Securing Telephone Networks: Toward a Collaborative Approach for Combating Fraudulent Communications Using Digital Certificates

Zimbabwe's Context

In the Absence of Mitigation

Senior citizens target of multiple financial scams

admin • Herald • January 12, 2024 • 0 Comments

1. **Free Wi-Fi**
2. **Public Wi-Fi**
3. **Free Mobile Apps**
4. **Free Online Tools**
5. **High Financial Services Penetration**

- Old iOS versions
- Old phones
- Ubiquitous–?Appearing everywhere, anytime
- launch of unlicensed financial services?
- SS7 Vulnerabilities

Current Cyber-related Crimes in Zimbabwe

Whatsapp Fraud

1. Obtain OTP
2. Install the account on another device
3. Restore contacts from online backup
4. Initiate conversations
5. Request for financial assistance

How do Scammers know one has been paid a pension?

DFS

Signalling System Number 7

I. Intercept Messages
II. Re-route calls
III. Location Tracking

BEC

1. **Impersonation of Supplier**
2. **Redirection**
3. **Change of banking details**

What can an individual do?

Avoid posting cell phone numbers on publicly available platforms or spaces(LinkedIn, Facebook, etc

I recommend receiving your OTP to a secure email address, as compared to SMS

Where features are available, make use of an Authenticator application

For your Recovery email, enforce primary device-based validation before the account can be accessed from an unauthorised device

General Cyber Security Hygience

DFS operator controls to mitigate SS7 risks

- Session time out
- Transaction limits for insecure channels
- User education
- Detecting and mitigating social engineering attacks with MT-USSD and interception of USSD
- Bidirectional OTP SMS flow

What can Telcos do in Simple English ?

1. Enforce policies to block any messages inconsistent with the characteristics of a subscriber on their home network,
2. Consumer awareness and education
3. Ensure that rogue BTS are not enrolled onto the network
4. Deploy inspection-sensitive firewalls to try to isolate illegitimate fake roaming traffic from actual roaming traffic
5. Explore embedding AI into establishing the practicality of a user's baseline locations and timestamps if they are possibly roaming without infringing privacy rights

What can Telcos do for Engineers?

Recommendations for MNO to mitigate SS7 Risks

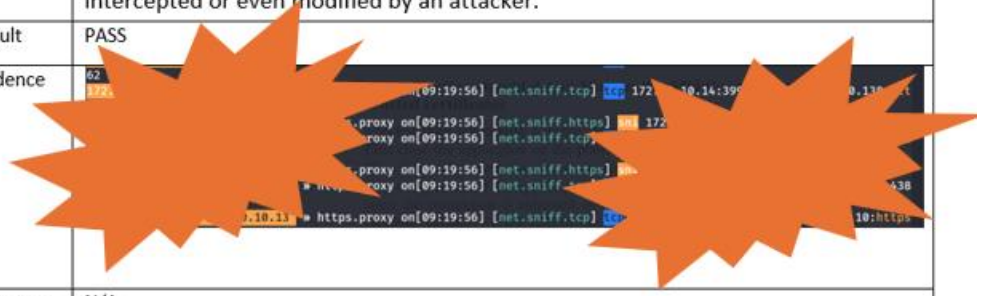
- Secure GSM ciphers for radio network traffic
- Session time out
- USSD PIN masking
- Secure and monitor core network traffic
- Limit access to traces and logs
- SMS filtering
- SMS home routing

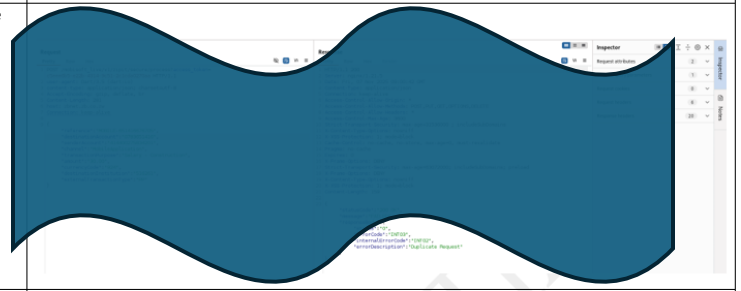
```
1 13:08:00.624000        1041                    8744

> 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-PhysSer
> 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
> 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.1
        v E.164 number (MSISDN): 27761485722
            Country Code: South Africa (Republic of) (27)
```

What is Zimbabwe doing?

- MOU between the Telecoms regulator and the Central Bank. A standing Committee convenes quarterly
- Joint guidelines that attempt to mitigate SS7 and DFS-associated risks
- Collaboration between the ITU and Telecom Regulator POTRAZ
- Advocacy at the highest level of Government
- Targeted awareness campaigns for the Elderly

	transferred over HTTP or other non-encrypted protocols, then it could easily be intercepted or even modified by an attacker.
Result	PASS
Evidence	
Recommendation	N/A

Test	Replaying a request (e.g. a money transfer) that was captured by a man-in-the-middle proxy should not result in the same request being executed twice. The risk is that an attacker intercepting a request for a money transfer could replay it to steal money from the victim.
Result	PASS
Evidence	
Recommendation	

Example of a DFS test done on a mobile application in Zimbabwe

- Over Ten Banking Apps have been tested in Zimbabwe,
- Recommendations extended to the banks for remediation
- All banks have submitted evidence of the remediation of time-bound plans to remediate

What is the ITU doing?

ITU-T Recommendations and Standards

ITU-T Study Group 11 leads signalling security work and has developed standards to strengthen SS7 and related protocols:

- **Q.3062 & Q.3063**: Procedures for interconnection between trusted network entities and authentication of calling line identification.
- **Q.3057**: Digital certificate-based mechanisms for caller ID authentication, even for legacy SS7 networks.
- Draft standards like **Q.TSCA** (certificate requirements for signalling trust) and **Q.DMSA** (detection and mitigation of signalling attacks)

Capacity Building

1. Assisting in the establishment of DFS Labs across the world
2. Training of trainers
3. Specialised skills training