DFS Security Assurance Framework

Vijay Mauree, ITU
About ITU

UN specialized agency for ICTs

‘Committed to Connecting the World’

Allocation of radiofrequency spectrum and satellite orbits

Bridging the digital divide

Establishing international standards

ITU Website: www.itu.int
About ITU

* Academia admitted to 3 Sectors of ITU for a single fee

193 MEMBER STATES  700+ PRIVATE-SECTOR ENTITIES  163 ACADEMIA
FIGI Security, Infrastructure and Trust WG

- Led by ITU
- Objectives
  - Build confidence and trust in the use of DFS
  - Develop technical guidelines and best practices for application security
  - Address cybersecurity issues in payments
  - Address unlicensed digital investment schemes (digital ponzi schemes)
  - Investigate impact of new technologies on security and consumer protection

More info see SIT WG Website:
https://www.itu.int/en/ITU-T/extcoop/figisymposium/Pages/FIGISITWG.aspx
DFS Security Assurance Framework

Objectives

- Identify DFS Security Threats and Vulnerabilities
- Propose Mitigation Measures to Security Threats
- Develop Guidelines For a DFS Security Audit
How this framework is formulated

- ISO 27001 – Risk Management Framework
- DFS Stakeholder Analysis for vulnerabilities and threats entry points
- We also consider elements of DFS ecosystems for:
  - Mobile payments using USSD, SMS, IVR and STK
  - Mobile payment applications and digital wallets (e.g. Google Pay, Apple Pay, WeChat Pay).
The ITU Recommendation X.805

The ITU-T Recommendation X.805 security architecture has eight ‘security dimensions’, which are measures designed to address a particular aspect of network security. We use these dimensions to classify and categorize the security controls for the different threats within the DFS ecosystem.
Elements of a DFS ecosystem using USSD, SMS, IVR, STK and NSDT
Mobile payment applications and digital wallets
Risk Assessment Framework (ISO 27001)

**Risk Identification**
- Identify DFS assets
- Identify associated vulnerabilities
- Identify threats
- Identify Existing controls
- Identify consequences

**Risk Analysis**
- Assessment of consequences
- Likelihood and impact of occurrence
- Define inherent risks
- Definition of residual risks

**Risk Evaluation**
- Identify controls implemented to reduce vulnerability
- Evaluate effectiveness of existing controls
- Define Risk Impact

**Risk Acceptance**
- Are risks acceptable

**Monitor and Review**
- Interesting Parties e.g. Regulators

**Establish Context**
- Risk Assessment
  - Identify Risks
  - Analyze Risks
  - Evaluate Risks

**Communicate Risks**
- Management

**Establish Context**
- Is risk assessment complete
  - Yes
  - No

**Treat Risks**
- Is risk acceptable
  - Yes
  - No

**Communicate Risks**
- Management

**Establish Context**
- Risk Assessment
  - Identify Risks
  - Analyze Risks
  - Evaluate Risks

**Risk Acceptance**
- Are risks acceptable

**Risk Identification**
- Identify DFS assets
- Identify associated vulnerabilities
- Identify threats
- Identify Existing controls
- Identify consequences

**Risk Analysis**
- Assessment of consequences
- Likelihood and impact of occurrence
- Define inherent risks
- Definition of residual risks

**Risk Evaluation**
- Identify controls implemented to reduce vulnerability
- Evaluate effectiveness of existing controls
- Define Risk Impact
The Threats to DFS Ecosystem

**User**
- Social engineering
- Unauthorized access to mobile device
- Disclosure of personal information

**Mobile Device and simcard**
- Code exploitation attack
- Malware
- Unauthorized access to mobile device/SIM
- Rogue devices
- Unauthorized access to DFS Data
- Denial of Service attack

**Mobile Network Operator**
- Signaling and control channel attacks
- Compromise of MNO infrastructure
- Compromise of MNO Services
- Insider attacks
- Denial-of-service attacks
- Man-in-the-Middle attacks
- Unauthorized disclosure of personal information
- Malware
- Account and session hijack
- Code exploitation attack
- Data misuse
- Malware

**DFS Provider**
- Attacks against credentials
- Attacks against systems and platforms
- Code exploitation attack
- Compromise of DFS infrastructure
- Compromise of DFS Services
- Data misuse
- Insider attacks
- Denial-of-service attacks
- Zero day attacks
- Unintended disclosure of personal information

**3rd Party**
- Code exploitation attack
- DOS
- Insider attacks
- Malware
- Unauthorized access to DFS data
Controls

- Use X.805 security dimensions as a way of classifying the vulnerabilities that arise from the threats
- Categorize the controls in terms of generalized threats: allows coalescing of threats common across multiple stakeholders to simplify discussion
- Risks, vulnerabilities, and threats discussed relative to the given stakeholder
Example Threat:
Account and Session Hijacking

- General threat: ability of an attacker to take control of an account or a communication session

- Affected entities (DFS stakeholders): DFS Provider, MNO
Example Threat: Account and Session Hijacking

- At the DFS provider:
  - Risk: *data exposure and modification*
  - Vulnerability: *Use of credentials to elevate access*
  - X.805 Security dimension: *access control*

- Controls:
  - **C1**: Set user session timeouts and auto logouts for access to DFS applications (logical sessions). Within the application, ensure support for password complexity (enforced by the server), set unsuccessful login attempts, password history and reuse periods, account lock-out periods to a reasonable minimal value in order to minimize the potential for offline attack.
Example Threat: Account and Session Hijacking

- At the DFS provider (continued):
  - Risk: *unauthorized account takeover*
  - Vulnerability: *Inadequate controls on dormant accounts*
  - X.805 Security dimension: *authentication*
  - Controls:
    - **C2**: Require user identity validation for dormant DFS accounts users before re-activating accounts.
Thank You

vijay.mauree@itu.int