Improving Resilience in the DFS Ecosystem with a Security Assurance Framework

Kevin Butler, University of Florida

Insights on Digital Financial Services during COVID-19 Webinar Series

27 July 2020

COVID-19 and Resilience

- COVID-19 has created an unprecedented strain on the world economy
  - Exacerbates existing inequalities
- Mobile devices play a unique role in maintaining connectivity and providing valuable services to users
- The digital financial services (DFS) ecosystem is uniquely vulnerable to a variety of threats
  - Interconnectedness of system entities
  - Reliance on numerous parties
  - Mobile ecosystem itself is increasingly complex – devices, OSes

Why a Security Framework?

- Resilience vs security:
  - Resilience = ability to withstand and recover from operational hardship
  - Business continuity planning, secure redundancy, identify attack surfaces, restore operations
  - Security = protection of computer systems and data against malicious adversaries
- A security policy that only considers protection will not in itself provide resilience
- But a *framework* that assess risk and provides a means for identifying and developing processes to assure secure operation will also provide resilience

Security Framework Goals

- The Security Assurance Framework developed under the Financial Inclusion Global Initiative (FIGI) Security, Infrastructure, and Trust WG
- Aims to bridge the knowledge gap and recommends a structured methodology for risk management
- How can the framework be used?
  - Enhance customer trust and confidence in DFS
  - Clarify roles and responsibilities for each stakeholder in the ecosystem
  - Identify security threats and vulnerabilities within the ecosystem
  - Establish security controls to provide end-to-end security
  - Strengthen management practices with respect to security risk management in a manner that is inclusive to all shareholders

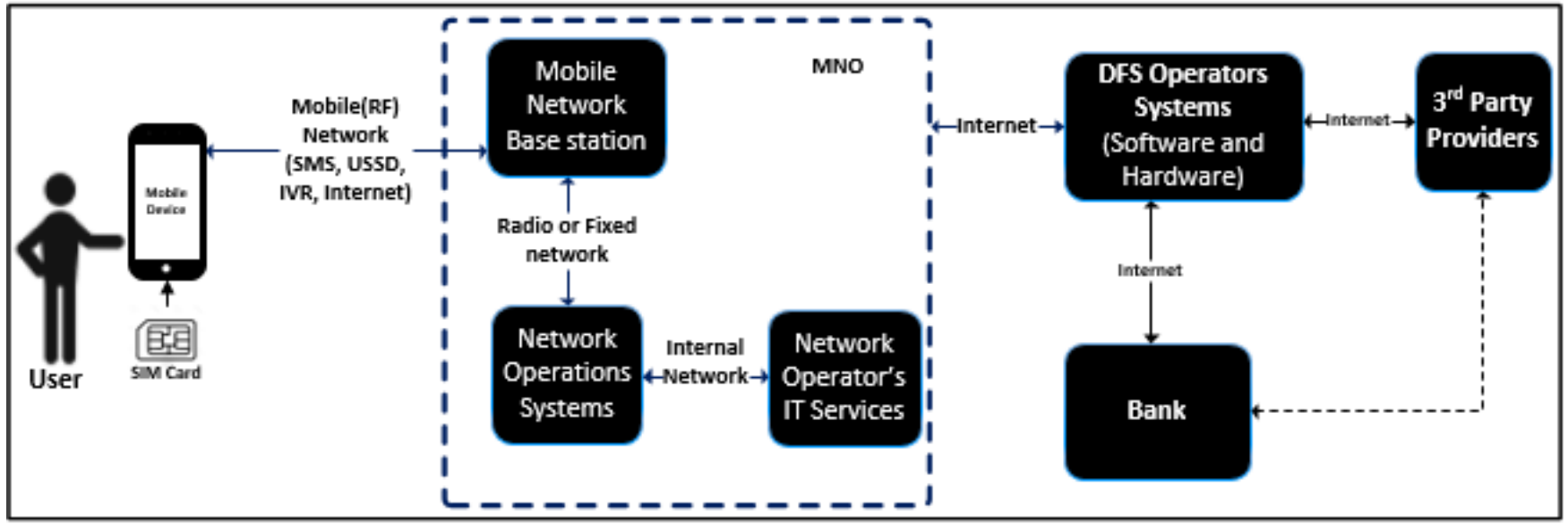
DFS Security Assurance Framework: https://www.itu.int/en/ITU-T/extcoop/figisymposium/Pages/FIGISITWG.aspx

Concepts

- **Vulnerability:** a weakness in a system that can be exploited by an adversary
- **Threat:** the specific means by which a vulnerability is exploited
- **Risk:** the consequences of a threat being successfully deployed

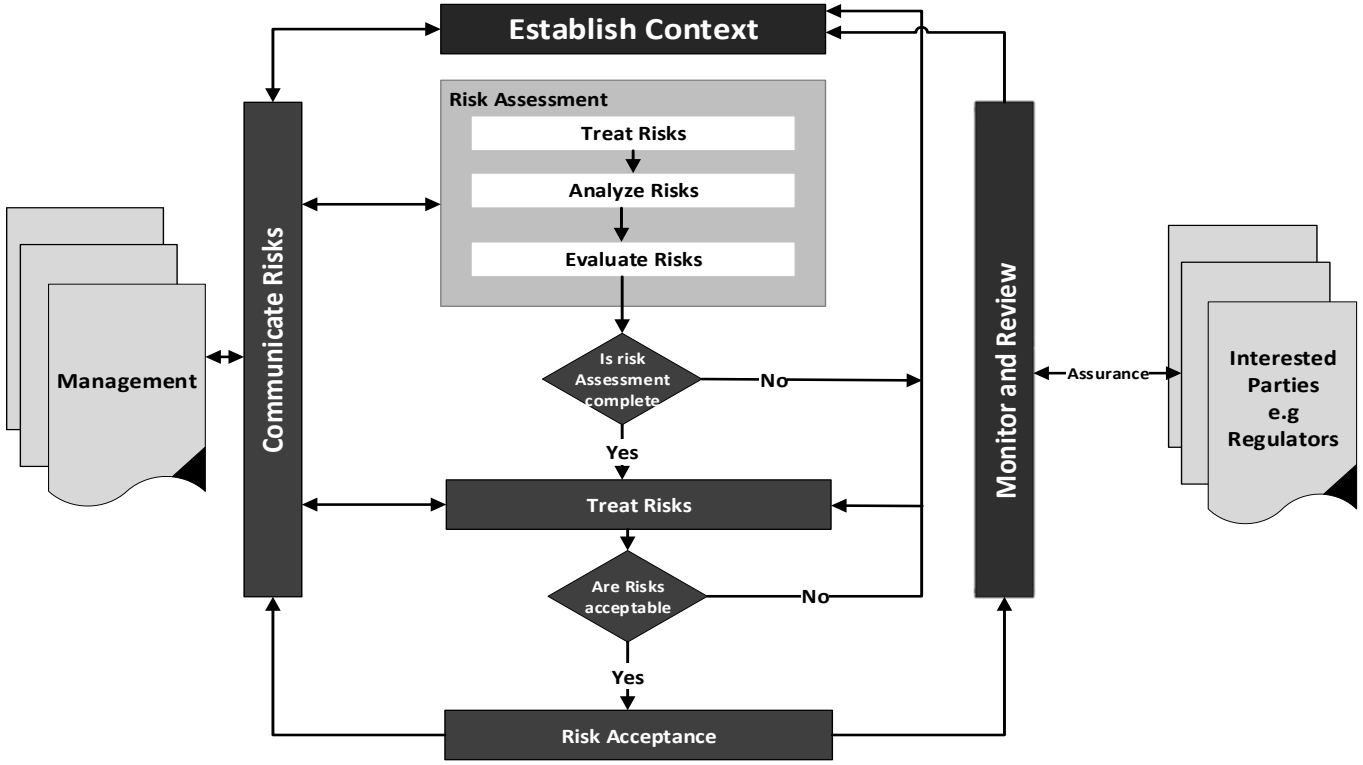
- ITU-T Recommendation X.805 provides a foundation for the document, with eight *security dimensions* to address security:
  - Access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability, privacy

Elements of DFS Ecosystem



- **User** is target audience 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** handles application component, interfaces with payment systems and third-party providers

Risk Assessment Methodology



- Based on Deming cycle of Plan, Do, Check, Act (PDCA) phases
- Monitoring and review depend on the stakeholder
  - E.g., regulator reviewing controls, audits by providers
- Context necessary for effective risk assessment/evaluation/analysis

Summary: DFS Ecosystem Threats

User

- Social engineering (8.8)
- Unauthorized access to mobile device (8.16)
- Unintended Disclosure of personal information (8.17)

Mobile Device and simcard

- Code exploitation attack (8.4)
- Malware (8.13)
- Unauthorized access to mobile device/ SIM (8.16)
- Rogue devices (8.15)
- Unauthorized access to DFS Data (8.12)
- Denial of Service attack (8.6)

Mobile Network Operator

- Unauthorized access to DFS data (8.12)
- Compromise of DFS infrastructure (8.9)
- Insider attacks (8.7)
- Denial of service (8.6)
- Man-in-the Middle attacks (8.8)
- Unauthorized disclosure of personal information (8.17)
- Malware (8.13)
- Account and session hijack (8.1)
- Code exploitation attack (8.4)
- Data misuse (8.5)

DFS Provider

- Attacks against credentials (8.2)
- Attacks against systems and platforms (8.3)
- Code exploitation attack (8.4)
- Compromise of DFS infrastructure (8.9)
- Compromise of DFS Services (8.11)
- Data misuse (8.5)
- Insider attacks (8.7)
- Denial-of-service attacks (8.6)
- Zero day attacks (8.14)
- Unintended disclosure of personal information (8.17)

3rd Party

- Code exploitation attack (8.4)
- Denial Of Service (8.6)
- Insider attacks (8.7)
- Malware (8.13)
- Unauthorized access to DFS data (8.12)

118 controls developed in framework

Example Threat: Denial of Service

- DoS as an example of the standardized threats we consider (Section 8.7 in the Security Assurance Framework document)
- Characterized as attacks designed to prevent services within the DFS ecosystem from being offered
  - Denial of service is not always caused by malicious attacks – can be the result of service oversubscription (e.g., sudden and massive rise in usage)
- Affected entities: MNO, DFS provider

Threat: Denial of Service (2)

- ***Risks*** at the **MNO:**
  - Inability to perform transaction due to a service outage
  - Transaction failure due to high delays
- ***Vulnerability:***
  - Network failure due to insufficient network capacity or to maintenance or design (*security dimension:* availability)
- ***Controls:***
  - **C22:** The mobile network operator should take steps to ensure network high network availability to allow access to DFS services through USSD, SMS and Internet.
  - **C23:** The MNO should perform technical capacity tests simulating different transactions based on customer numbers, expected growth, expected number of transactions and expected peak periods to ensure continued system performance.

Summary

- Security Assurance Framework is designed to provide guidance to stakeholders within the DFS ecosystem
- Not designed to be static: is a living document where security advice will evolve as new access technologies, vulnerabilities, and threats are discovered
- A systematic approach to developing processes and controls informed by threats and risks against the DFS ecosystem will assure its resilience