TIC Working Group Security Recommendations

Workshop on DFS and Financial Inclusion
Washington, DC, USA
19 April 2017

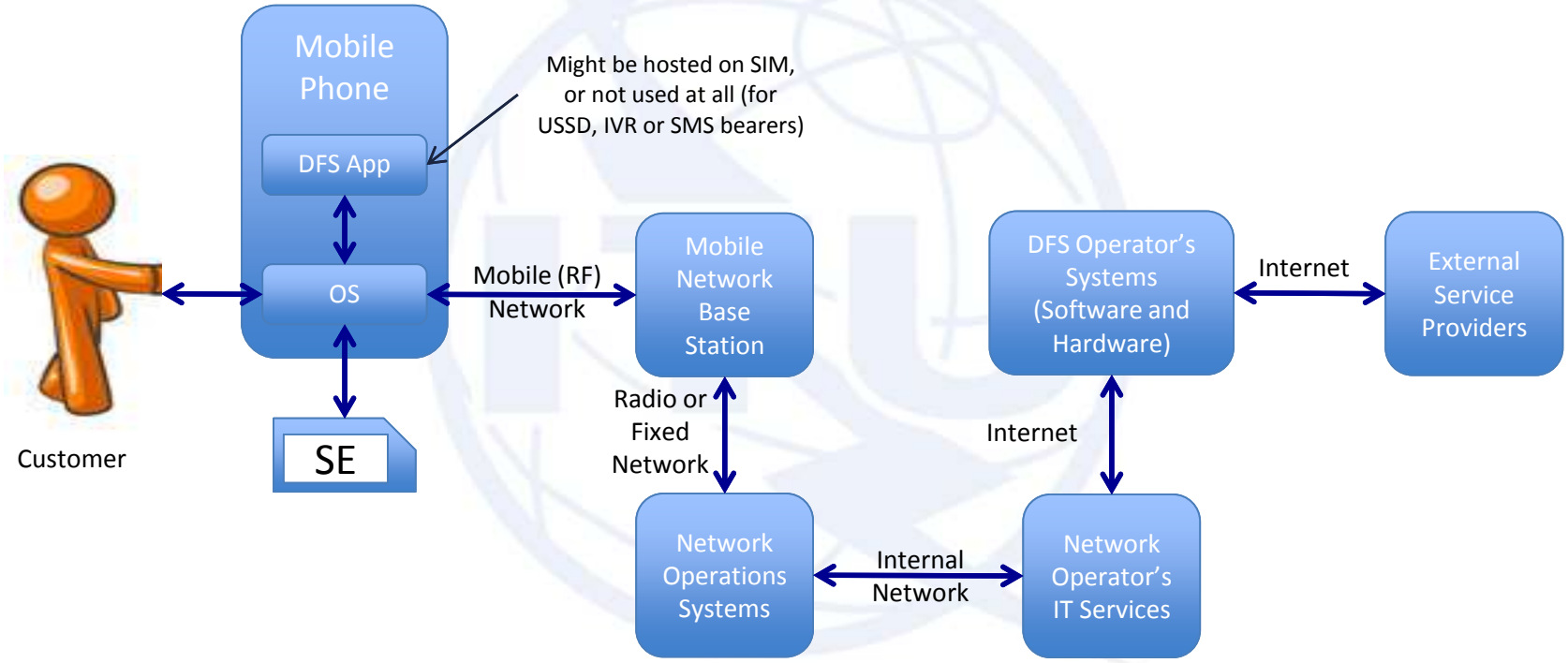
Background and Motivation

- DFS applications offer the promise of enabling financial inclusion.
- While mobile money and payment systems have seen widespread adoption, serious challenges to their security have been presented.
- Many emerging threats in the DFS ecosystem and many new stakeholders need to be protected as cyber-enabled attackers can exploit multiple attack vectors.
- Security must be managed at multiple layers, from operational policy to securing hardware and software.

Technical Ecosystem: Security Dimensions

The hardware, software and services that underpin DFS service delivery

Any digital / mobile financial service relies on a combination of IT systems and mobile or fixed networks, and is therefore itself vulnerable to the various weaknesses of that ecosystem.



There are many elements of this ecosystem – including the links between the elements - and each has its own vulnerabilities. It should also be noted that systems and services are, in almost every case, combinations of hardware and software.

Context: X.805

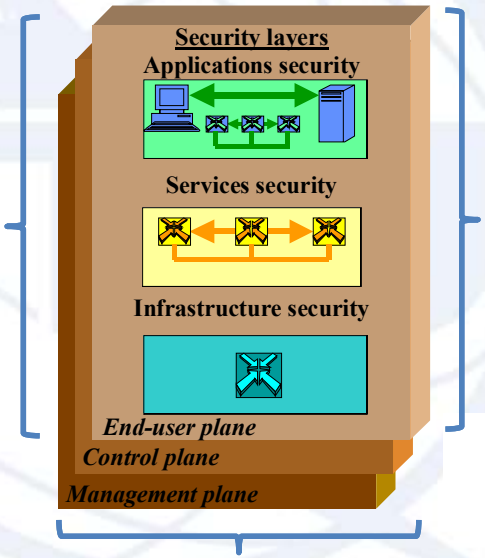
Security dimensions, layers and planes

ITU-T has defined X.805 as the standard for the "Security architecture for systems providing end-to-end communications". Although its origins are in the management of the security of network and telecommunication services, it provides a useful reference framework for the security management of digital financial services.

The approach X.805 takes to service management is founded on eight 'security dimensions'. Each of these applies across three 'security layers', which in turn are considered to act across three 'security planes'.

The dimensions must be applied to 'a hierarchy of network equipment and facility groupings', which build on one another to provide network-based solutions. This hierarchy is:

- **The Applications Security Layer**
- **The Services Security Layer**
- **The Infrastructure Security Layer**



X.508 defines security dimensions as 'a set of security measures designed to address a particular aspect of network security'. Eight security dimensions are defined:

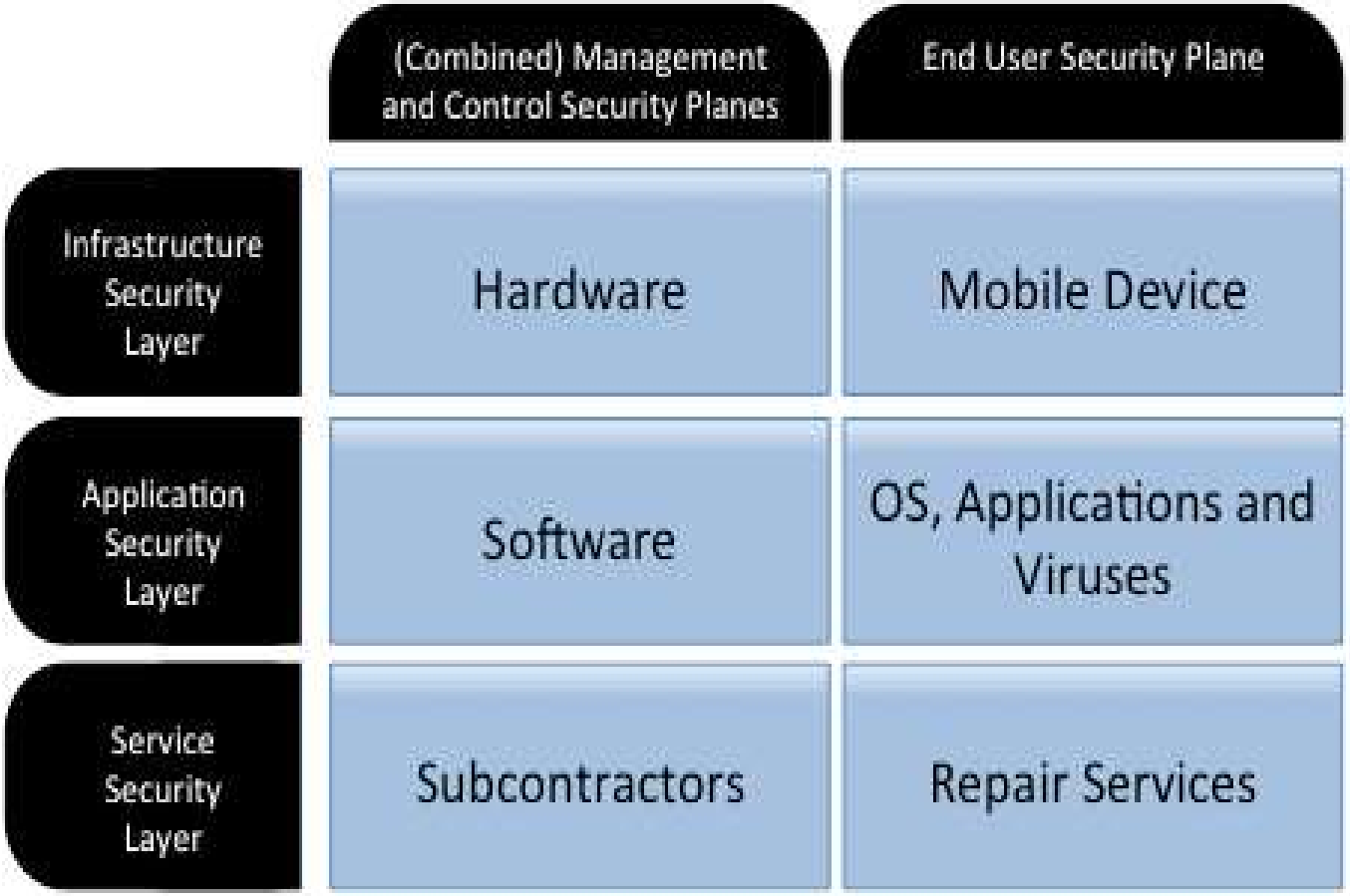
- **Access control**
- **Authentication**
- **Non-repudiation**
- **Data confidentiality**
- **Communication security**
- **Data integrity**
- **Availability**
- **Privacy**

In addition, X.508 describes security planes, defined as 'a certain type of network activity protected by security dimensions'. These are:

- **The Management Plane**
- **The Control Plane**
- **The End-User Plane**

Layers and Planes

Within DFS, this is how layers and planes can be represented:



Y.2740 Security Levels

Security dimension	Security level			
	Level 1	Level 2	Level 3	Level 4
Access control	The access to every system component shall be granted to authorised system personnel only. The activation of special applications uploaded to mobile terminals should be permitted to authorised clients only.			
Authentication	System authentication is ensured by the next-generation network (NGN) data transfer environment.	Single-factor authentication at system services usage.	Multifactor authentication at system services usage.	In-person subscription to services where personal data with obligatory identification is used. Multifactor authentication at system services usage. Obligatory usage of a hardware cryptographic module.
Non-repudiation	The impossibility of a transaction initiator or participant denying his or her actions upon their completion is ensured by explicit and implicit legal contracts legally stated or reserved in mutual contracts means and accepted authentication mechanisms. All system personnel and end-user actions shall be logged. Event logs shall be change-proof and hold all actions of all users.			
Data confidentiality	Ensured by environment, storage, access control (communications security)	Ensured by additional message encryption/protocols		

Methodology

- Consider each stakeholder within the DFS ecosystem as defined in the previous diagram and consider their role in the ecosystem.

- With regards to each of the eight security dimensions defined by the X.805 standard, consider threats and vulnerabilities against each element.

- Based on this threat model, recommend strategies for mitigating threats/vulnerabilities.

- Example: *mobile phone application*
  - **Role within the ecosystem:** Represents the primary means by which customers interface with DFS, either through direct interaction or mediated by an agent.
  - **Threats and Vulnerabilities (examples):**
    - ***Access Control:*** Risk of attackers leveraging code vulnerabilities, misconfigured permissions settings that can allow unauthorized information disclosure
    - ***Authentication:*** applications that do not sufficiently protect password and PIN credentials allow adversary to maliciously authenticate as the customer
  - **Recommended mitigations:** Design and implement apps in accordance with best practices (e.g., encrypted communication, secure coding practice); external review and pen-testing for apps; secure data management within apps of username and passwords so credentials cannot be forged; strong authentication mechanisms

Scope of Recommendations

- Cooperation and MOUs
- Mobile Devices
- DFS Apps
- Network Access and Fake Base Stations
- Trusted Phone Number Spoofing
- SIM Cards
- Infrastructure Security
- Third-Party Providers
- Companion Cards
- Consumer Protection

Recommendation Summary

- 21 specific security recommendations made with regards to DFS stakeholders
- An additional 72 recommendations for the protection of information technology systems, which are used within and across stakeholders in the DFS ecosystems, spanning the following broad areas:
  - Policies and access control
  - Systems Development
  - Audit and Response

Overall Summary of Recommendations

- It is clear that the security of mobile payment transactions rests on the safe and secure transmission of data between users and payment providers. We thus strongly recommend the development and implementation of end-to-end security techniques to ensure data stays confidential and has integrity protection from the time it leaves the user's handset until it is delivered to its destination. The response from the provider to the user should be similarly protected.

- Mobile devices increasingly contain additional hardware to improve data security; we recommend that DFS providers make use of these technologies to assure the security of information on the mobile device platform.

- Best practices for data handling within DFS provider systems and networks, such as the maintenance of audit logs, the use of least privilege, assuring data confidentiality, and premises security, are essential to ensuring the security of data and increasing its resistance to data breach attacks. The development of security benchmark assessments and regular testing of defenses to protect against new attacks is vital to assuring the continued security of stored data in these environments.