عمانتل
Omantel

Voice Threats Management- Omantel’s Corporate Security experience

Abdullah Barwani
GM, Corporate Security

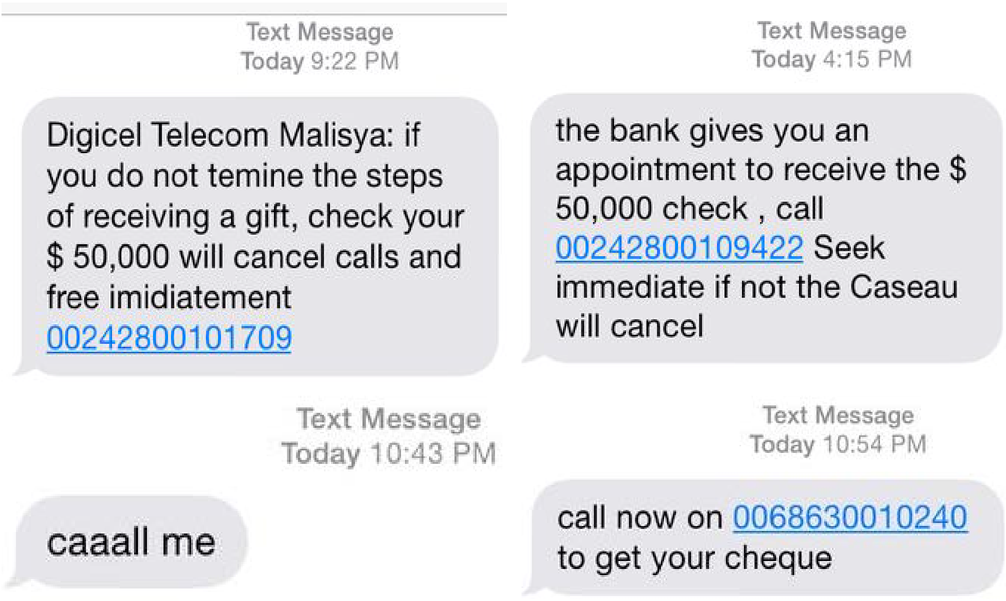
April 21, 2024

CONFIDENTIAL

Agenda

- Emerging telecom threats witnessed globally
- Why telecom security is important
- Voice specific threats
- How Omantel has implemented its voice protection
- Our learnings.

Some Telecom Threats & Scams Are Seen Commonly..



Text Message
Today 9:22 PM

Digicel Telecom Malisya: if you do not temine the steps of receiving a gift, check your $ 50,000 will cancel calls and free imidiatement 00242800101709

Text Message
Today 4:15 PM

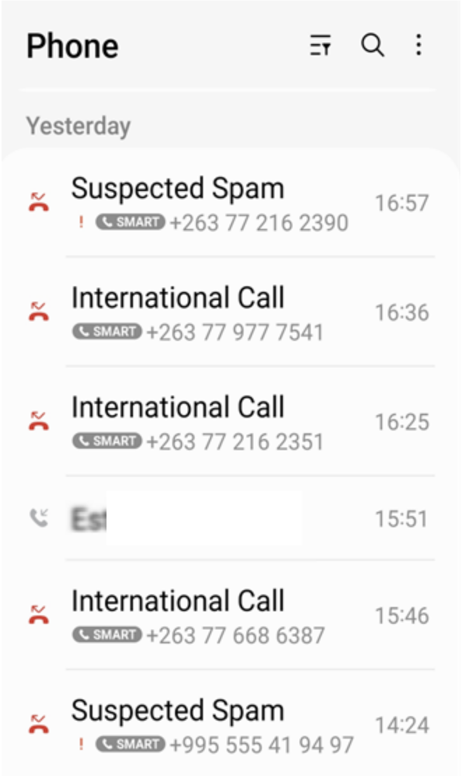
the bank gives you an appointment to receive the $ 50,000 check , call 00242800109422 Seek immediate if not the Caseau will cancel

Text Message
Today 10:43 PM

caaall me

Text Message
Today 10:54 PM

call now on 0068630010240 to get your cheque



Phone

Yesterday

Suspected Spam
! SMART +263 77 216 2390 16:57

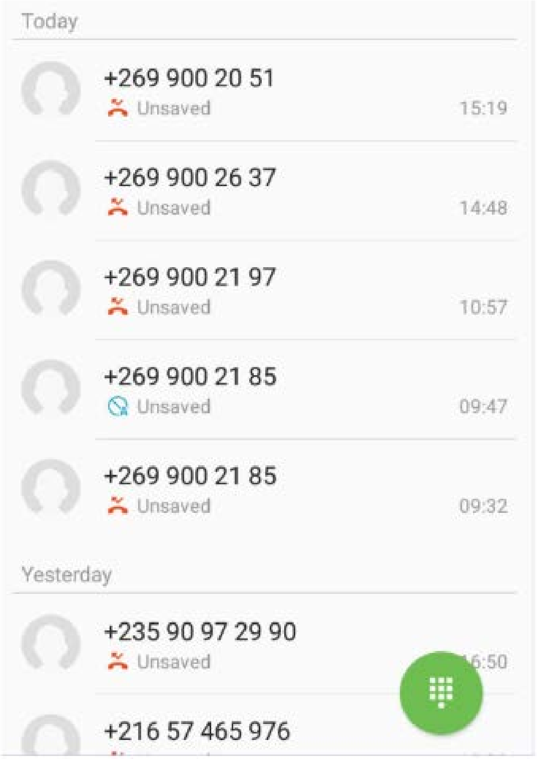
International Call
SMART +263 77 977 7541 16:36

International Call
SMART +263 77 216 2351 16:25

[redacted] 15:51

International Call
SMART +263 77 668 6387 15:46

Suspected Spam
! SMART +995 555 41 94 97 14:24



Today

+269 900 20 51
Unsaved 15:19

+269 900 26 37
Unsaved 14:48

+269 900 21 97
Unsaved 10:57

+269 900 21 85
Unsaved 09:47

+269 900 21 85
Unsaved 09:32

Yesterday

+235 90 97 29 90
Unsaved 16:50

+216 57 465 976

Nobody wants unwanted scam or spoofed calls. But, such scams are real

But We Often Come Across Headlines Which Highlight More Sophistication

REPORT TECH CYBERSECURITY

For $500, this site promises the power to track a phone and intercept its texts

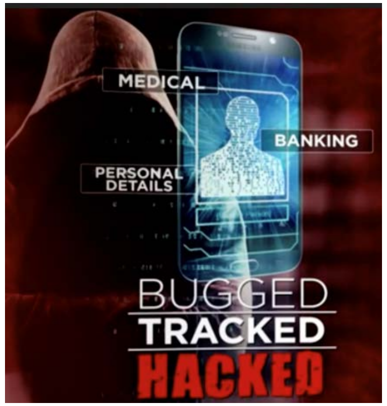
Paid access to a deeply insecure phone network

The Register®
Biting the hand that feeds IT

Security 34

After years of warnings, mobile network hackers exploit SS7 flaws to drain bank accounts

O2 confirms online thefts using stolen 2FA SMS codes

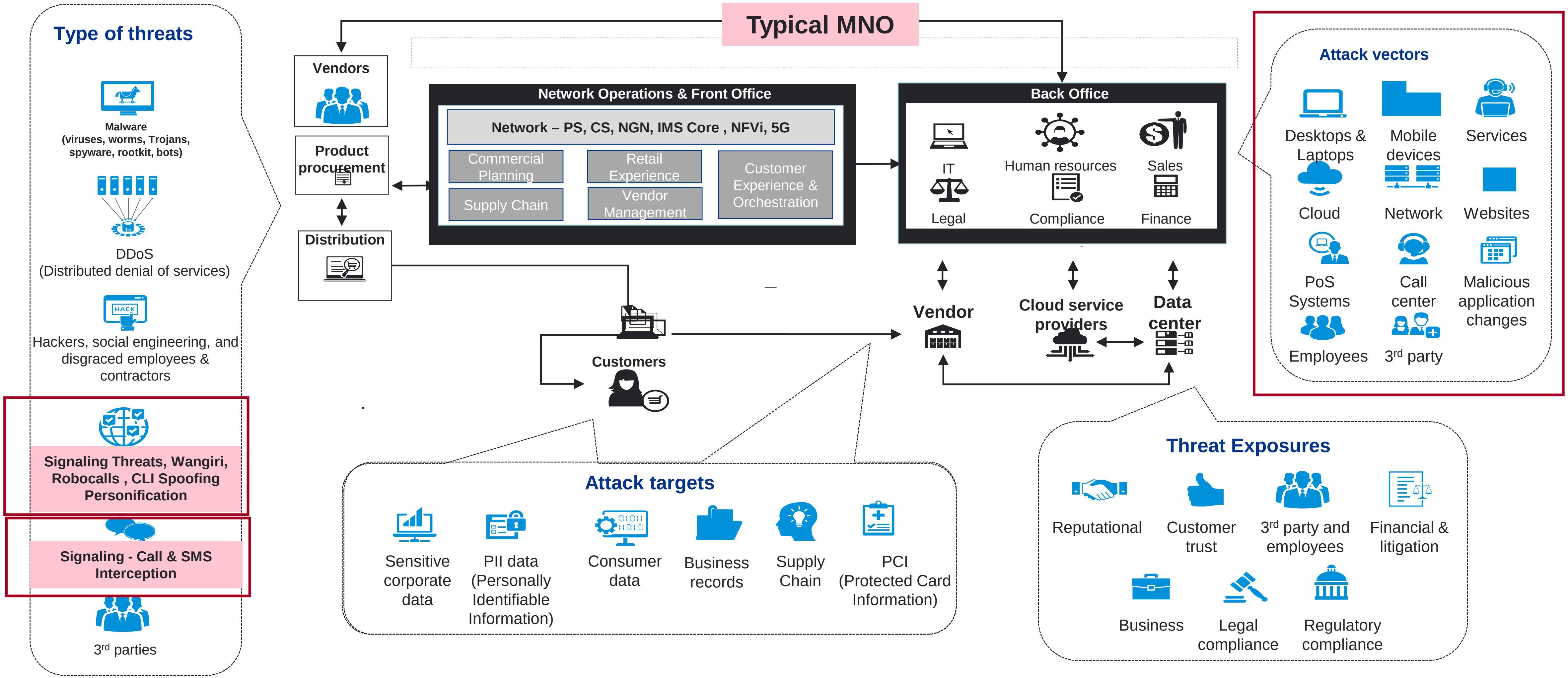


Security 24

White hats do an NSA, figure out LIVE PHONE TRACKING via protocol vuln

SS7 hole already used in Ukraine & Russia

Cyber Threats Have Very Wide Touchpoints In a MNO Ecosystem…



Type of threats

Malware
(viruses, worms, Trojans, spyware, rootkit, bots)

DDoS
(Distributed denial of services)

Hackers, social engineering, and disgraced employees & contractors

Signaling Threats, Wangiri, Robocalls , CLI Spoofing Personification

Signaling - Call & SMS Interception

3rd parties

Typical MNO

Vendors

Product procurement

Distribution

Network Operations & Front Office

Network – PS, CS, NGN, IMS Core , NFVi, 5G

Commercial Planning

Retail Experience

Customer Experience & Orchestration

Supply Chain

Vendor Management

Back Office

IT

Human resources

Sales

Legal

Compliance

Finance

Vendor

Cloud service providers

Data center

Customers

Attack vectors

Desktops & Laptops

Mobile devices

Services

Cloud

Network

Websites

PoS Systems

Call center

Malicious application changes

Employees

3rd party

Attack targets

Sensitive corporate data

PII data (Personally Identifiable Information)

Consumer data

Business records

Supply Chain

PCI (Protected Card Information)

Threat Exposures

Reputational

Customer trust

3rd party and employees

Financial & litigation

Business

Legal compliance

Regulatory compliance

Why These Threats Are challenging...

- Silent Data Interception & Data Privacy
- Hidden Call Monitoring & Call Interception
- Unauthorized Configuration Changes
- Revenue / Premium Number Frauds
- Ambiguous Loopholes In Network Configurations
- Hidden data manipulation or unauthorized access
- Undisclosed flaws in data storage and encryption
- Unnoticed security vulnerabilities

Why Telecom Security Is Important

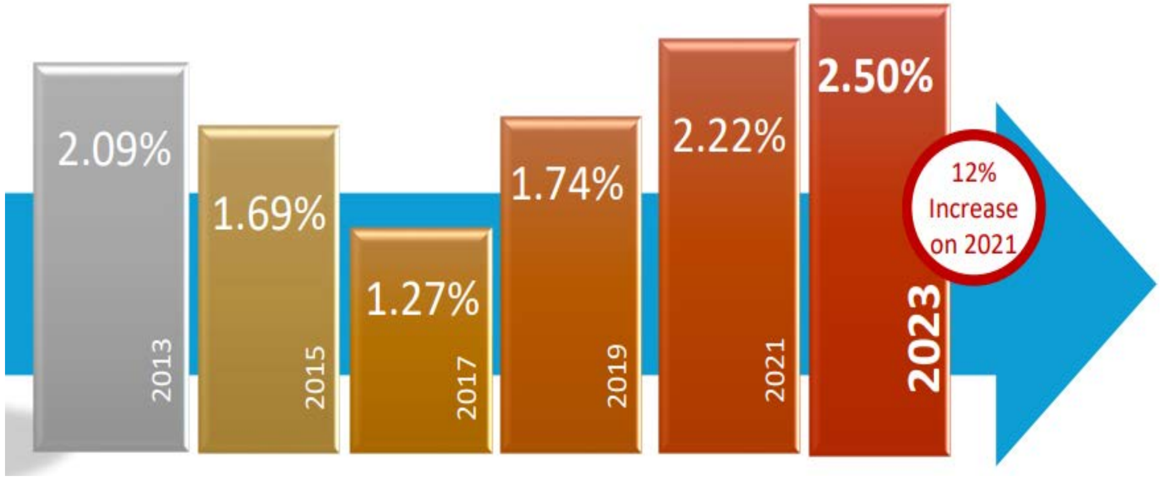
These Threats Have Wider Implications

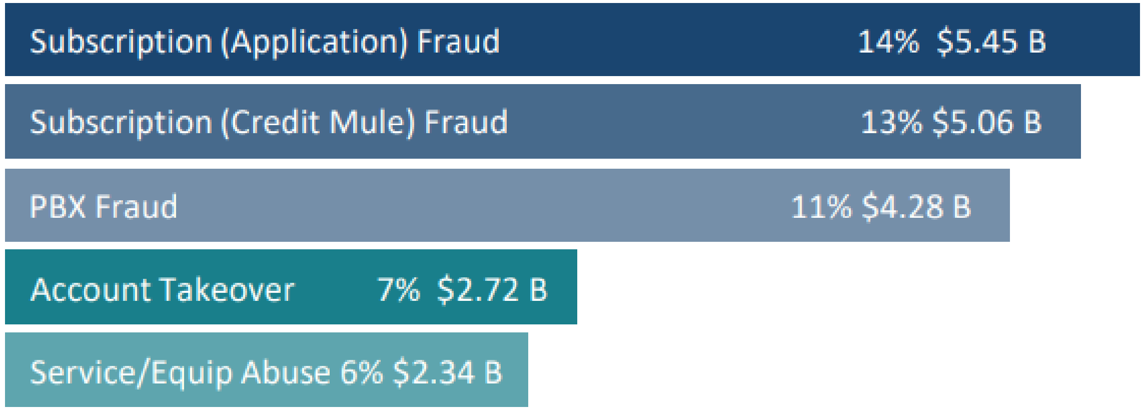
- Brand protection
- Regulation (or threat of)
- Churn (retention and acquisition)
- Fraud
- Fines
- Lost revenue (e.g. A2P SMS, sim swap/location checks)

Infact They Are More Common Than You May Know..

- 2023 Telecom revenue loss due to fraud is estimated to be 2.5% of revenues or $ 38.95 Billion Billion USD*.
- 2 of the top 3 frauds were not in the top 10 in 2019!

- Subscription fraud retains the top position for fraud types
- In the Middle East the emerging threat highlighted was Account takeover, particularly in the mobile sector where fraudsters are targeting customers ”Super Apps which are being provided in that market

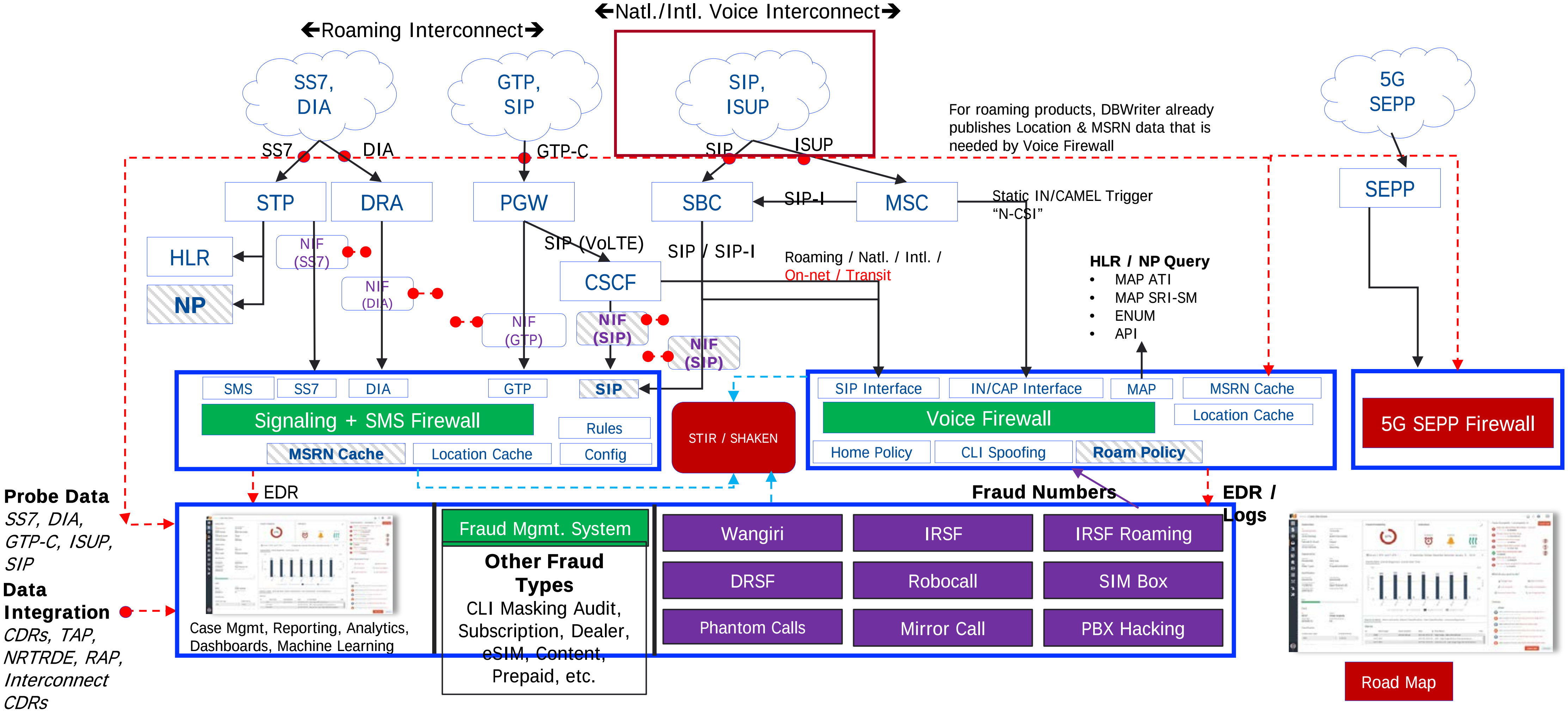




Source -Communications Fraud Control Association – Fraud Loss Survey Report 2023

Omantel’s experience Voice Threats Management

We Have Developed A Robust Architecture To Mitigate Such Threats..

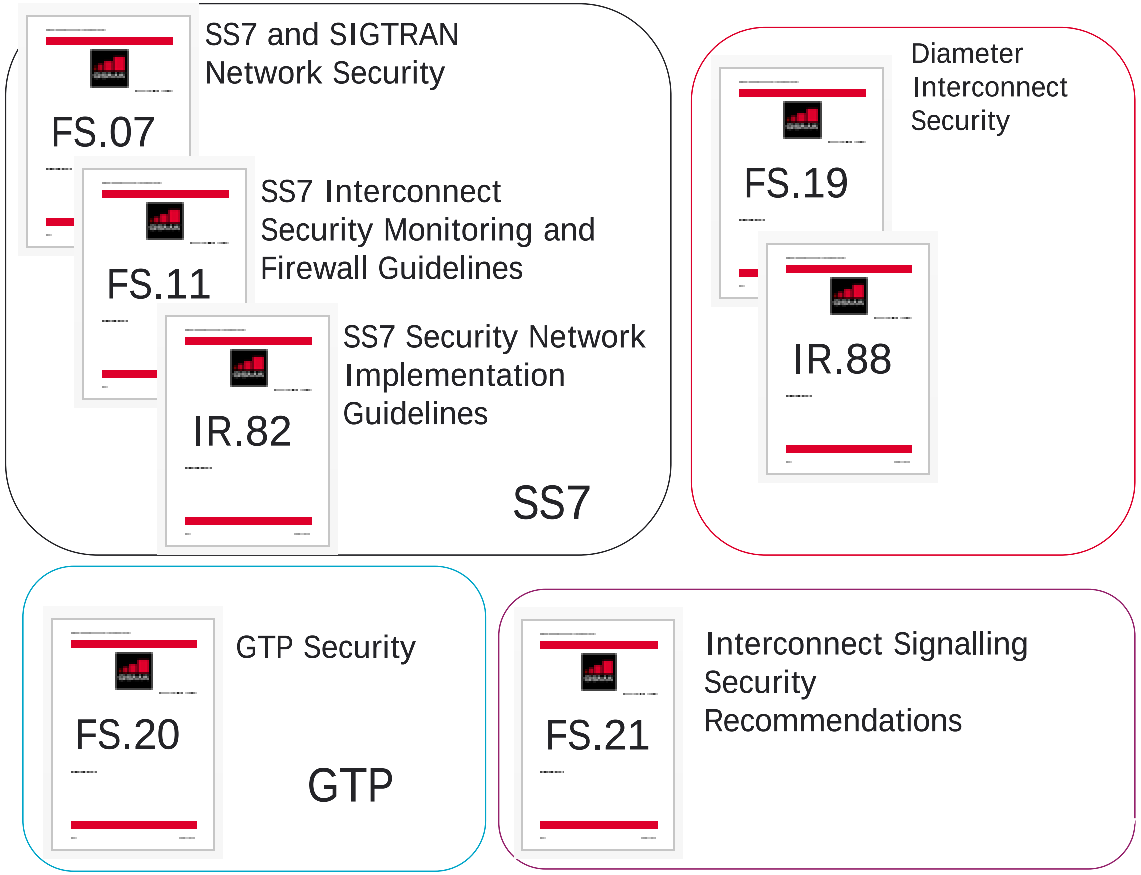


For roaming products, DBWriter already publishes Location & MSRN data that is needed by Voice Firewall

Our Approach Is Based On GSMA and FASG Recommendations

Ref	Doc Number	Title
1	GSMA PRD FS.07	SS7 and SIGTRAN Network Security
2	GSMA PRD FS.11	SS7 Interconnect Security Monitoring Guidelines
3	GSMA PRD IR.82	SS7 Security Network Implementation Guidelines
4	GSMA PRD FS.19	Diameter Interconnect Security
5	GSMA PRD FS.20	GPRS Tunnelling Protocol (GTP) Security
6	GSMA PRD SG.22	SMS Firewall Best Practices and Policies
7	GSMA PRD IR.70	SMS SS7 Fraud
8	GSMA PRD IR.71	SMS SS7 Fraud Prevention
9	GSMA PRD IR.77	Inter-operator IP Backbone Security Requirements for Service and Inter-operator IP Backbone Providers
10	GSMA PRD IR.88	LTE and EPC Roaming Guidelines

Ref	Doc Number	Title
1	FASG#6 Doc 009	Recommended Signaling Firewall Rules and Data Sharing presentation to FASG#6
2	RIFS42_03	RIFS42_03 Interconnect Signalling Security RecommendationsDRAFTv0_10


FS.07
SS7 and SIGTRAN Network Security
FS.11
SS7 Interconnect Security Monitoring and Firewall Guidelines
IR.82
SS7 Security Network Implementation Guidelines
SS7
FS.19
Diameter Interconnect Security
IR.88
FS.20
GTP Security
GTP
FS.21
Interconnect Signalling Security Recommendations

Our Deployed Use Cases

Our Key Use Cases

Wangiri Fraud

- Fraudulent calls where the phone rings just once and disconnects, aiming to trick users into calling back at a premium rate.
- **Impact:** Loss of revenue for Omantel, customer frustration. Criminals:” can use Wangiri calls to lead to premium rate numbers, generating revenue for themselves through return calls.
- **Solution:** Automated AI-based call pattern analysis for real-time detection and blocking with minimal impact on legitimate calls

CLI Spoofing

- Calls appearing to come from a familiar number (e.g., bank) to steal personal information.
- **Impact**: Identity theft, financial loss for customers. Criminals can spoof the caller ID to impersonate trusted sources (e.g., banks, authorities) to trick victims into revealing personal information or financial details.
- **Solution**: Utilize HLR, check real time location of originated call. If call is impersonating as originated from inside oman but real location is outside Oman, then block the call

Blank/Invalid Caller ID

- Calls with missing or invalid caller ID information.
- **Impact**: Difficulty identifying call origin, potential spam.
- **Solution**: Rules to block calls matching specific criteria, including missing valid CLI. Omantel can manage these settings.

Mirror Calls

- Calls where the incoming number exactly matches the outgoing number, often used for call forwarding scams.
- **Impact**: Potential for incurring unwanted charges.
- **Solution**: Rules to block calls with matching A and B numbers. Omantel can manage these settings.

Our Key Use Cases

Subset Calls

- Calls where the incoming number partially matches the outgoing number, used to bypass call filtering.
- **Impact**: Difficulty identifying scam calls.
- **Solution**: Firewall rules to block calls with partial A and B number matches. Omantel can manage these settings.

MSRN Check

- Verification of Mobile Station Roaming Number (MSRN) against various data sources to identify potential fraud.
- **Impact**: Prevents fraudulent calls disguised as roaming subscribers.
- **Solution**: Check if MSRN has been allocated to any subscriber within last 30 seconds, if yes, allow else block

Phantom Calls

- Calls with missing or invalid CLI information, similar to Blank Caller ID but with additional blocking rules.
- **Impact**: Difficulty identifying call origin, potential spam.
- **Solution**: Firewall rules to block calls matching specific criteria, including missing valid CLI. Omantel can manage these settings

IRSF Calls

- International Revenue Share Fraud (IRSF) involves diverting international calls to local terminations for profit.
- **Impact**: Loss of revenue for Omantel.
- **Solution**: AI-based call pattern analysis for automated detection and blocking with minimal impact on legitimate calls. Check performed by FMS

Our Key Use Cases

Number Length Check

- Blocking calls with invalid phone number lengths.
- **Impact**: Prevents unexpected call attempts.
- **Solution**: Rules to block calls with invalid number lengths after checking incoming call number length against published number length information by the operator. Check performed through a query to reference database

Deny / DND / Allow

- Ability to set firewall rules to unconditionally block or allow calls based on specific criteria.
- Impact: Provides granular control over call filtering.
- Solution: Rules with allow/deny options based on defined criteria. Omantel can manage these settings.

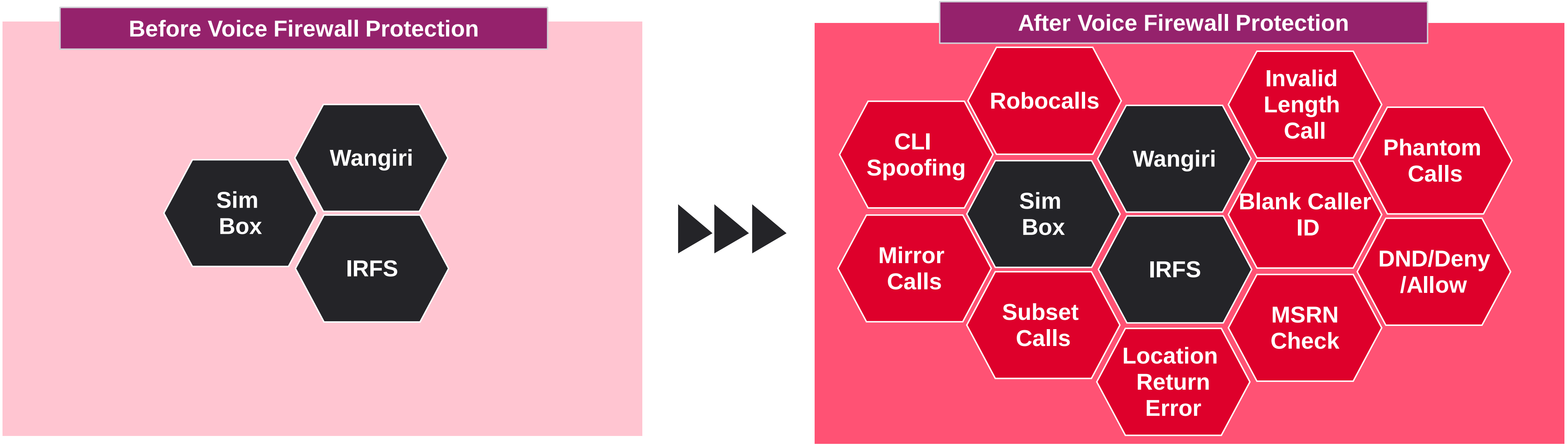
SIM Box Fraud

- Fraudsters use SIM boxes to terminate international calls as local traffic for cheaper rates.
- **Impact**: Loss of revenue for Omantel.
- **Solution**: Logic in FMS to detect SIM box fraud. FMS passes feed to Voice firewall which starts blocking the number in real time

Spam / Robocalls

- Automated spam calls used for advertising or phishing scams.
- **Impact**: Customer annoyance, potential scams.
- **Solution**: Real-time call pattern analysis for automated detection and blocking with minimal impact on legitimate calls

How Voice Firewall Changed The Game



- Only 3 use cases supported through **manual blocking** based on **FMS input**
- Major **spoof cases undetected**, leading to revenue loss
- **Operational overhead** due to multiple team involvement in blocking
- Blocking implemented in multiple platforms with **significant time delays**

- **13 use cases supported** –
  - 4 through manual blocking via FMS feed
  - **9 automatically in real time**
- **All major spoof cases detected**, leading to revenue savings
- **Simplified operational process** – Increased operational efficiency
- **Centralized real-time blocking and control**
- **In process to add more cases**

And Oman Is No Exception

1.29 Mn

Voice Threats Calls Blocked by Voice Firewall
Jan – Mar'24

383K

Calls Were CLI Spoofed or Callers Location Could Not Be Assessed
Jan – Mar'24

553K

Wangiri Calls Blocked
Jan – Mar'24

13

Use Cases Implemented

**Interceptions by Omantel Only*

Our Learnings

And What We Learned/Recommendations..

Telecom Security is business critical

Solutions must support a multi-operator environment and comply with regulatory requirements

Many solutions are dynamic and continues to evolve. Its critical to look beyond traditional solutions

Implement industry-standard security practices recommended by organizations like 3GPP (3rd Generation Partnership Project) and GSMA (Global System for Mobile Communications Association) to enhance network security further

Perform at least an annual independent Audit

Thank You