Digital Financial Services Security Webinar

Episode #4:Securing the USSD and STK Infrastructure for Mobile Payments

Mwesigwa Vincent
Manager- Information Security, UCC
28th May 2025

Agenda

- Context & Adoption
- Why security matters
- Threat Landscape
- DFS ecosystem
- Common Vulnerabilities
- Best Practices for Operators & DFS Providers
- Summary & Key Takeaways

USSD & STK

Over 90% of transactions in Africa depend on USSD and STK

Services such as account opening, money transfer, bill payments

Popular due to accessibility, real-time response, low cost, no data connection needed

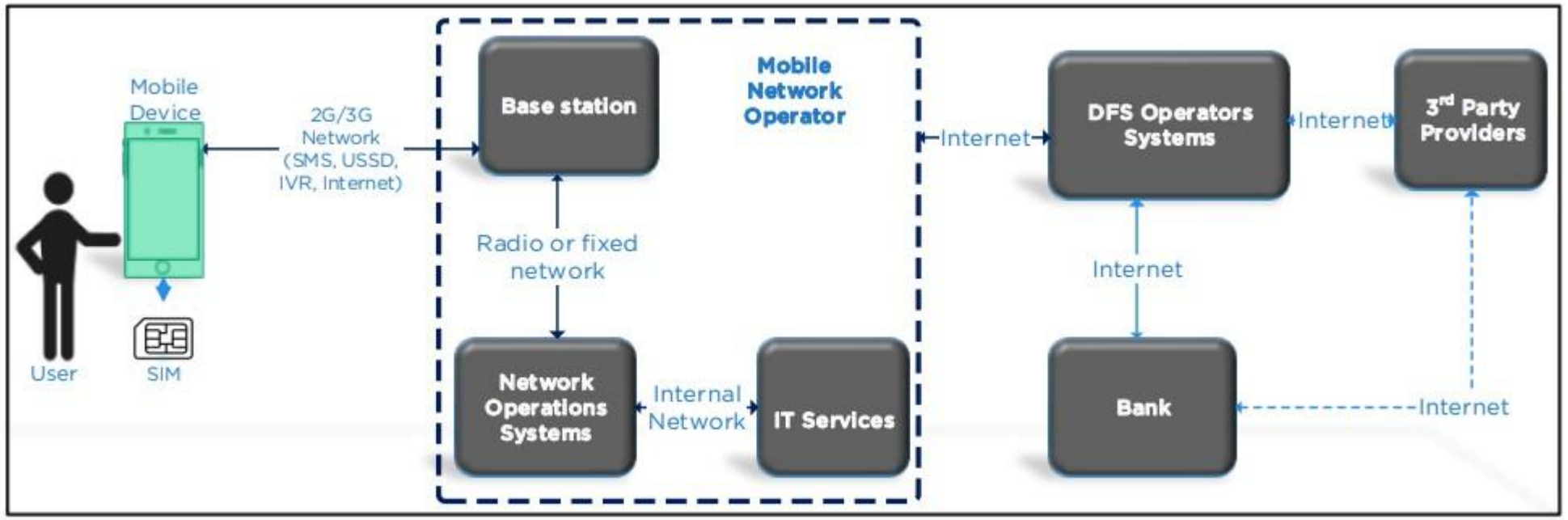
Why Security Matters

- Multiple touchpoints create opportunities for cyber attacks
- Risks like service disruption, fund diversion, data breaches
- Trust in mobile money relies on secure infrastructure

Threat Landscape

- Social engineering and phishing via USSD
- Unauthorized access to the mobile device/theft.
- SIM swap and recycling attacks
- Rogue base stations (IMSI catchers)
- SS7 protocol abuse and remote SIM toolkit misuse

DFS ecosystem



User

target user for DFS, uses mobile money application on a mobile device to access the DFS ecosystem

MNO

provides communication infrastructure from wireless link through the provider network

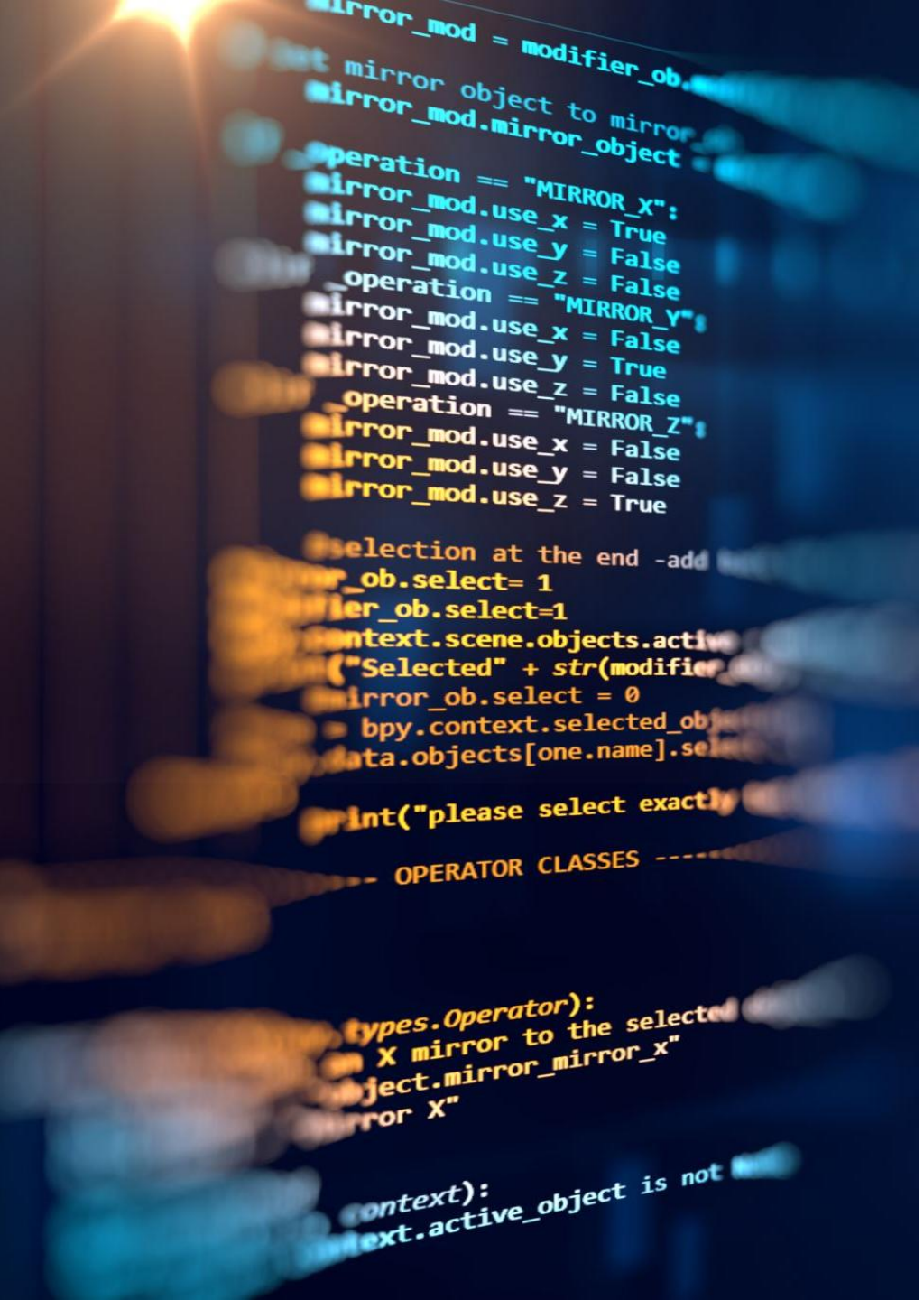
DFS Provider

application component, interfaces with payment systems and third-party providers.

Common Vulnerabilities

- Weak session validation and timeouts
- Unencrypted channels between core systems
- SIM vulnerabilities (e.g., SIMjacker, OTA attacks)

Security practices for DFS applications based on USSD and STK



Mitigation against retrieval of user data

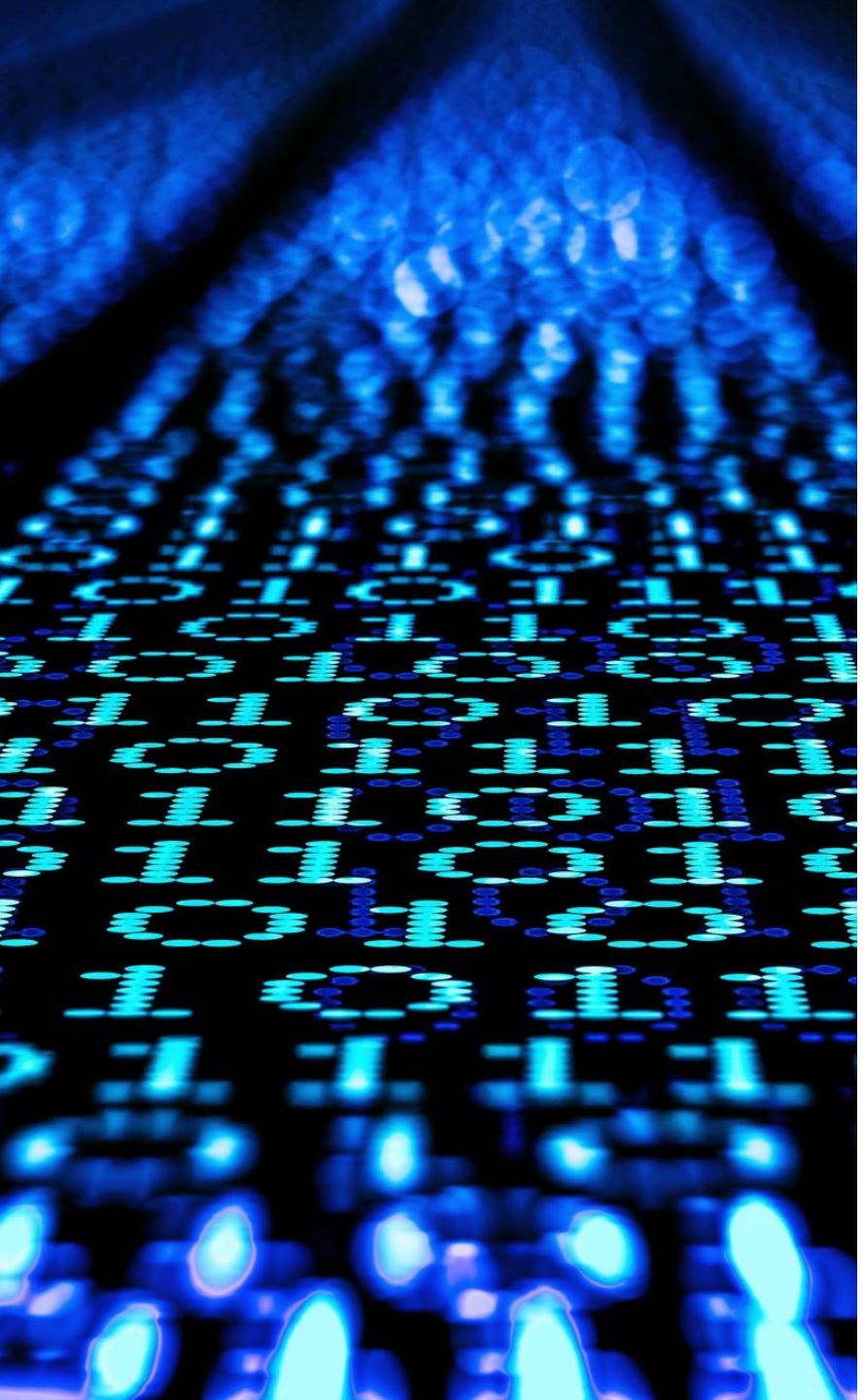
- Enable Encryption between users' devices and base stations
- Use session timeout on the client-side to limit altered requests/responses.
- Deploy USSD PIN masking whenever possible
- Ensure there is an auditable process
- Enable option to opt-out of the USSD or STK channels
- Set transaction limits for customer withdrawals and transfers over the USSD

SIM swap and SIM recycling risks mitigation measures

- Device authentication using the IMEI’s
- The user identity verification (pin, finger face etc.
- Real time detection of sim swap and replacement
- IMSI validation gateway
- Securely store SIM data like IMSI

Remote USSD execution mitigation measures

- Disable the ADB interface, and device vendors should not ship products with Android Debug Bridge enabled over a network
- DFS users should be educated on the dangers of connecting to public Wi-Fi and granting permissions to an app on a device
- Avoid using rooted devices for DFS transactions



SIM exploitation using binary OTA mitigation measures

- Monitoring and SMS filtering, SMS should only be allowed from whitelisted sources
- OTA messages with STK coding restricted to only from MNO platform and not from or to other subscribers
- A2P SMS traffic from content providers must be free of any STK commands
- SMS home routing

Summary & Key Takeaways

1

USSD/STK are essential yet vulnerable channels

2

ITU-T X.1456 provides a robust defense model

3

Secure implementation is achievable with proper tools and collaboration

4

Start with practical steps today to strengthen user trust and security

Q&A

Thank you!