ITUWebinars

Digital financial services

Episode #1: Addressing SS7 vulnerabilities affecting digital financial services

14:00 - 15:00 CET
18 February 2025
Fully virtual

itu.int/en/ITU-T/webinars/dfs/sc

Digital Financial Services (DFS) Webinar Series

Addressing SS7 Vulnerabilities affecting Digital Financial Services

18 February 2025
14:00 - 15:00 CET
Fully Virtual

Join us online!
http://www.itu.int/go/dfs_ws_ss7

Arnold Kibuuka
Project Officer
ITU-T

Assaf Klinger
Head of R&D,
Vaulto

ITUWebinars

Digital financial services

Episode #1: Addressing SS7 vulnerabilities affecting digital financial services

Assaf Klinger,
CEO, **Klinger Consulting**

itu.int/en/ITU-T/webinars/dfs/sc

A LITTLE ABOUT MYSELF

- Husband, father (+2), geek 8-)
- Security researcher for the last 20 years
  - Specialize in telecom, IoT & blockchain
  - Member of ITU-T Study Group 11
  - Member DFGI SA WG
- Handles:

Assaf.klinger@gmail.com

@AssafKlinger

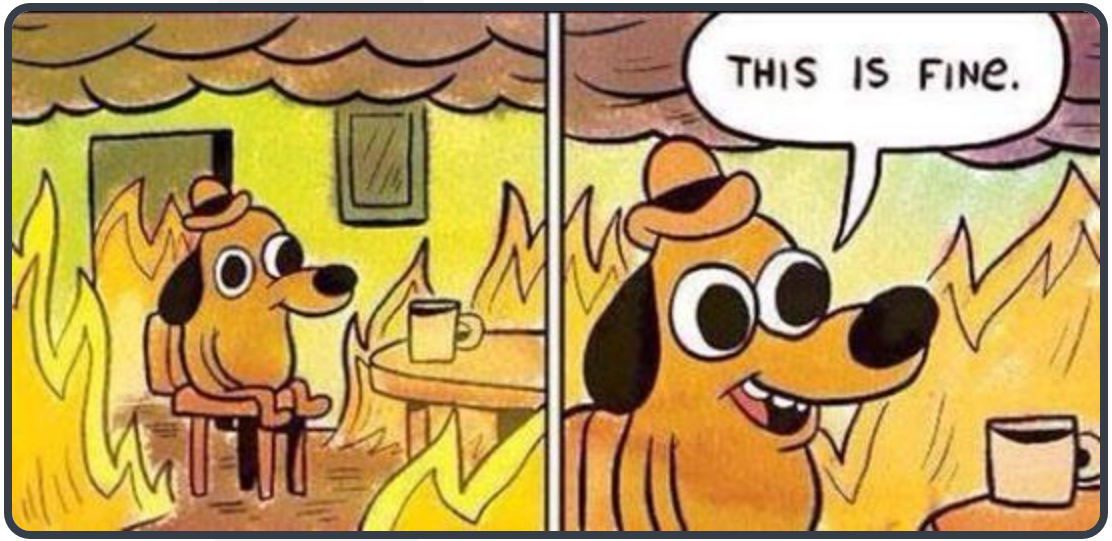
https://www.linkedin.com/in/assaf-klinger-8a0b7159/

DFS - DIGITAL FINANCIAL SERVICES

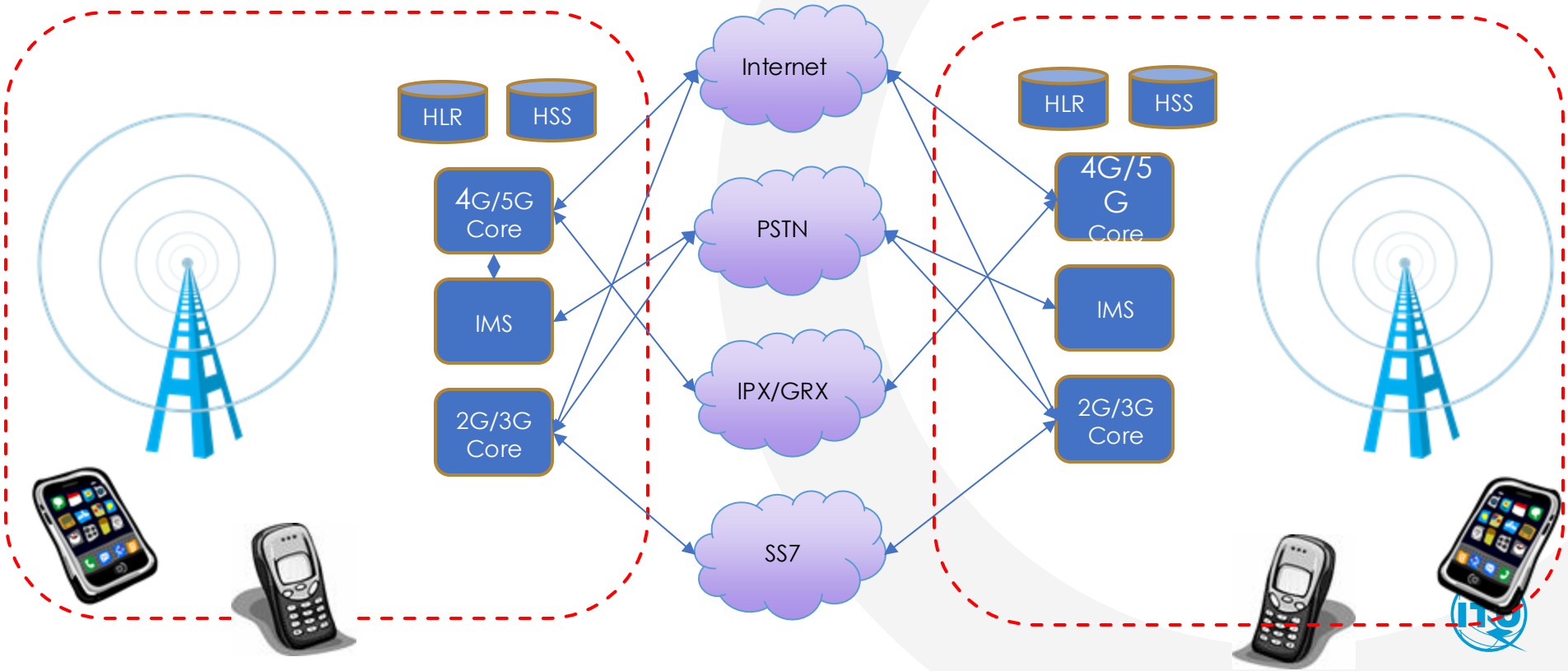
- Digital financial services (DFS) relies heavily on the underlying teleco infrastructure to enable users send and receive money
- DFS is very popular in developing countries where traditional banking infrastructure is not present
- The channels in which the end-user communicates with the DFS provider are mostly USSD and SMS, due to the lack of 3G/LTE deployment in these countries.

SS7: VULNERABILITY BY DESIGN

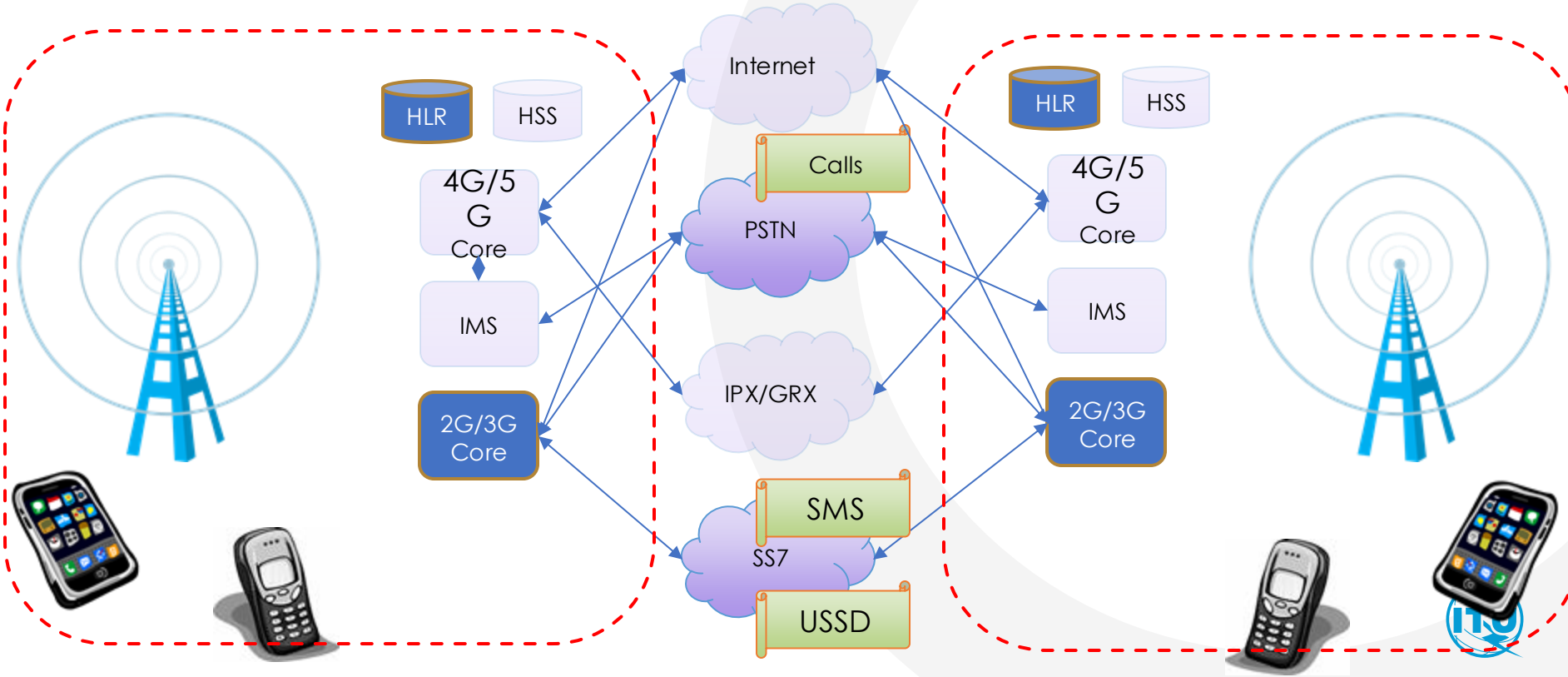
- Flat network (switched, not routed, no NATs)
- Static address allocation (ITU managed)
- All network elements are trusted without question
- No encryption
- No authentication required to join the network



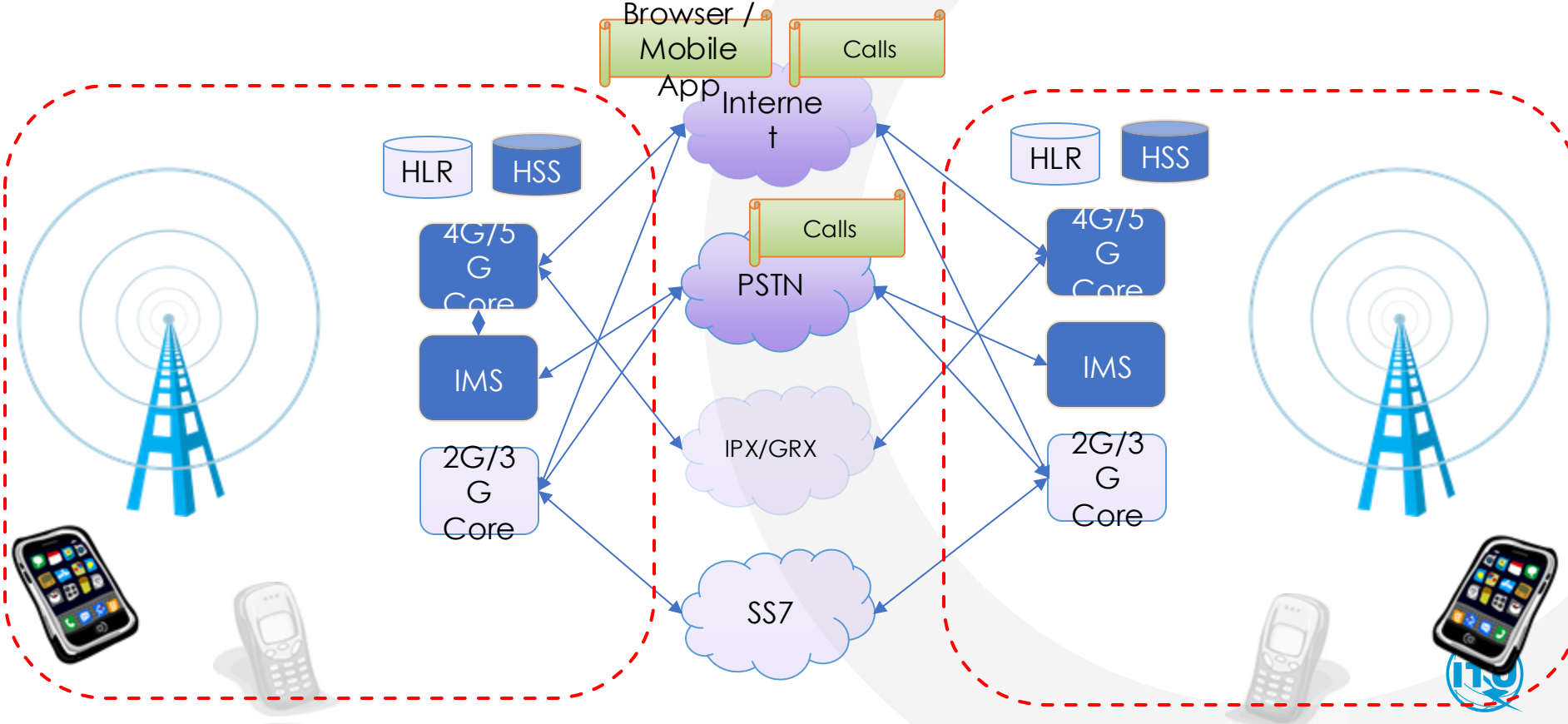
TELCO'S CORE NETWORK



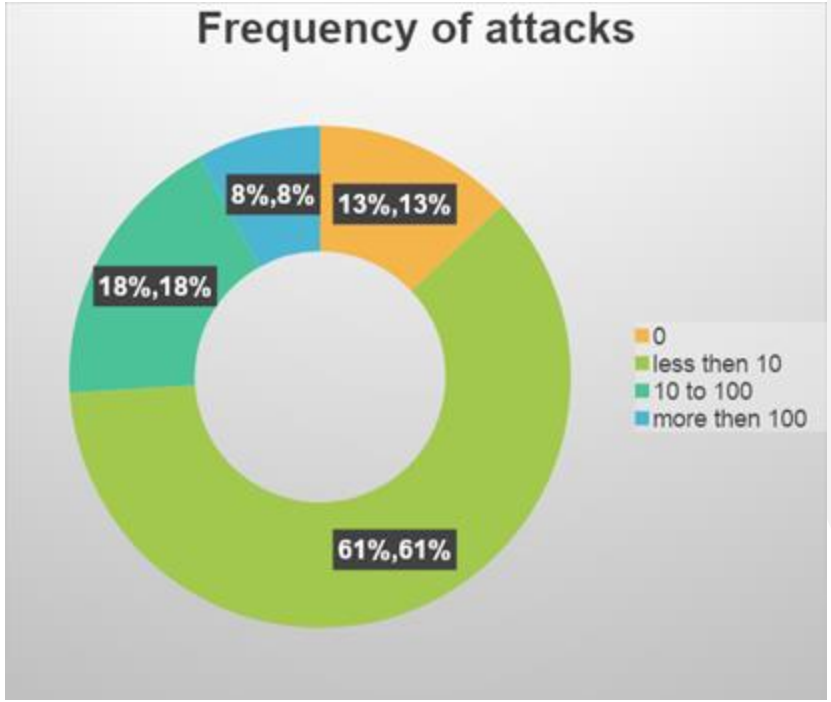
DFS SERVICES OVER TELECOM

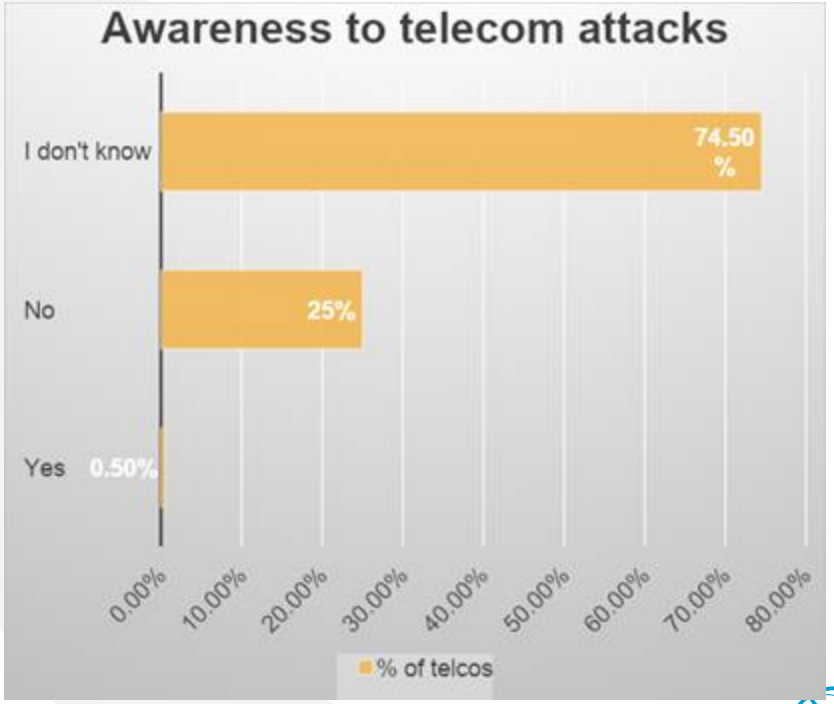


DFS SERVICES OVER MOBILE INTERNET



THE COMMONALITY OF TELECOM ATTACKS





EXAMPLE FROM A MAJOR EU OPERATOR

Cat.	Events	Action	Min.	Max.	Average	
	Total throughput		375 M	517 M	454 M	
1	**All Category 1**					
	ATI, SRI, SendIMSI	Blocked	560	3.835	3.200	100%
2	**All Category 2**		24,6 M	30,1 M	27,8 M	
	- Home IMSI	Blocked	2	40	21	0,75 pm
	- GT Mismatches	Still pass	10.500	19.930	15.300	550 pm
	- SSN Mismatches	Still pass	123	332	210	7,5 pm
3.1	**All Category 3.1**		224 K	360 K	294 K	
	- No or Unexpected Location	Blocked	84	9.700	4.400	1,50%
	- Foreign IMSI	Still pass	3	42	15	51 pm

MAJOR TYPES OF TELECOM ATTACKS ON DFS

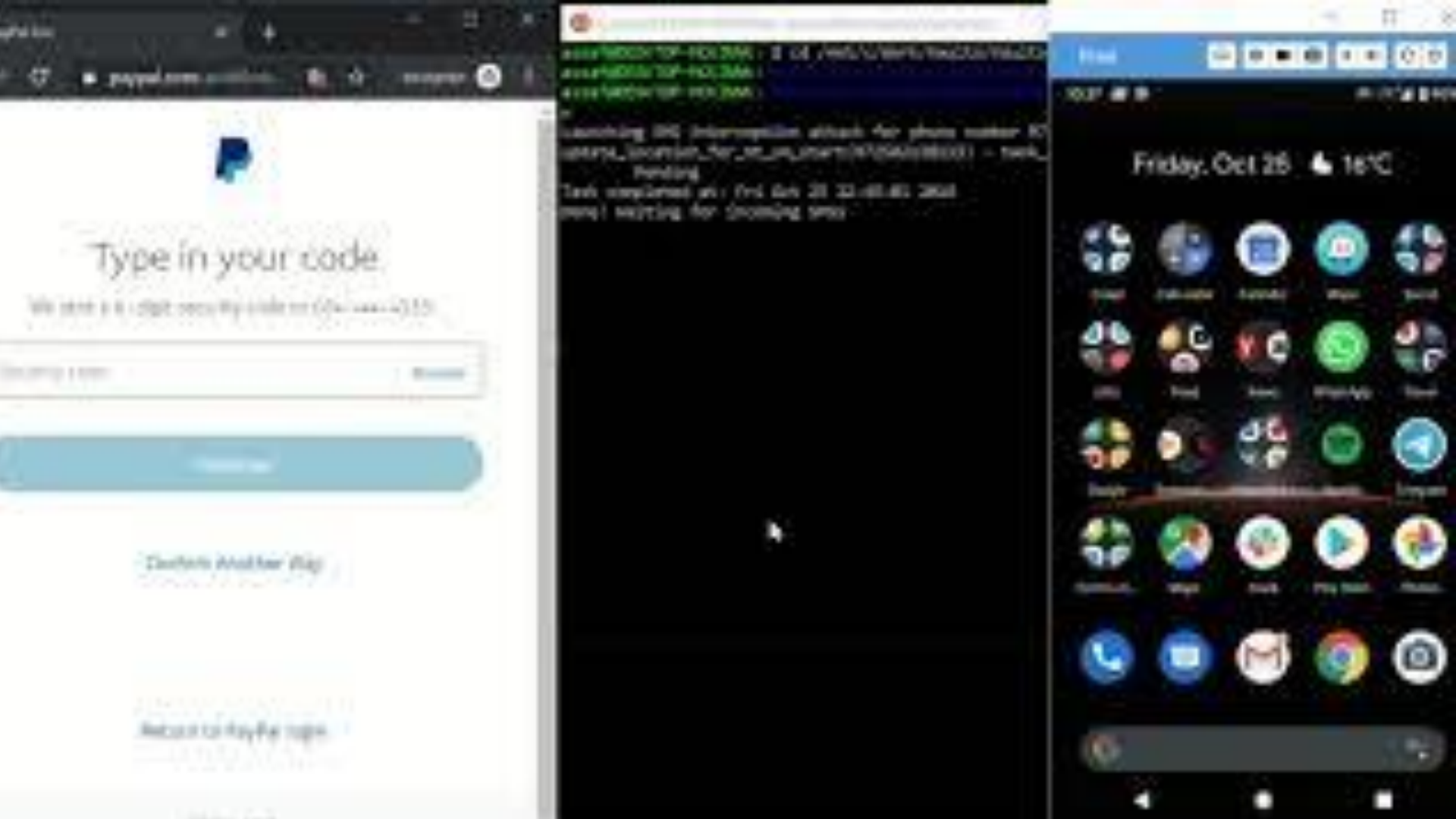
Caller ID spoofing

2FA account takeover

SIM swap

2FA SMS INTERCEPTION

Example


Type in your code
Friday, Oct 25
16°C

SS7 CALL INTERCEPTION

Example

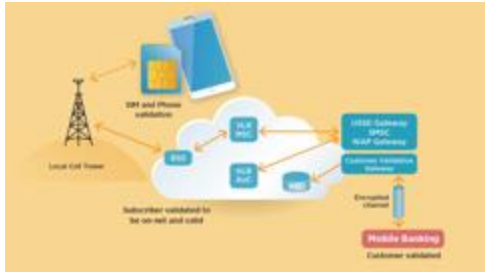

054-255-8192
Attack a mobile phone
Vaulto-galaxyS5
<— Target

MITIGATION MEASURES

For DFS providers

- Change the direction of 2FA

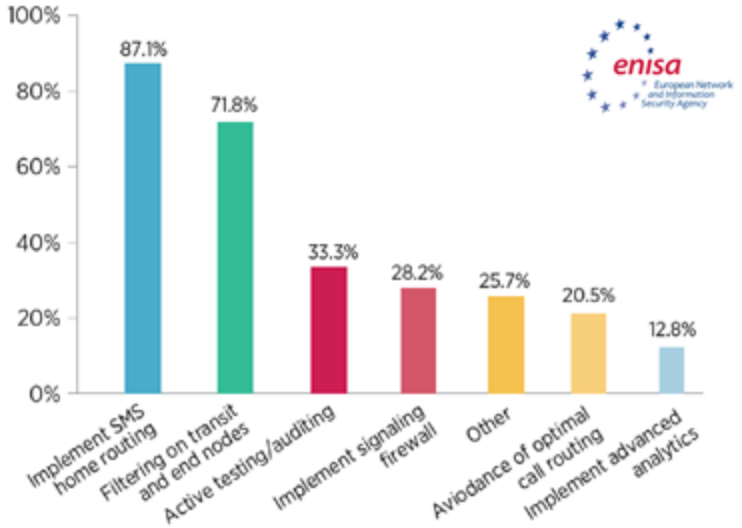
- Use a SIM Validation gateway

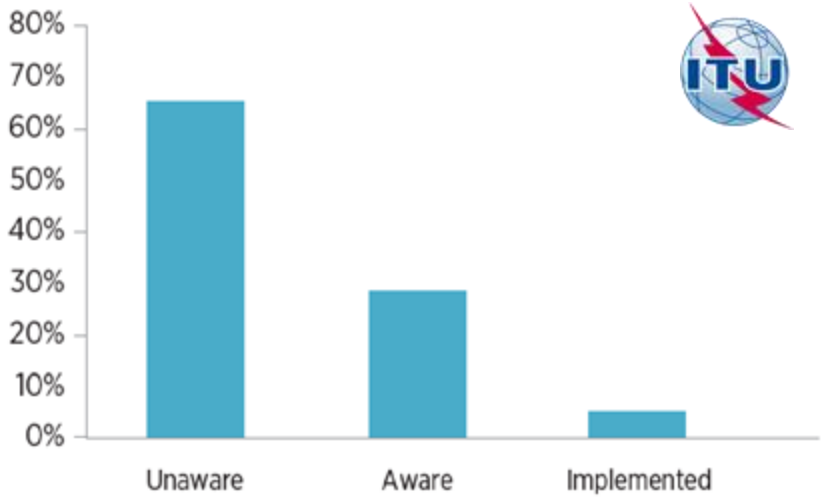


For Operators

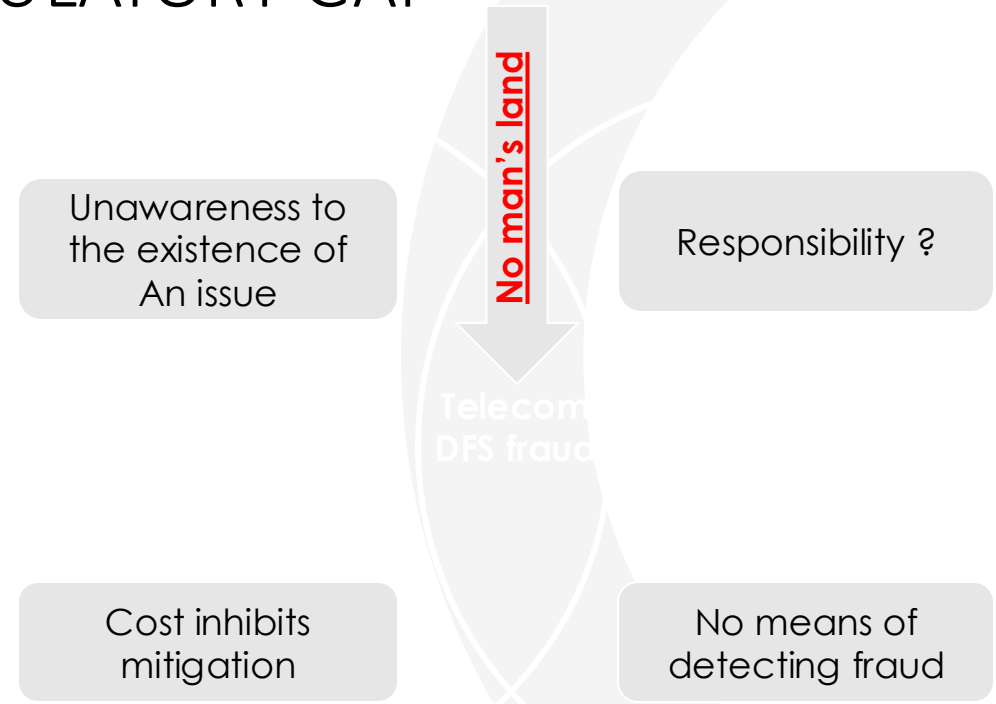
Attack	FS.11 (2/3G)	FS.07 (2/3G)	IR.82 (2/3G)	IR.88 (4G)
Spoofing	✓	✓	✓	×
SMS Hijack	×	✓	×	×
SIM swap	×	✓	✓	✓

IMPLEMENTATION OF COUNTERMEASURES





THE REGULATORY GAP



Mitigation Measures

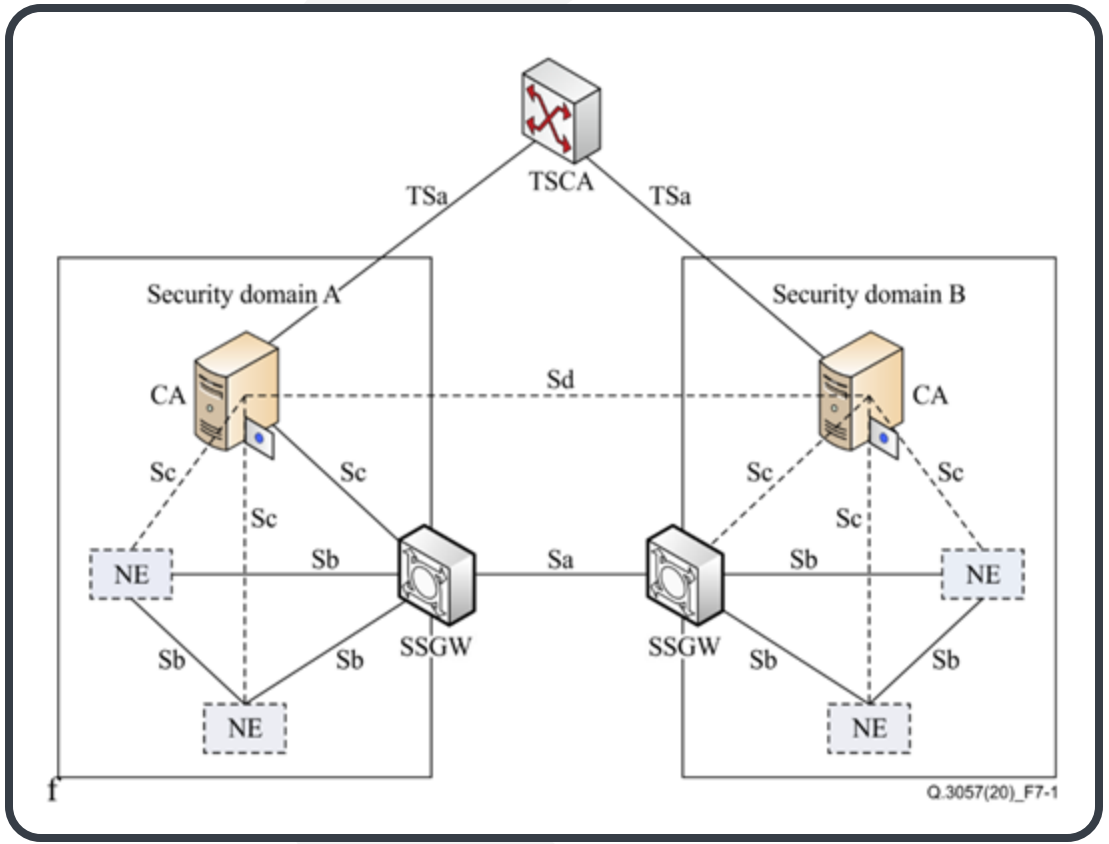
1. **Standardize trust in telecom signaling**
   - On going work in ITU-T study group 11
2. **Build an international trust chain**
   - WTSA Resolution 65 and on going work in study group 2 and study group 11
3. **Create a security posture baseline**
   - Telecom regulators to establish baseline security measures
4. **Close the regulatory gap by (financial <-> telecom)**
   - bilateral Memorandum of Understanding (MOU) related DFS should be in place between the telecommunications regulator and the central bank

Standardize trust in telecom signaling

- SG11 conducts several activities to advance SS7 security
  - Recommendation ITU-T Q.3057, Q.3062 & Q.3063 were approved in 2022
  - Technical report on USSD encryption was released in 2021
- ITU conducts security clinics and webinars on how to address SS7 vulnerabilities

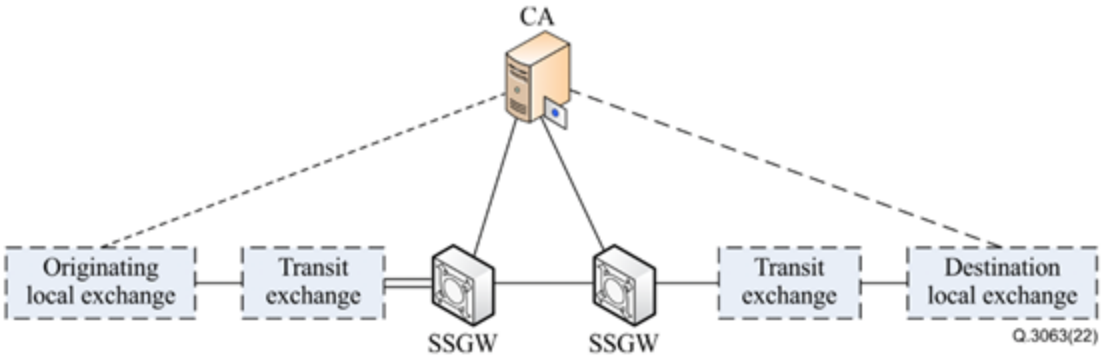
ITU-T Q.3057 & Q.3062

- Add digital signature to SS7 messaging (based on TCAP-SEC)
- Prevents hackers from impersonating legitimate network functions on the SS7 network
- Enables operators to manage trust of other operators
- Using PKI as a reference model



ITU-T Q.3063
CALLING LINE IDENTIFICATION AUTHENTICATION

-
-
-



TR-USSD ENCRYPTION

- Advances in encryption implementation and sim card technology enable advanced crypto to run from STK
- USSD encryption can be implemented, **and be quantum safe**
- The TR surveys **available** technologies that can be used **today**
- The quantum safe crypto can be used in feature phones (STK)

Standardize trust in telecom signaling - Q.TSCA

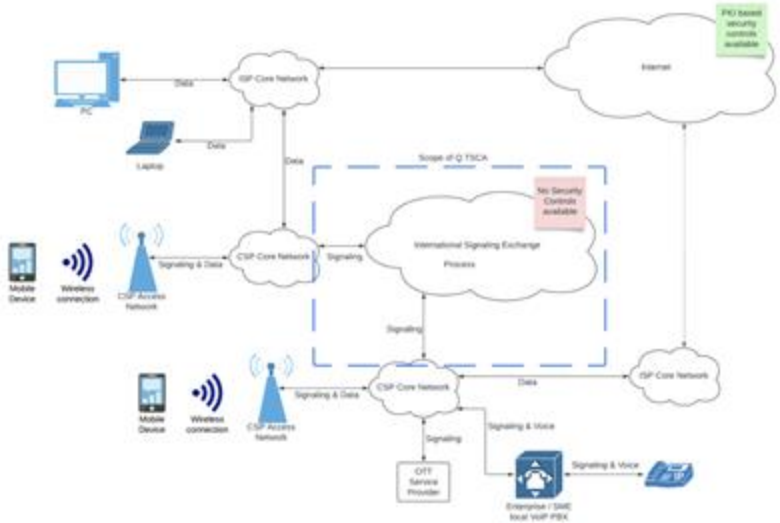


Figure 1 - current connectivity of CSPs to the international signalling exchange networks

Figure 2 - general representation for the TSCA trust chain.

Create a security posture baseline - Q.DMSA

- Telecom signaling networks are critical to the operation of mobile networks
- they are also susceptible to a range of sophisticated attacks.
  - Simple, Single Request Attacks
  - Single Protocol, Multi-Request Attacks
  - Multi-Protocol Attacks
  - Cross-Generational Signaling Attacks

Signaling attack detection methods - Q.DMSA

- SSGW Authentication and Verification: ensuring only legitimate messages enter the core network, the SSGW blocks forged or manipulated signaling requests that might otherwise trigger attacks.
- Rate Limiting and White-List Enforcement: crucial for mitigating simple, single-request attacks and multi-request attacks that attempt to overwhelm network elements.
- Heuristics Analysis: catches subtle, engineered discrepancies that may indicate tampering or malicious intent, especially effective against multi-protocol and multi-request attacks
- Anomaly Detection: monitor traffic patterns across the network, can detect inter-operator anomalies (such as SMS routes that deviate from standard A2P channels) as well as subscriber-level anomalies (such as unusual activity during off-peak hours)
- Cross-Protocol Consistency Checks: verify that information remains consistent as it passes between different protocols (e.g., confirming that data extracted via SS7 matches corresponding Diameter or SIP messages)

THANK YOU

Join the ITU DFS Security Knowledge Sharing Platform

https://www.itu.int/en/ITU-T/dfs/Pages/share-platform.aspx

ITUWebinars

Digital financial services

Episode #2: Securing Mobile Payment Applications - 1

14:00 – 15:00 CET
26 March 2025
Fully virtual

itu.int/en/ITU-T/webinars/dfs/sc