ITUWebinars

Signalling Security

Enhancing signalling security and privacy using globally interoperable digital signatures

16 June 2022
15:00-17:00, CEST

Assaf Klinger, SG11

https://itu.int/go/WB-SSP-01

Agenda

- Overview of the SS7 signalling network and main use cases
- Current security issues in signalling protocols
- Available mitigations and their limitations
- Applying globally interoperable digital signatures signalling messages: ITU-T Q.3057 and draft Q.Pro-Trust.
- Use cases for application of Recommendations for improving signalling security: CID (over interconnect) and Roaming

A little about myself

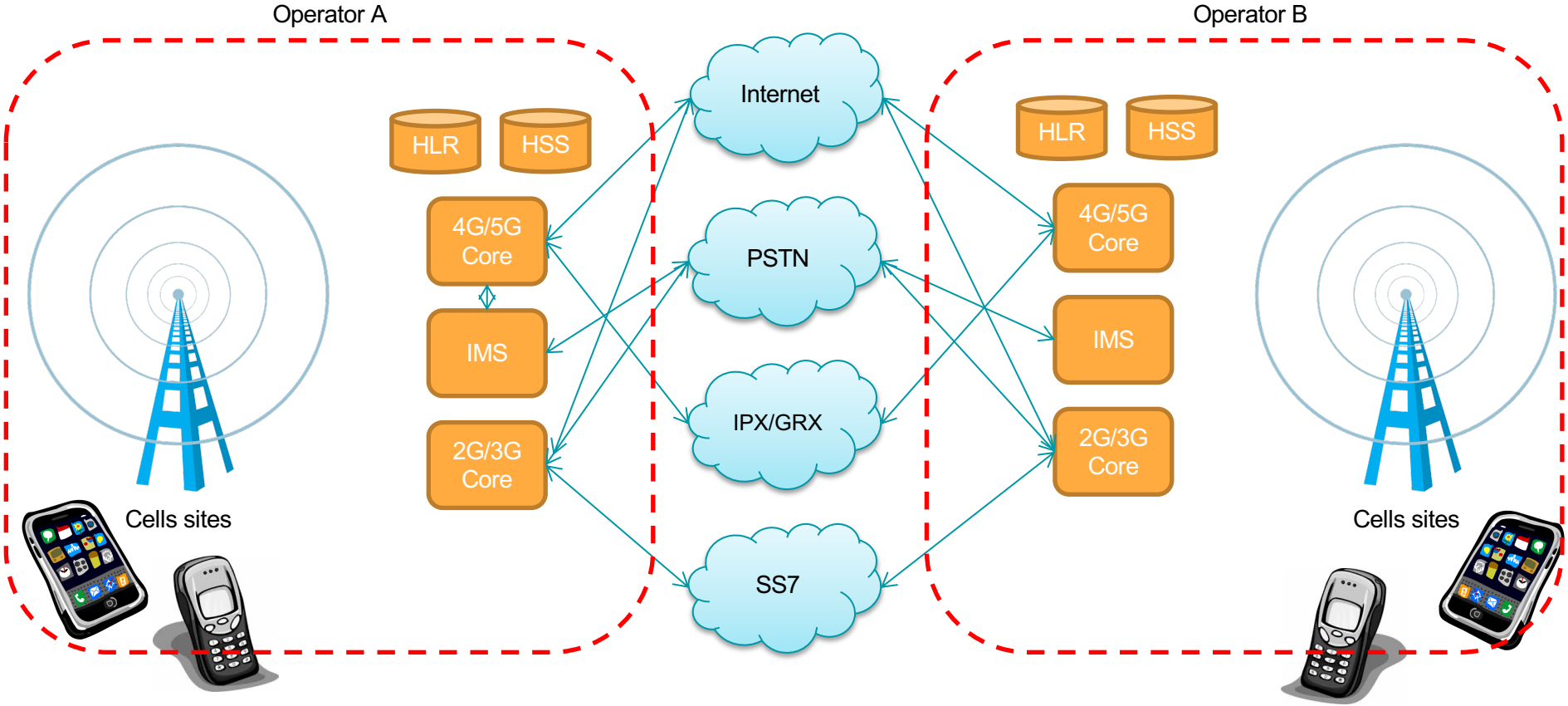
- Husband, father (+2), geek 8-)
- Security researcher for the last 18 years
  - Specialize in telecom, IoT & blockchain
  - Editor of ITU-T Study Group 11 recommendations
  - Member of FIGI SIT WG & DFGI SA WG
- Handles:

Assaf.klinger@gmail.com

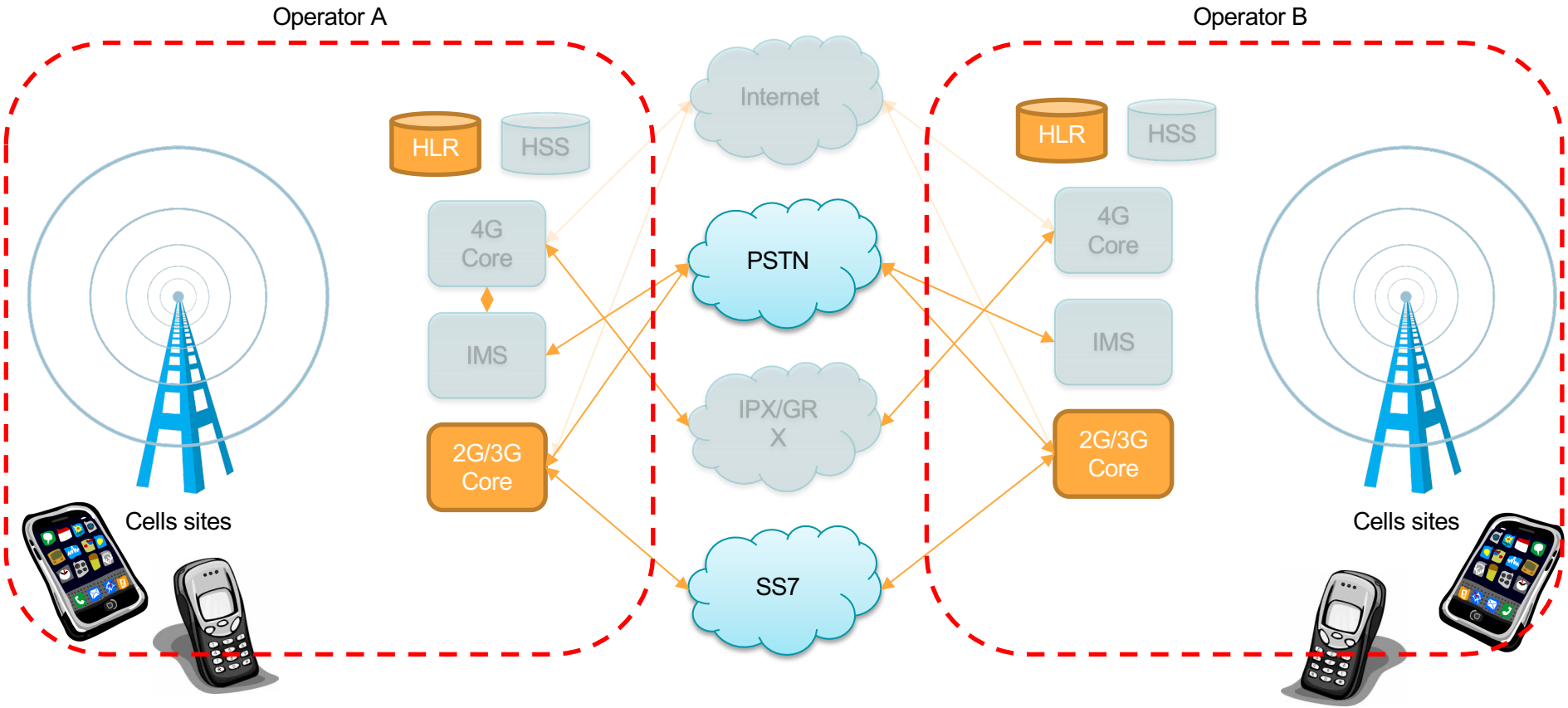
@AssafKlinger

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

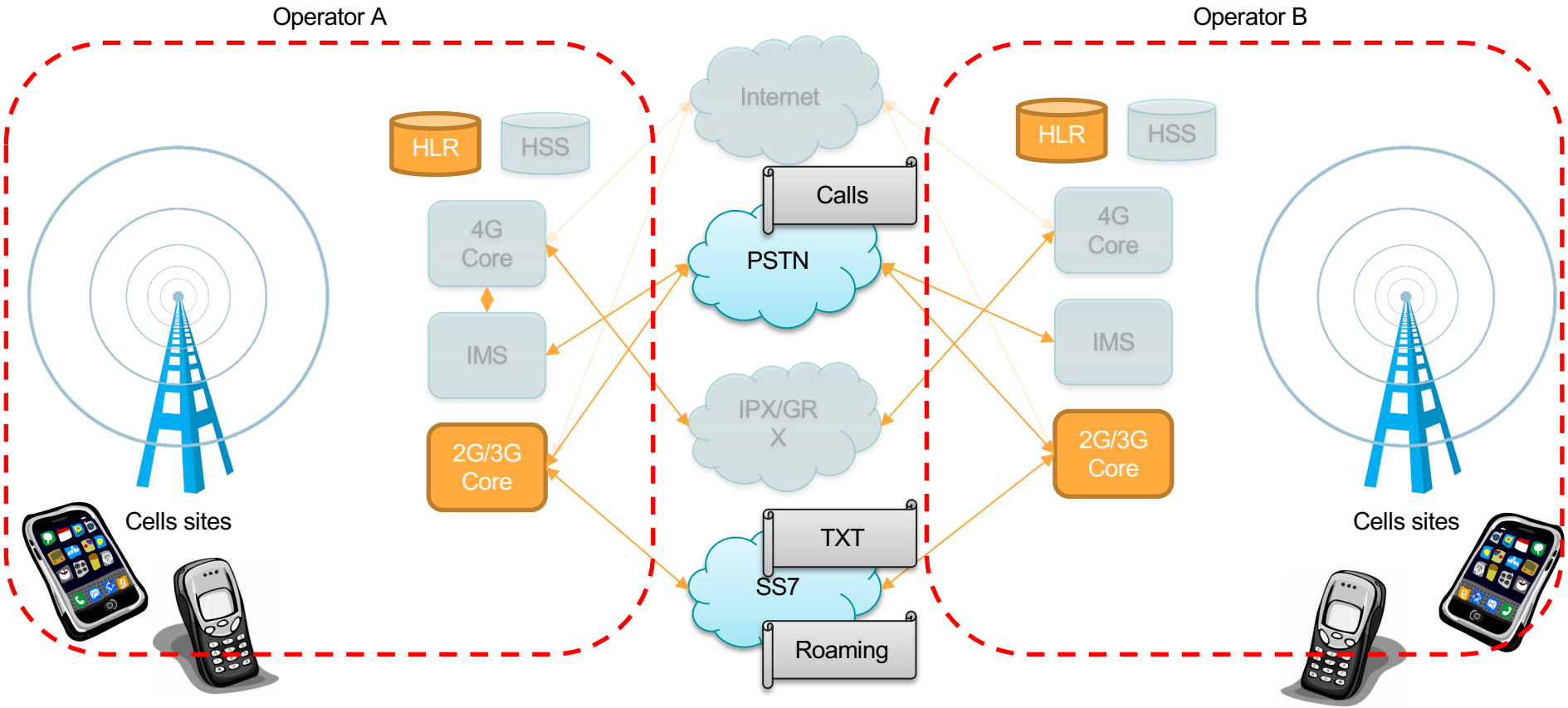
Telco’s core network (very high level)



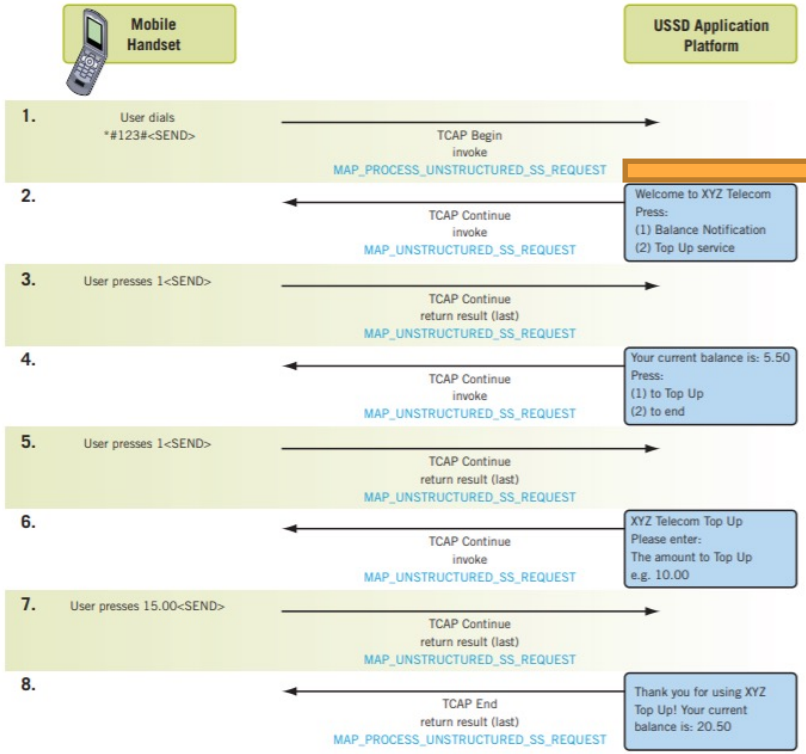
The scope of SS7



Telecom services over SS7



Example: MO USSD call flow

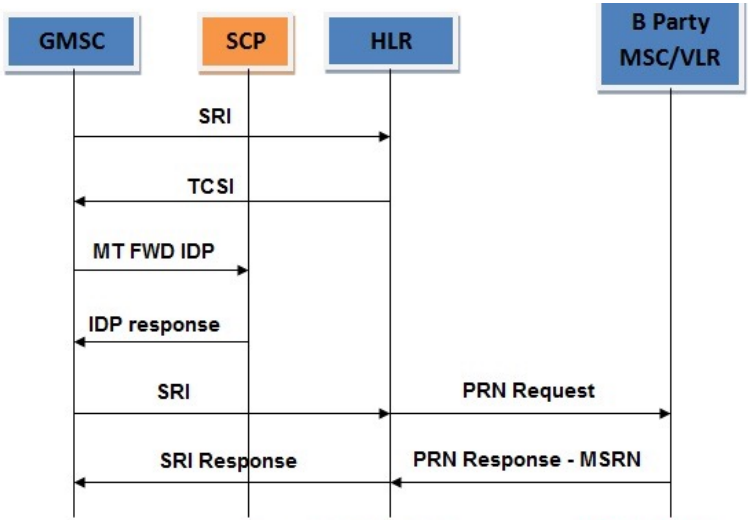


No.	Time	Source	Destination	Protocol	Length	Info
1	13:08:00.624000	1041	8744	GSM MAP	218	invoke processUnstructuredSS-Request

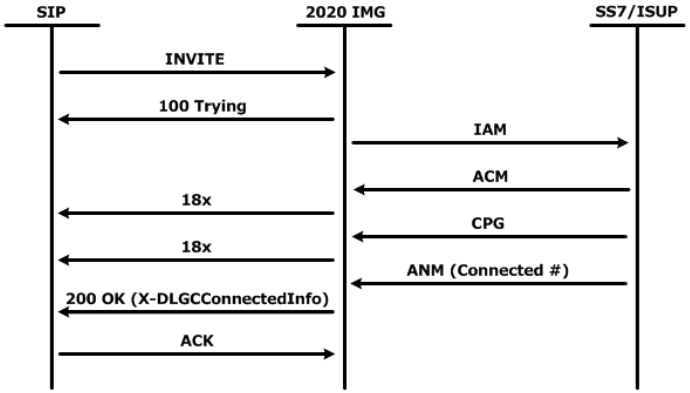
```
> Frame 1: 218 bytes on wire (1744 bits), 218 bytes captured (1744 bits)
> Ethernet II, Src: Private_01:01:01 (01:01:01:01:01:01), Dst: MS-NLB-PhysServer-02_02:02:02:02 (02:02:02:02:02:02)
> Internet Protocol Version 4, Src: 1.1.1.1, Dst: 2.2.2.2
> Stream Control Transmission Protocol, Src Port: 2904 (2904), Dst Port: 2904 (2904)
> MTP 2 User Adaptation Layer
> Message Transfer Part Level 3
> Signalling Connection Control Part
> Transaction Capabilities Application Part
v GSM Mobile Application
  v Component: invoke (1)
    v invoke
        invokeID: 1
      > opCode: localValue (0)
      > ussd-DataCodingScheme: 0f
      v ussd-String: aa180da682dd6c31192d36bbdd46
          USSD String: *140*0761241377#
      v msisdn: 917267415827f2
          1... .... = Extension: No Extension
          .001 .... = Nature of number: International Number (0x1)
          .... 0001 = Number plan: ISDN/Telephony Numbering (Rec ITU-T E.164) (0x1)
        v E.164 number (MSISDN): 27761485722
            Country Code: South Africa (Republic of) (27)
```

Other Examples

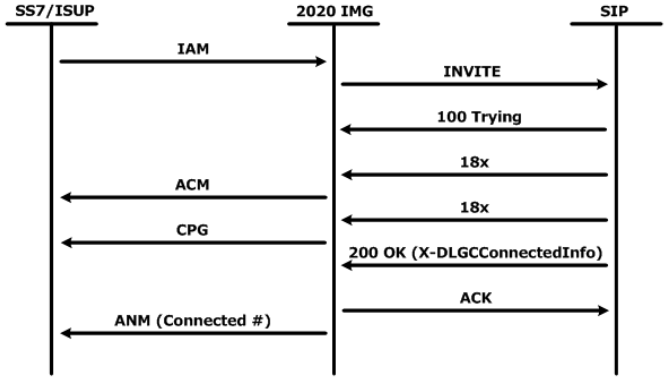
ISUP Roaming call flow



SIP to ISUP call

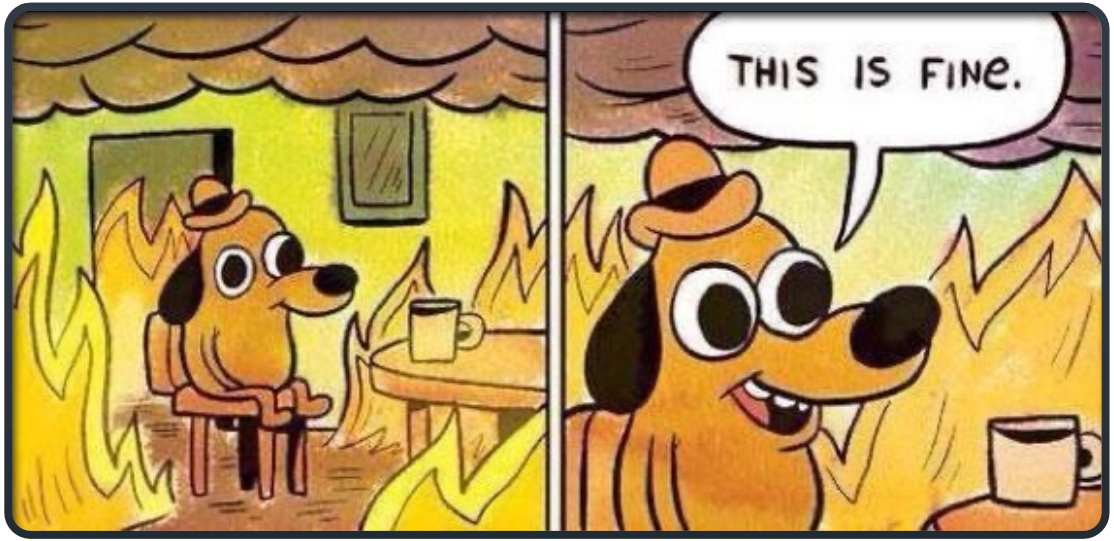


ISUP to SIP call

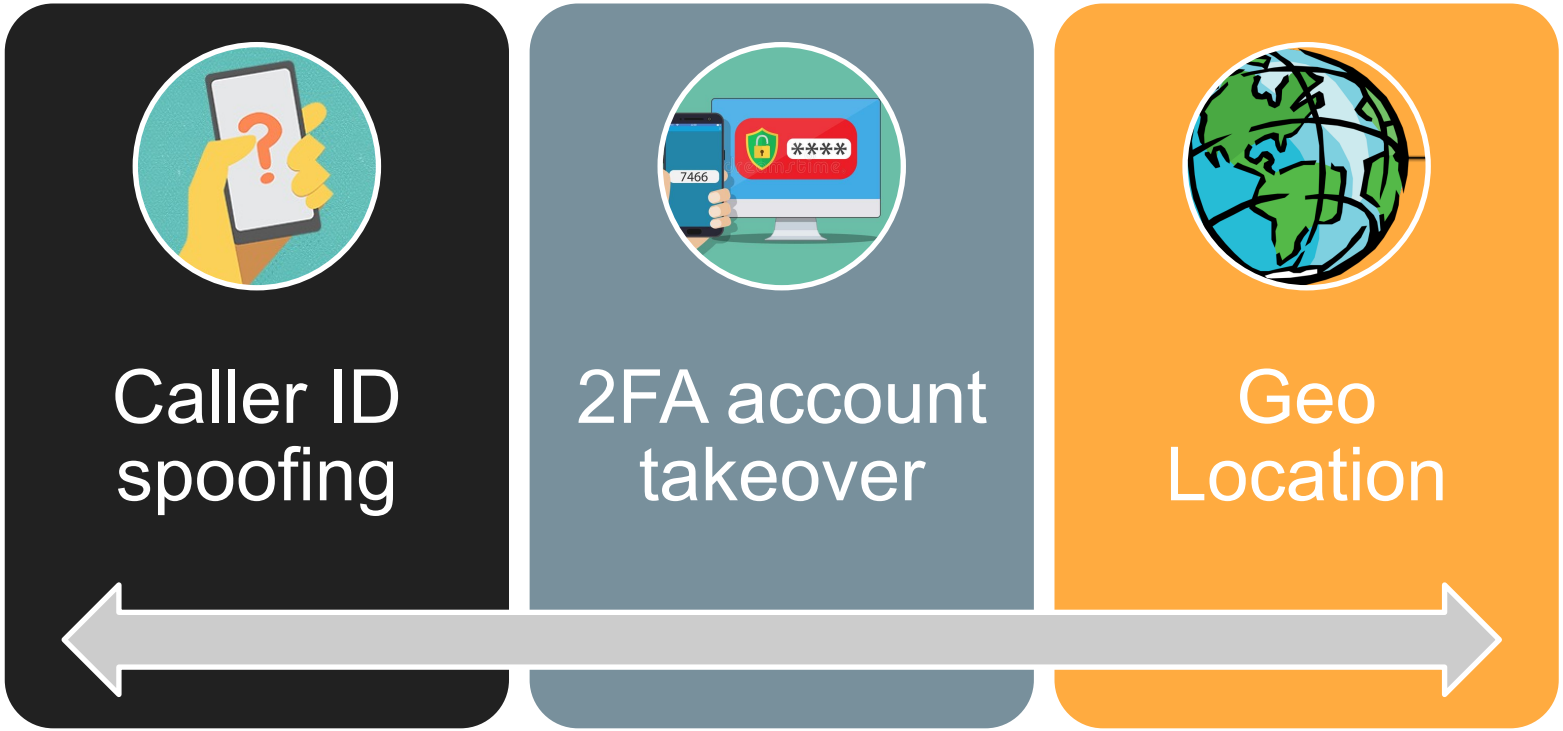


SS7: vulnerability by design

- 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

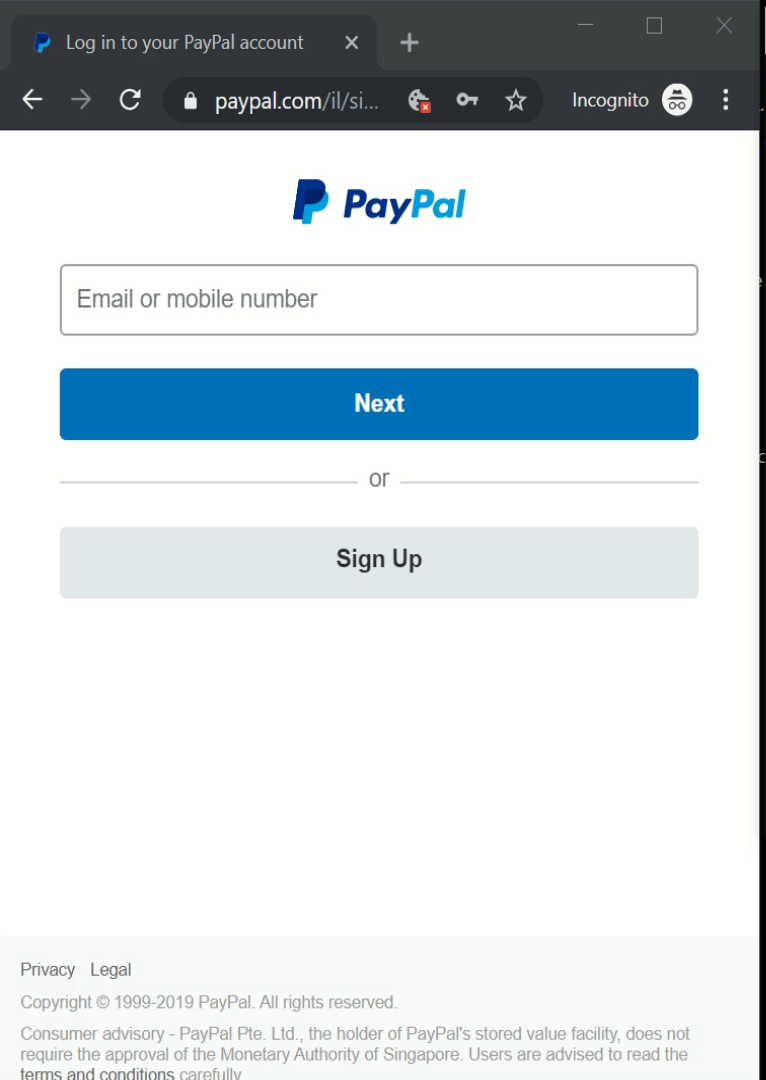


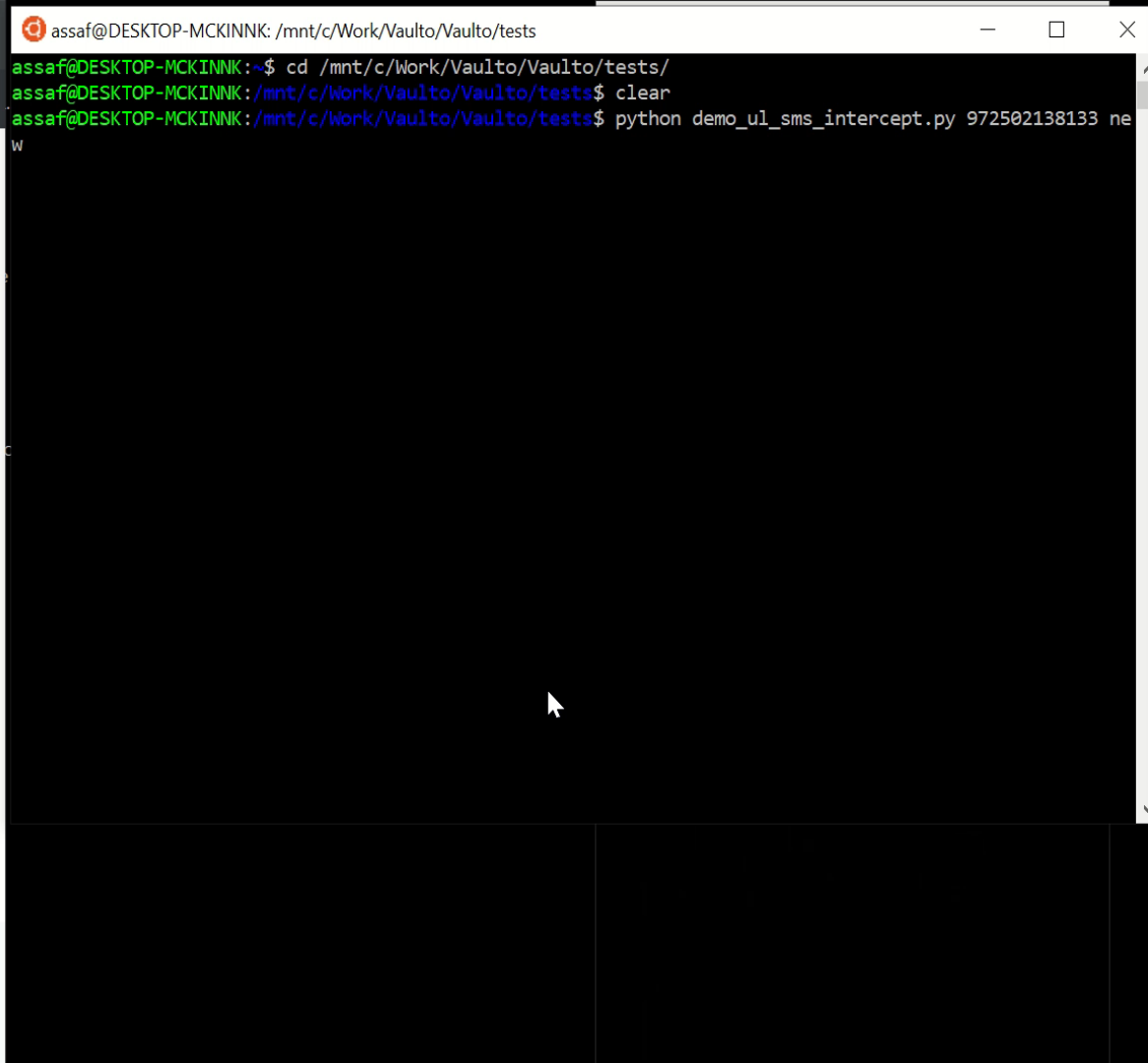
Major types of signaling attacks in the wild



2FA SMS interception

Example


Log in to your PayPal account
paypal.com/il/si...
Incognito
PayPal
Email or mobile number
Next
or
Sign Up
Privacy
Legal
Copyright © 1999-2019 PayPal. All rights reserved.
Consumer advisory - PayPal Pte. Ltd., the holder of PayPal's stored value facility, does not require the approval of the Monetary Authority of Singapore. Users are advised to read the terms and conditions carefully


assaf@DESKTOP-MCKINNK: /mnt/c/Work/Vaulto/Vaulto/tests
assaf@DESKTOP-MCKINNK:~$ cd /mnt/c/Work/Vaulto/Vaulto/tests/
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ clear
assaf@DESKTOP-MCKINNK:/mnt/c/Work/Vaulto/Vaulto/tests$ python demo_ul_sms_intercept.py 972502138133 new

Available Mitigation Measures

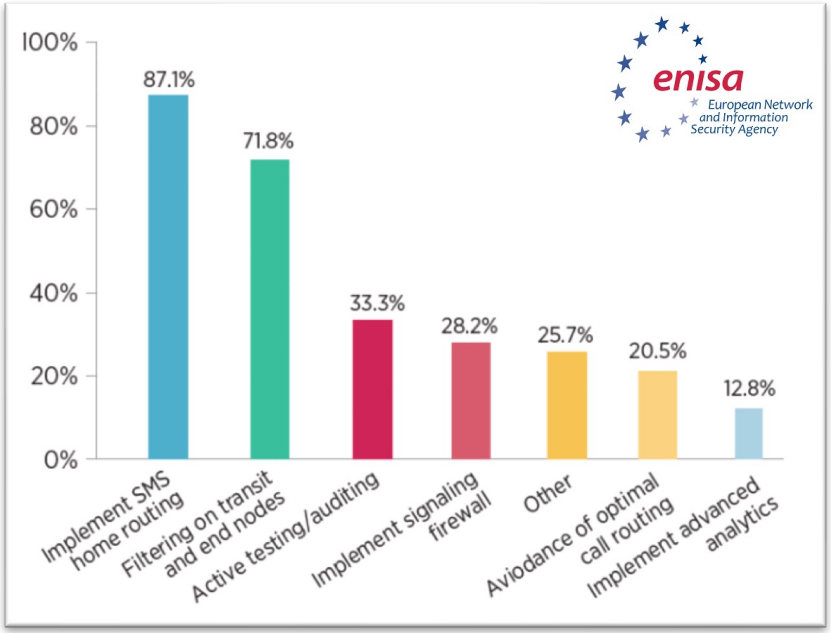
- Implementation of configuration recommendations

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

- Commercial signaling firewalls
  - Stateless vs. stateful
  - Threat intelligence

Limitations of available mitigation measures

- Implementation of configuration recommendations
  - Doesn’t solve attacks using legitimate signaling flows
  - Low adoption by operators
- Commercial signaling firewalls
  - Low adoption by operators
  - Threat intelligence depends on attack information sharing between operators



The solution

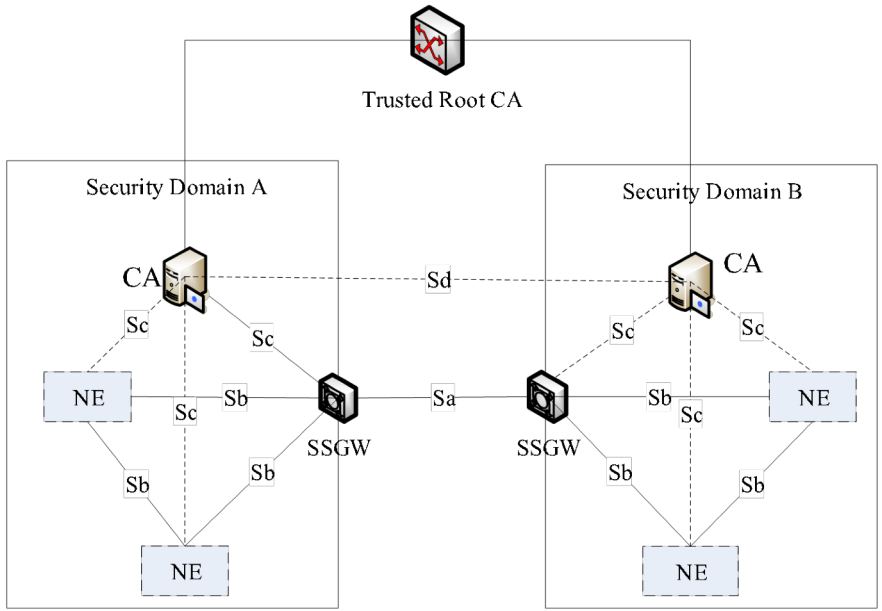
- Adding an integrity layer to signaling transactions to enable trustable communications
- Some example of applications:
  - Calling Line Identification (CLI) authentication
  - 2FA
  - Digital Financial Services (DFS)
  - And more…

But didn’t we already try that?

- TCAP-SEC was released in the early 2000’s but was never adopted
  - Did not specify the trust model
  - Used crypto that wasn’t “mainstream” (i.e. did not use PKI)
  - Did not specify any governance or policy regarding issuance of authentication keys

Current work in SG11

- ITU-T Q.3057 and ITU-T Q.Pro-Trust
  - Adds digital signature to SS7 signaling to authenticate the sender
  - Prevents hackers from impersonating legitimate network functions on the SS7 network
  - Enables operators to manage trust of other operators
  - Using TLS 1.3 as a reference trust model
- ITU-T Q.CIDA
  - Uses *Q.3057* and *Q.Pro-Trust* as infrastructure for CLI authentication
  - Uses authentication tokens to prevent CLI spoofing



But what about the trust model?

In Nov. 2021 SG11 and SG2 had a brainstorming session regarding this issue

The main takeaways from this session were:

Trust model

- We will need to build a hierarchy of trust, country/regional first, then global. where each local regulator will have to determine how to implement the certification depending on their local forms of identification and rules
- **Technically the digital certificates must be interoperable across domains** (SIP, SS7 and others).
- This trust chain and certification standard must account for the fact that numbering is no longer geographical and different authorities can govern the same numbering range
- **The trust anchor needs to be a globally trusted SDO**, preferably one already in charge of numbering and this anchor must interoperate with existing repositories (such as the ones in the US and Canada)

vetting/certification process

- **We will need to formulate a way to standardize these local/regional certification processes** in order to keep the bad actors out. This standardization process should involve as many counties as possible in order to improve its applicability on the global scale
- The certification process implemented in the US and Canada for STIR/SHAKEN is a good use case to learn from in order to standardize it on the global scale
- These certification process standardization must be connected to a largely accepted digital identity management frameworks for the operator plane and for the individual plane

US & Canada use case

FCC developed the STI (Secure Telephone Identity) framework, which is comprised from:

- STI-GA – Governance Authority
  - Managed by a board consisting of representatives from across the telecom industry
  - Defines the policies and procedures for which entities can acquire a digital certificate
  - Can revoke a service provider's certificate due to breach of trust
  - Selects the STI Policy Administrator
- STI-PA – Policy Administrator
  - Approves STI-CAs
  - Validates that service providers are authorized to obtain STI Certificates
  - Maintains a secure list of all authorized STI-CAs and Certificate Revocation List (CRL)
- STI-CA – Certification Authority
  - Issues STI Certificates to service providers

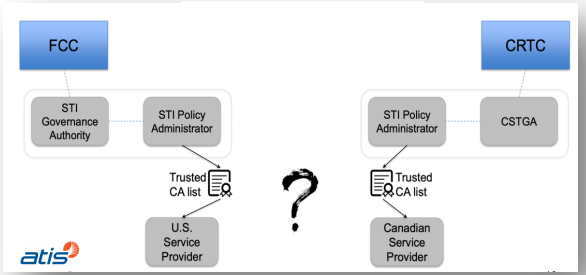
- GBSD
- Metaswitch
- NetNumber
- Neustar
- Sansay
- PeerhingHub
- TransNexus

STI Framework on the signaling level

- IETF STIR (RFC 8224-6) for adding authentication token to SIP headers
  - PKI based token (JWT encoded) – modeled after TLS
- Authentication is done cross-operator, which means:
  1. Only calls that cross between operators are signed
  2. Each cross-operator call is signed with the same operator certificate, i.e., the CLI itself is not signed, only the originating operator's identity is asserted
  3. A valid certificate indicates to other operators that the call is not a robocall nor is it spoofed
  4. Each operator is mandated by the STI-PA to verify internally that it does not provide service for robocalls and/or CLI spoofers
  5. If the STI-PA receives reports that robocalls of spoofed calls originate from an operator holding a valid certificate, it can petition the STI-GA to revoke the operator's certificate

Open issues in STI

- International interoperability



- Trust Anchor - according to NANC report
  - The STI framework will not “solve” illegal caller ID spoofing, but it is an enabler that can lay the groundwork for a variety of techniques to address the problem
  - Establishing the Call Authentication Trust Anchor, a secure certificate management infrastructure will provide the necessary building block for securing the call authentication

ITU-T Q.3057 & Q.Pro proposed trust model

- Each operator is assigned a digital certificate by the TSCA (the trust anchor)
- A provisional certificate is issued via API (machine verifiable)
  - The provisional certificate is valid for only 6 months
- A certificate is issued by TSCA after verifying the requestor's identity
  - The full certificate is valid for 2 years
- The TSCA can entrust a national/regional CA (Certification Authority) to issue the operator certificates
- Each operator holds its own CA which works in a hierarchical trust chain: operator → national/regional CA (if applicable) → TSCA
- Certificates are ITU-T X.509 (same as in TLS) which are interoperable with STIR
- The TSCA can revoke a rouge operator (bad actor) certificate, excluding them from the SS7 network

Next steps

- We will need to formulate a way to standardize these national/regional certification processes
- Standardize a governance policy to govern national/regional certification authorities, including certificate revocation
- To achieve true end-to-end authentication of caller identity the proposed framework needs to be connected to a largely accepted and adopted personal digital identity management framework
- Establishment of a global trust anchor which will aggregate a repository of approved CAs which can verify certificates (operator or personal)
- Standardize an IWF (Interworking Function) between ITU-T X.509 and RFC 8226

Open discussion

Thank you

Assaf.klinger@gmail.com

@AssafKlinger

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