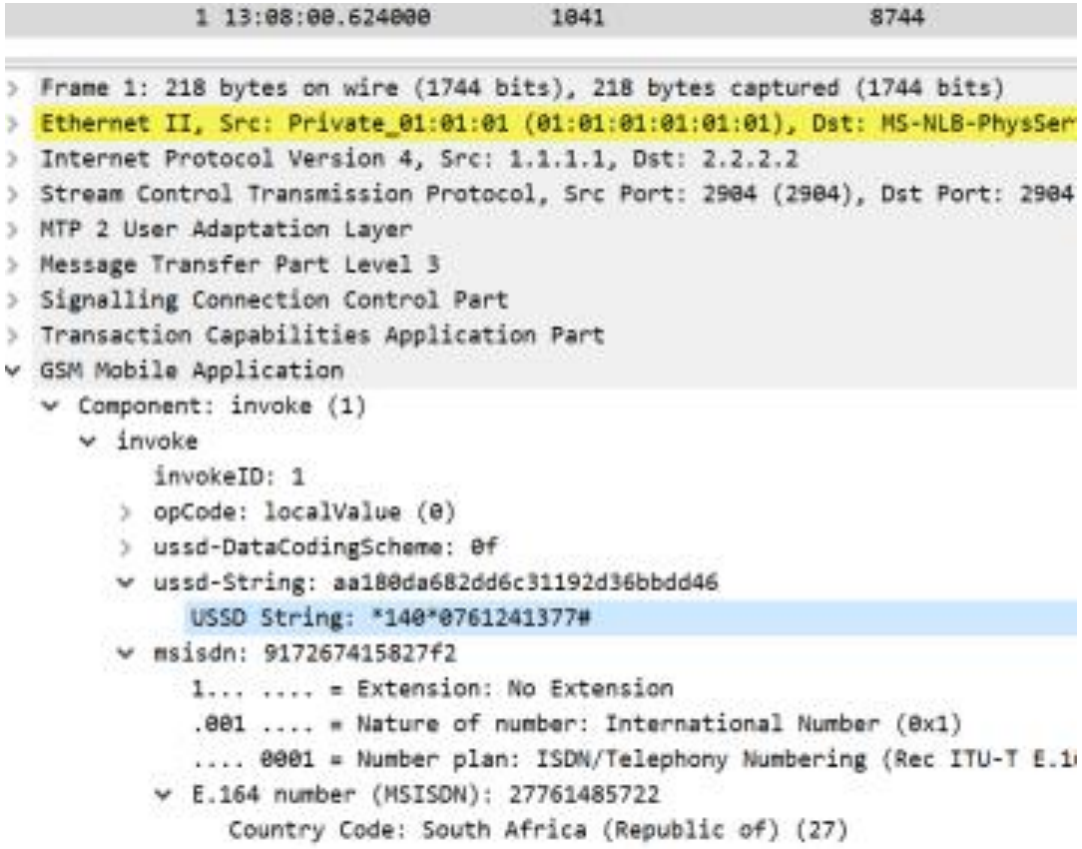
- Regulatory coordination between telco and DFS regulator on SS7 vulnerabilities.
- Incentivize the industry
- Education for telecom and financial services regulators on SS7 vulnerabilities and impact to DFS
- Telecom regulators to establish baseline security measures for each SS7 risk category
- IMSI validation gateway

IMSI validation gateway



Recommendations for MNO to mitigate SS7 risks

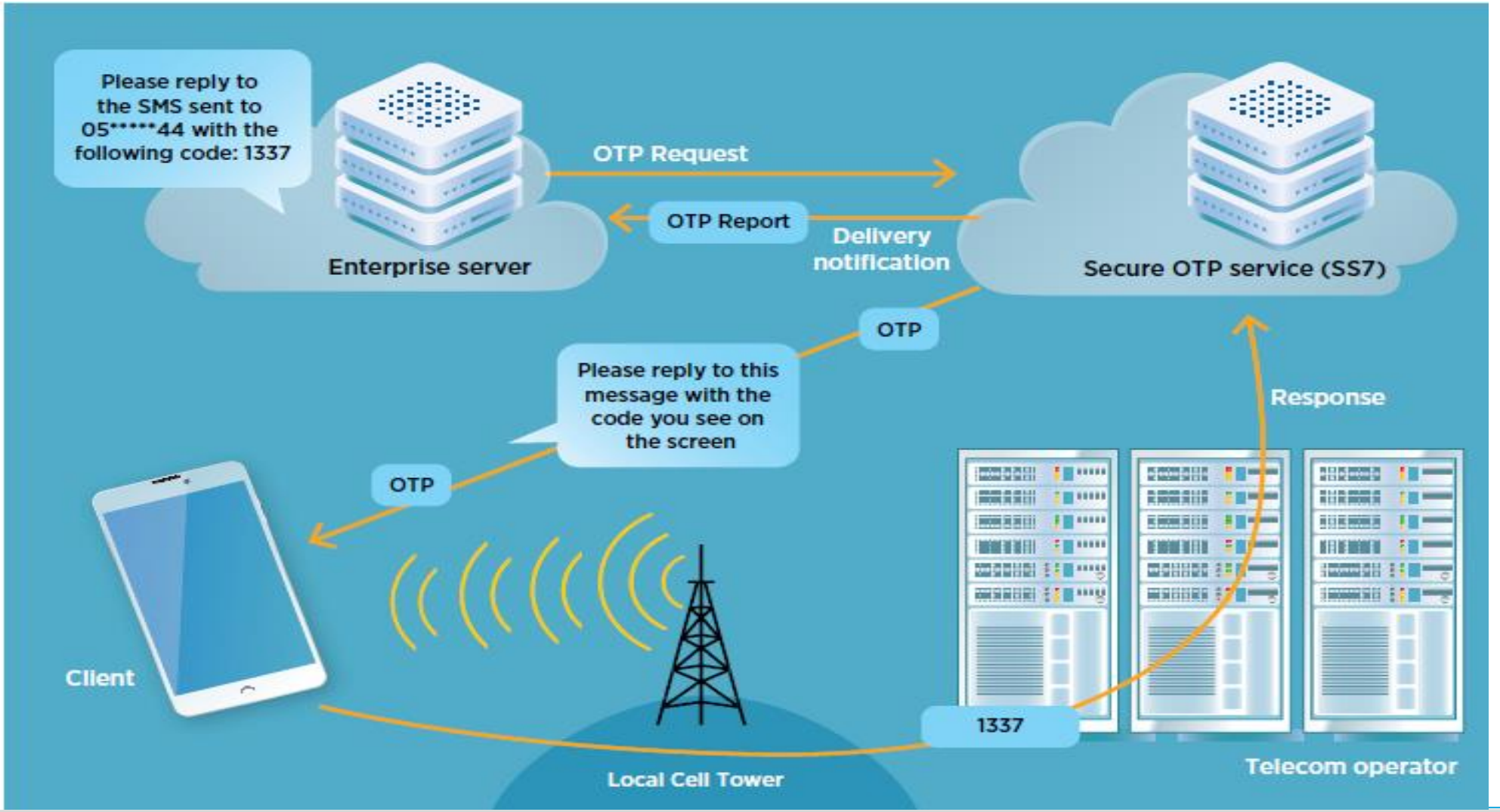
- Secure GSM ciphers for radio network traffic
- Session time out
- USSD PIN masking
- Secure and monitor core network traffic
- Limit access to traces and logs
- SMS filtering
- SMS home routing



DFS operator controls to mitigate SS7 risks

- Session time out
- Transaction limits for insecure channels
- User education
- Detecting and mitigating social engineering attacks with MT-USSD and interception of USSD
- Bidirectional OTP SMS flow

Bidirectional OTP SMS flow



Questions

Contact: dfssecuritylab@itu.int

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