Cybersecurity Challenges in Telecom

Salem Itani

Telecom Expert

INTRODUCTION

Cybercriminals excessively challenge the Telecom Networks, they can steal confidential data or insert malware on specific downstream customer networks, or conduct a DDoS or other broad-based attacks.

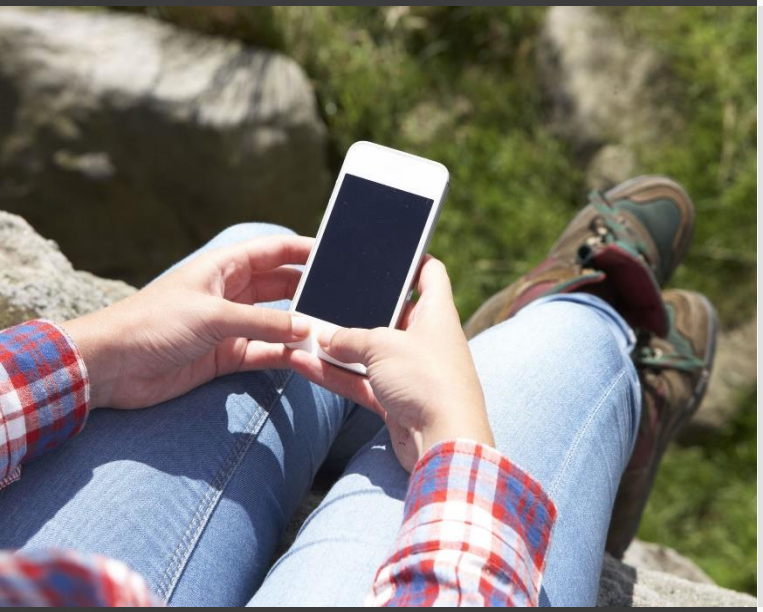
The scope, variety, and complexity of current cybersecurity threats on Telecom networks are increasing exponentially. The GSMA predict that the threat to industry will continue increasing over time.

In 2018, 43% of telco companies were victimized by DNS-based malware and 81% took more than 3 days to apply a critical security patch for resolution.

Cybersecurity threats are more challenging with the emerging technologies such as IoT, 5G, and NFV…

Cybersecurity Ventures predicts cybercrime damages will cost the world $6 trillion annually by 2021.

Cyber attacks on smartphones



More smartphones >>> more phishing attacks >>> more data breaches

4.6 m
Subscriptions in Lebanon
in 2018

86%
Using Smartphones
Highest in the Region

200M
Cyber attacks in 2018
.....and growing

37%
Increase in Phishing Attacks 1st 3 Months of 2020
and growing

Main Cyber Threats in Telecom

SS7 and Diameter Signaling Threats

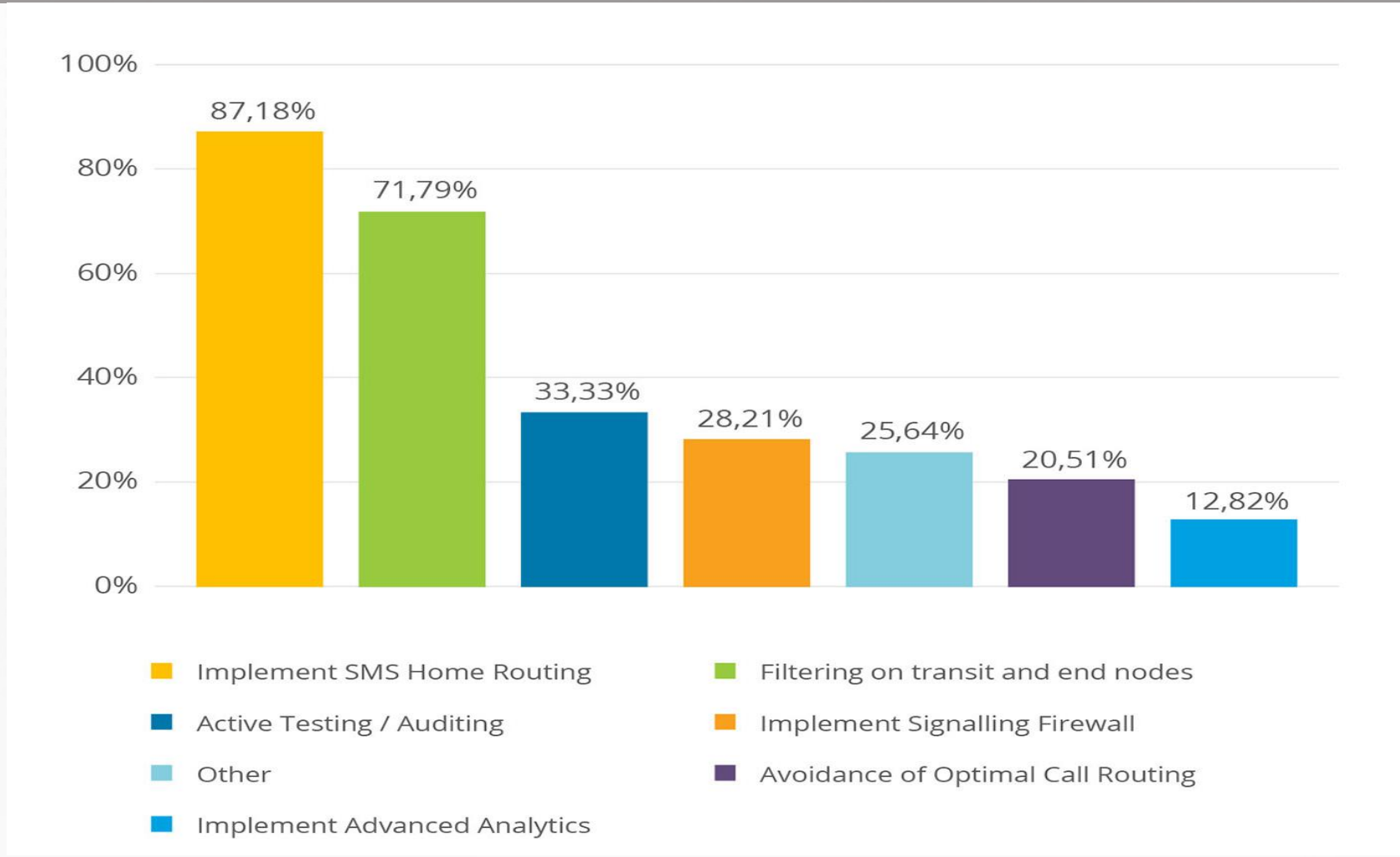
A number of core telecommunication services are still powered by weak protocols such as SS7 (Signaling System No. 7) or Diameter.

SS7 protocol, in particular, has become one of the central cyber threats to the Telecom sector since hackers can easily intercept its authentication process.

Implementing better signaling controls is proving to be a challenge for most telecoms due to the following:

- Overall complexity
- Privacy concerns
- Global title use
- Network configurations
- Traffic reliability

Used security measures to mitigate SS7 attacks



Main Cyber Threats in Telecom

SIP Hacking

Session Initiation Protocol (SIP), used in most voice-over-IP (VoIP) communications, is another main target for cybercriminals.

The common SIP cybersecurity threats are:

- SIP trunk hacking
- SIP toll fraud
- Eavesdropping
- Caller ID spoofing

Protection methods against SIP Hacking

Best Practices for Protecting SIP Signaling:

- Enforce strong encryption over the Transport Layer Security (TLS) and Real-Time Protocol (RTP) to protect all data transmissions.
- Implement anti-spoofing for SIP messages. Ensure proper mechanisms for challenging messages and authenticating SIP clients.
- Maintain strong Session Border Controller (SBC) controls in order to perform deep packet inspection of all SIP messages and prevent unauthorized SIP traffic.

Main Cyber Threats in Telecom

DNS Attacks

DNS attacks still remain the major pain for Telecom companies.

In 2017, one attack cost a telecom operator $622,100. In 2018, the figure rose by 42% and reached $886,560.

Telecom providers have the highest volume (30%) of sensitive customer information stolen through DNS attacks when compared to healthcare, banking, education, and public services sectors.

In general, 43% of telecom companies were victims of DNS-based malware and 81% needed 3+ days to apply a critical security patch.

DNS Attack Preventions

DNS Attack Prevention Best Practices:

- Implement real-time analytics for DNS transactions and build up a behavioral threat detection suite, capable of detecting both known and emerging cyber threats and protect against data theft/leaks.

- Enhance the firewalls with ML-driven response policies on traffic to suspicious hostnames.

- Implement query monitoring and logging for all suspicious endpoints

Main Cyber Threats in Telecom

DDoS (distributed denial of service) Attacks

Telecommunications sector faces this type of attack more than any other industry.

65% of the global DDoS attacks in year 2018 were aimed at telecom service providers and the figure still remains high in 2020.

The biggest issue with DDoS attacks for telcos is that a large-scale attack could create a domino effect.

A telecom network overload would likely affect a customer who is connected through the infrastructure transporting the attack.

DDoS Attack Protection Methods

Telcos Protection Against DDoS Attacks:

Set up robust Access Control Lists (ACL) – this is the first line of defense. However, the ACL has a scaling issue. An increase of ACLs, built to resist a large-scale attacks, can have a major performance impact on routers' hardware and software.

Implement Black Hole Scrubbing – In this technique, the traffic is redirected to a different physical interface – a scrubbing center – that can filter the good traffic from the malicious one. Notably, multiple vendors offer such solution…

Real-Time DDoS Monitoring is today a must – This is the best tool and nowadays powered with ML functionality, thus the detection accuracy progressively increases over time.

RECOMMENDATIONS

Protection of telecom networks against the cybersecurity threats is a must

Need to switch from reactive to proactive security approaches by relying on extensive online monitoring with predictive capabilities, powered by advanced analytics and AI

Conduct proper risk assessments for current systems, decentralize and automate the core security requirements with appropriate tools and run deeper assessments for emerging technologies such as IoT, 5G, and NFV…

Finally, need to increase awareness, educate telco employees and invest in suitable technology solutions

Cybersecurity Challenges in Telecom

THANK YOU!

Salem Itani

Telecom Expert