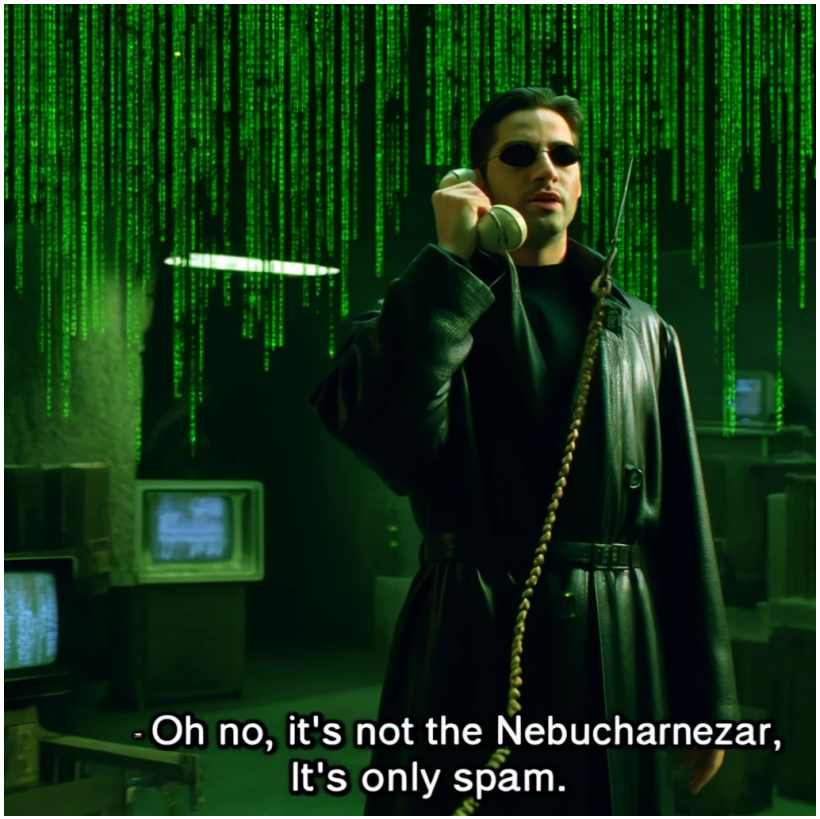
Evaluating Technical Countermeasures for Telecom Spam and Scams in the AI Era

Marcello Pietri, Marco Mamei, Michele Colajanni

DIPI Lab
DIstributed & Pervasive Intelligence Laboratory

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

"Meanwhile, as I was reading the title, some of you were receiving a few... unwanted calls."



Don't answer your phone. That's it. That's the answer.

James Martin/CNET

Thank you for your attention...

Topics

- What economic impact do spam/scam calls have?
- Why do spam/scam calls persist in 2024?
- What methods are used for spam/scam calls today?

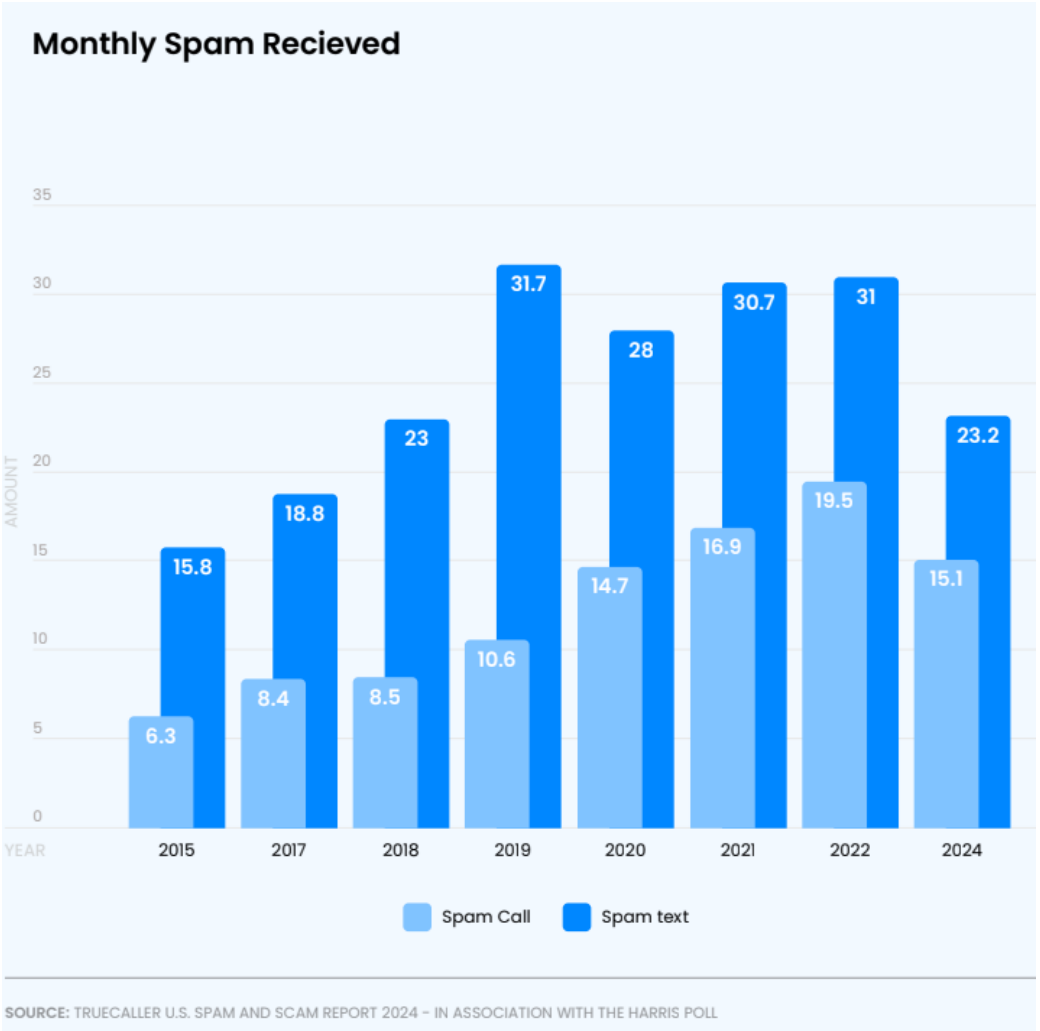
Topics

- How can we reduce spam/scam calls?
- How are spam/scam calls regulated in different countries?
- What role do governments play in combating spam/scam calls?

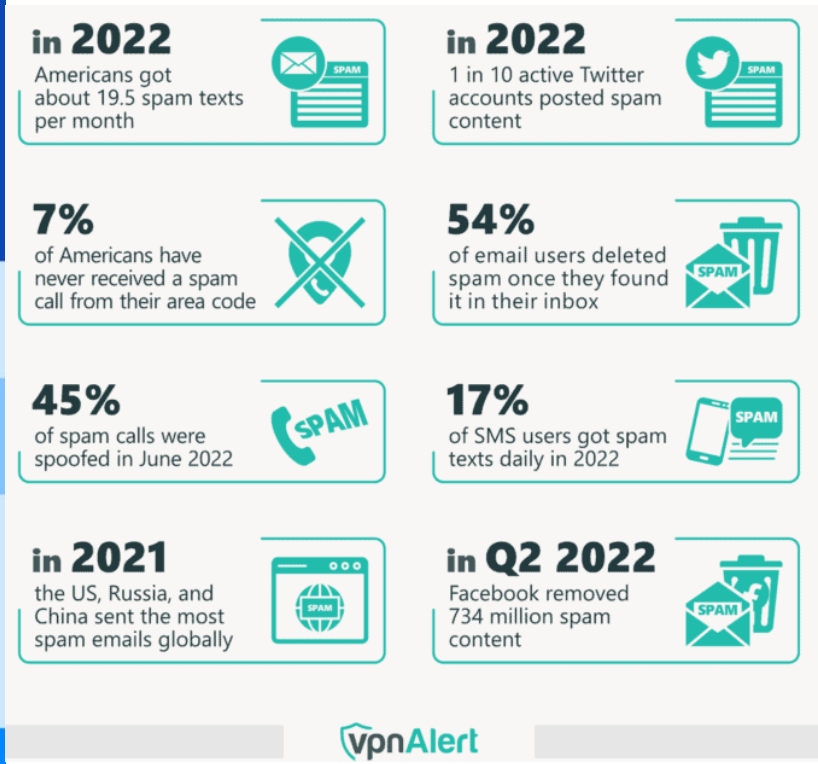
- What economic impact do spam/scam calls have?

https://drive.google.com/file/d/1M0J0wO6YqxDzsOizfal-AH_vI8dsyojb/view

- What economic impact do spam/scam calls have?

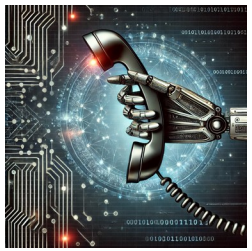


- What economic impact do spam/scam calls have?



- Why do spam/scam calls persist in 2024?

1) **Profitability**
Scammers still find financial success, exploiting vulnerable individuals.



2) **Technology** advancements
Automated robocall systems make it easy and inexpensive to send mass calls… (+AI!)

- Why do spam/scam calls persist in 2024?

3) **Lack of global regulations**

While some countries have anti-spam laws, enforcement and international coordination remain weak.

4) **Spoofing** technology

Scammers easily disguise their **caller IDs**, making detection harder.

- Why do spam/scam calls persist in 2024?

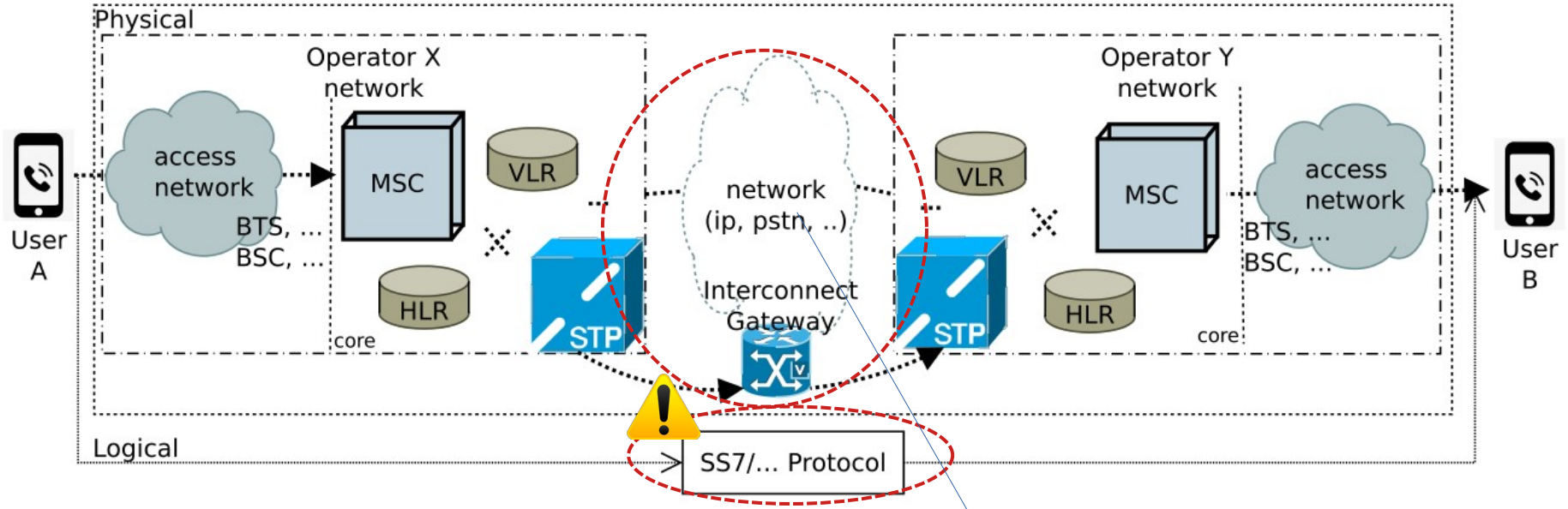


Fig. 2: Example of Communication schema interconnecting two users with different operators

Public Switched Telecom Network

- Why do spam/scam calls persist in 2024?

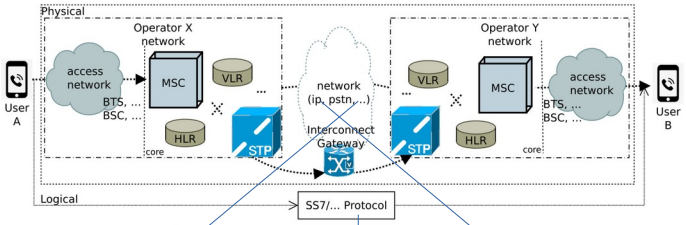


Fig. 2: Example of Communication schema interconnecting two users with different operators

PSTN

SS7 over IP

OSI Model

SS7 Protocol Stack

SIGTRAN Protocol Stack

1 Physical
2 Data Link
3 Network
4 Transport
5 Session
6 Presentation
7 Application

MTP Level 1
Physical, Electrical, and Functional characteristics

MTP Level 2
Error correction, Flow control, and Sequence validation

MTP Level 3
Message Handling, Signal Routing, and Congestion control

SCCP
Addressing, Routing, and Error correction beyond MTP Level 3

TCAP

ASE ... OMAP

ISDN user part (ISUP/ BICC/ TUP)

MTP

NSP

Level 4

SCTP

M3UA

M2PA

MTP3

SUA

SCCP

TCAP

ASE ... OMAP

ISDN user part (ISUP/ BICC/ TUP)

Transaction

Circuit

IAM (Initial Address Message) & SAM (Subsequent Address Message) ----- Sender & Receiver number

Fig. 3: Signaling System No. 7 (SS7) and SIGTRAN protocol stack

- Why do spam/scam calls persist in 2024?

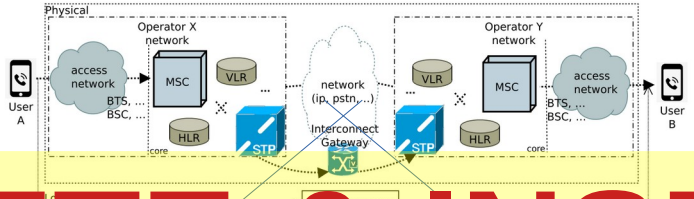
RFC: 3788

The SIGTRAN protocols **assume** that messages are secured by using either IPsec or TLS

3. Security in Telephony Networks

The security in telephony networks is mainly based on the closed network principle. [...] SS7 protocol stack in the core network. As SS7 networks are often physically remote and/or inaccessible to the user, **it is assumed that they are protected from malicious users**. Equipment is often **under lock and key.** At network boundaries between SS7 networks, packet filtering is sometimes used. End-users are not directly connected to SS7 networks. The access protocols are used for end-user signaling. End-user signaling protocols are translated to SS7 based protocols by telephone switches run by network operators. Regulatory Authorities often require SS7 switches with connections to different SS7 switches to be conformant to national and/or international test specifications. **There are no standardized ways of using encryption technologies for providing confidentiality or using technologies for authentication.** This description applies to telephony networks operated by a single operator, and also to **multiple telephony networks being connected and operated by different operators**.

- Why do spam/scam calls persist in 2024?



PSTN

SS7 over IP

OBSOLETE & INSECURE PROTOCOLS

Lacks built-in encryption and authentication mechanisms, making it vulnerable to interception, spoofing, and fraud.

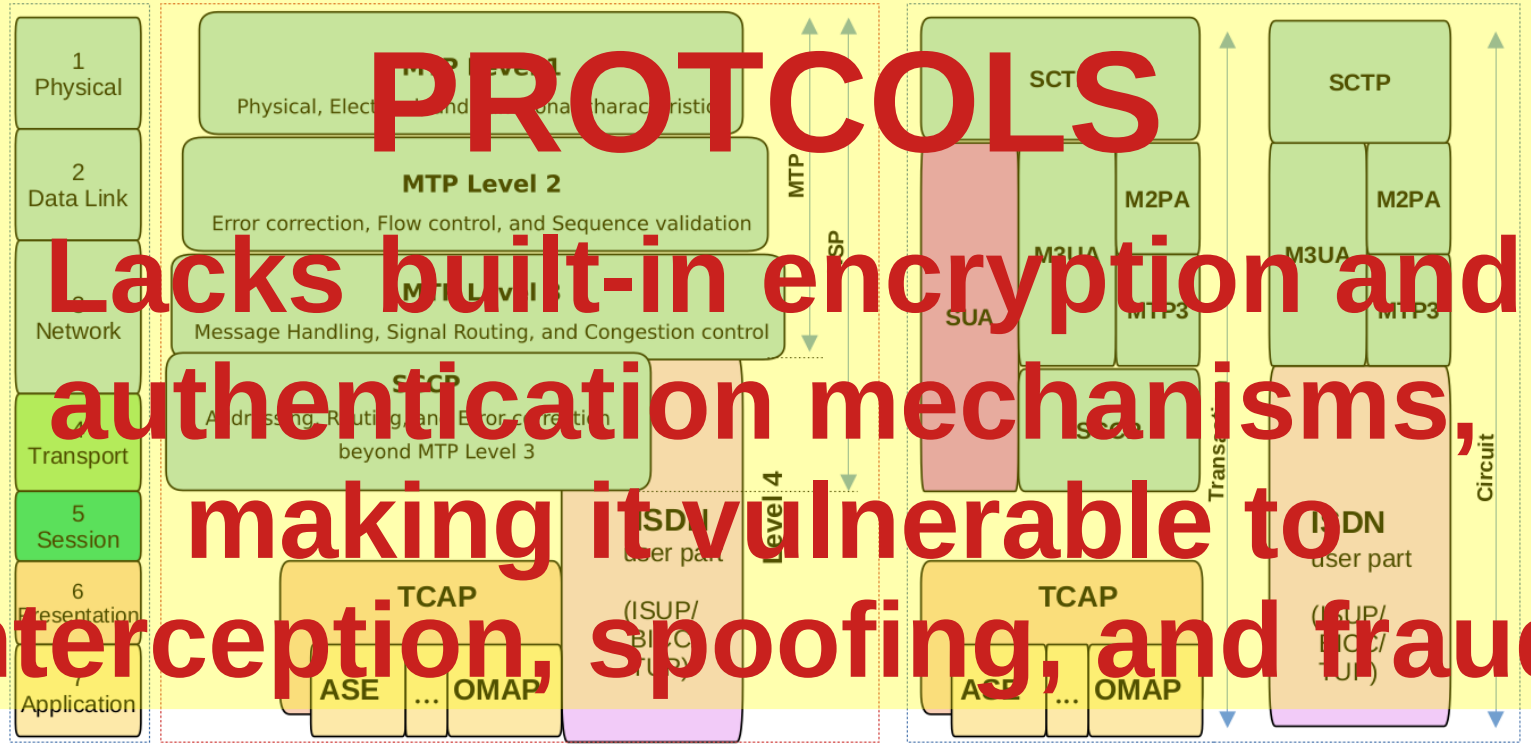


Fig. 3: Signaling System No. 7 (SS7) and SIGTRAN protocol stack

- Why do spam/scam calls persist in 2024?

Diameter is a more secure and scalable protocol than SS7, designed for modern IP-based networks like **4G and 5G**, with built-in encryption, handling authentication, authorization, and accounting (AAA) in next-generation mobile networks

• Why do spam/scam calls persist in 2024?

SIP:

- Widely used for VoIP and multimedia; requires TLS/SRTP for secure signaling.
- Operates in IP networks, more flexible than SS7, but depends on external layers for security.

H.323:

- Designed for voice/video over IP, supports H.235 encryption but more complex than SIP.
- More secure than SS7 with encryption but less flexible and secure than Diameter.

• Why do spam/scam calls persist in 2024?

SS7 is still used due to its long-established role in traditional telephony and its robustness in handling carrier-to-carrier signaling.

Legacy Interoperability: Many older telecom systems and networks are built on SS7. Replacing SS7 entirely would require significant infrastructure changes (and costs).

International Roaming: SS7 is integral for global roaming, **especially in 2G/3G networks**, where i.e. SIP does not provide the same seamless compatibility.

Circuit-Switched Networks: SS7 is designed for circuit-switched networks, while SIP operates over packet-switched networks. **Some regions and carriers still rely on older infrastructure.**

- Why do spam/scam calls persist in 2024?

=

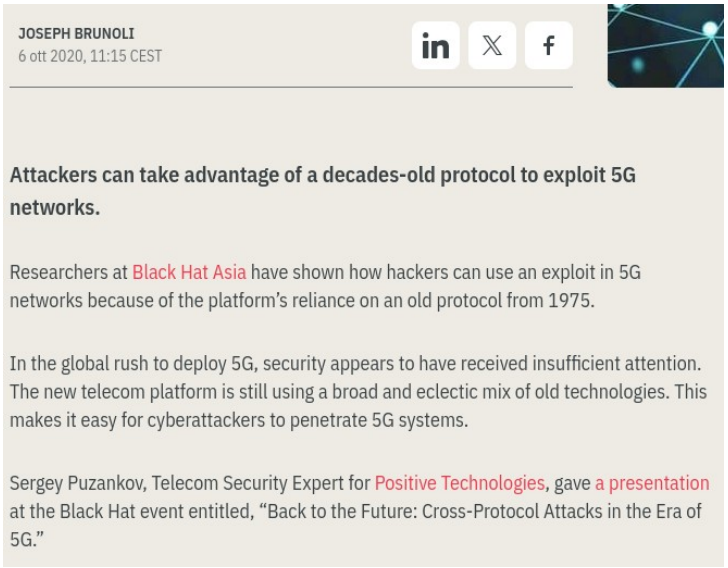
The transition is gradual and slow because of the need to maintain backward compatibility with existing systems.

Moreover, the costs can be significant!

Overview

Communications providers in the UK are replacing the technology they use to provide fixed telephone networks (landlines). For most customers, the upgrade is expected to be complete by January 2027.

https://www.gov.uk/guidance/uk-transition-from-analogue-to-digital-landlines



JOSEPH BRUNOLI
6 ott 2020, 11:15 CEST

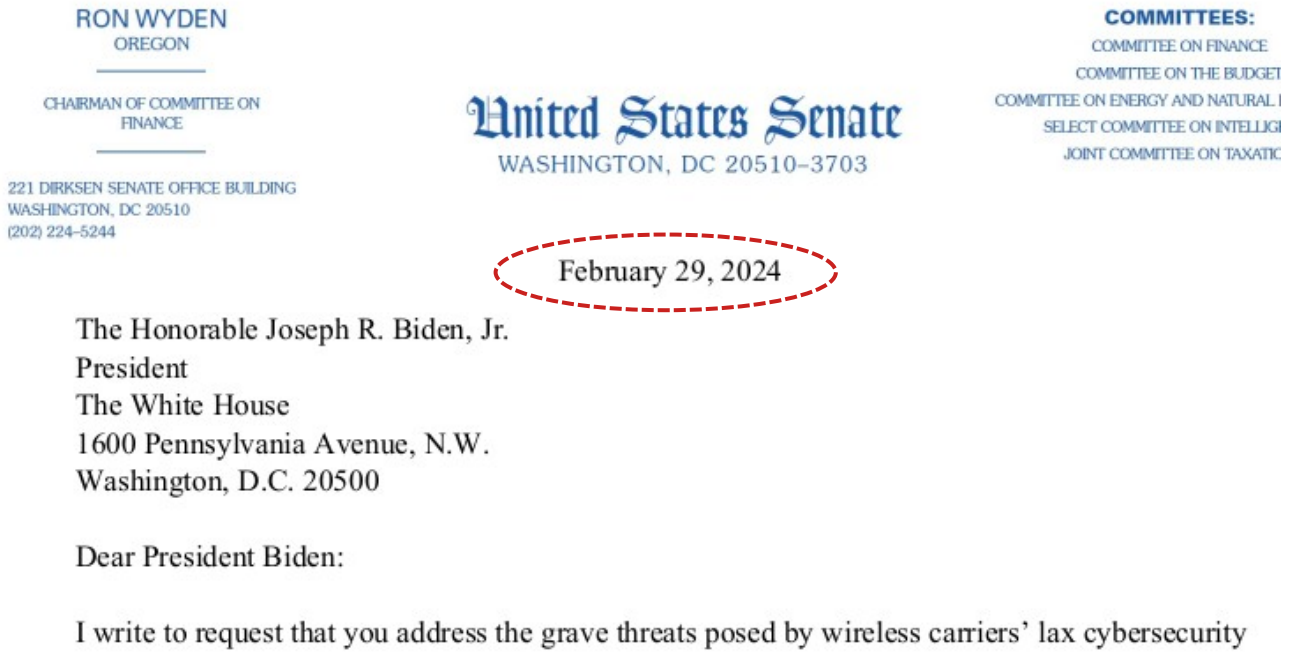
Attackers can take advantage of a decades-old protocol to exploit 5G networks.

Researchers at Black Hat Asia have shown how hackers can use an exploit in 5G networks because of the platform's reliance on an old protocol from 1975.

In the global rush to deploy 5G, security appears to have received insufficient attention. The new telecom platform is still using a broad and eclectic mix of old technologies. This makes it easy for cyberattackers to penetrate 5G systems.

Sergey Puzankov, Telecom Security Expert for Positive Technologies, gave a presentation at the Black Hat event entitled, "Back to the Future: Cross-Protocol Attacks in the Era of 5G."

- Why do spam/scam calls persist in 2024?



RON WYDEN
OREGON

CHAIRMAN OF COMMITTEE ON FINANCE

221 DIRKSEN SENATE OFFICE BUILDING
WASHINGTON, DC 20510
(202) 224-5244

United States Senate
WASHINGTON, DC 20510-3703

COMMITTEES:
COMMITTEE ON FINANCE
COMMITTEE ON THE BUDGET
COMMITTEE ON ENERGY AND NATURAL
SELECT COMMITTEE ON INTELLIGI
JOINT COMMITTEE ON TAXATIC

February 29, 2024

The Honorable Joseph R. Biden, Jr.
President
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Dear President Biden:

I write to request that you address the grave threats posed by wireless carriers' lax cybersecurity

https://www.wyden.senate.gov/imo/media/doc/wyden-phone-hacking-letter-to-president-biden.pdf

• Why do spam/scam calls persist in 2024?

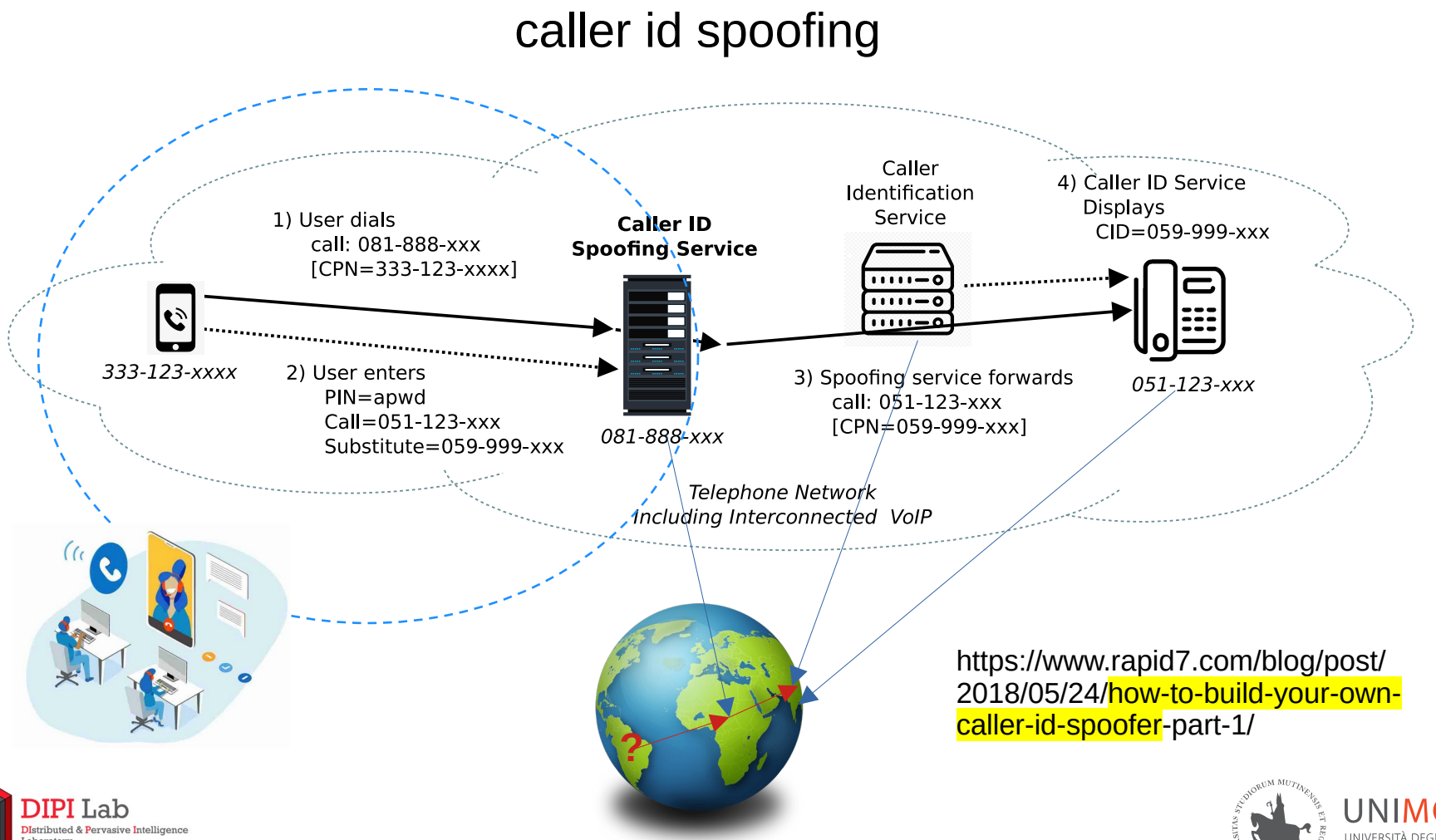
These phone company hacking services exploit flaws in two obscure technologies, known as Diameter and Signaling System 7 (SS7). These two technologies are used by wireless carriers around the world to deliver text messages between phone companies, and for roaming by their customers traveling abroad. For the last decade, cybersecurity researchers and investigative journalists have highlighted how wireless carriers' failure to secure their networks against rogue SS7 and Diameter requests for customer data has been exploited by authoritarian governments to conduct surveillance.

There is a simple reason for the wireless industry's failure to protect subscribers, including federal agencies: the U.S. government has failed to set minimum cybersecurity standards for wireless carriers like AT&T, T-Mobile, and Verizon. The FCC, Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA) have all acknowledged the serious threat of SS7 surveillance and of the importance of securing America's communications networks. Yet no official or agency has taken responsibility for this problem, and consequently, very little has been done. In addition to not taking responsibility for this problem, CISA is actively hiding information about it from the American people. The agency commissioned an independent expert report on this topic in 2022 which it permitted my staff to read at CISA's office in the fall of 2023. CISA refuses to publicly release this unclassified report, which includes details that are relevant to policymakers and Americans who care about the security of their phones.

[…] Moreover, OMB and the FCC should look to the United Kingdom's (UK) Telecommunications Security Code of Practice as a model. [...]

https://www.wyden.senate.gov/imo/media/doc/wyden-phone-hacking-letter-to-president-biden.pdf

- What methods are used for spam/scam calls today?



https://www.rapid7.com/blog/post/2018/05/24/how-to-build-your-own-caller-id-spoofer-part-1/

- What methods are used for spam/scam calls today?

Version 1: SS7

SigPloit will initially start with SS7 vulnerabilities providing the messages used to test the below attacking scenarios A- Location Tracking B- Call and SMS Interception C- Fraud

Version 2: GTP

This Version will focus on the data roaming attacks that occur on the IPX/GRX interconnects.

Version 3: Diameter

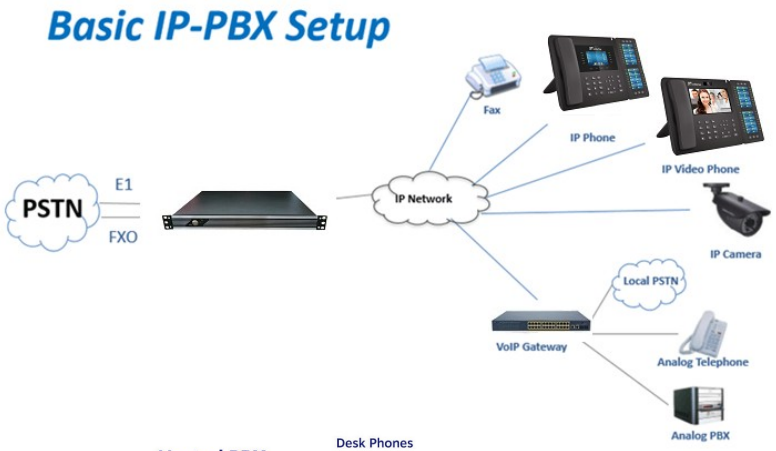
This Version will focus on the attacks occurring on the LTE roaming interconnects using Diameter as the signaling protocol.

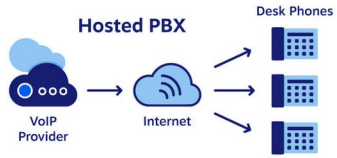
Version 4: SIP

This is Version will be concerned with SIP as the signaling protocol used in the access layer for voice over LTE(VoLTE) and IMS infrastructure. Also, SIP will be used to encapsulate SS7 messages (ISUP) to be relayed over VoIP providers to SS7 networks taking advantage of SIP-T protocol, a protocol extension for SIP to provide intercompatability between VoIP and SS7 networks

https://github.com/PenteSploit/ss7-attack

• What methods are used for spam/scam calls today?





Currently, cloud PBXs are rapidly replacing traditional PBXs, but this transition poses an additional concern for the security of cloud PBXs.

How do you evaluate your PBX security?

When we select a PBX in the cloud or that will be exposed to the Internet, it is very important to consider the following security features.

1. Does your PBX have a Firewall?
2. Does your PBX have intrusion blocking (fail2ban)?
3. Is your PBX blocked by Geo Firewall?
4. Does your PBX have the latest versions of the libraries used and operating system?

Some PBXs only have 2 of these three features, which makes them less secure.

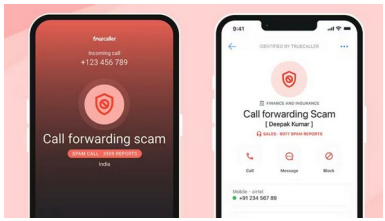
It is also very important that your PBX have the latest OS updates and use applications that are supported by the developers, which leads us to the following questions.

- What version of PHP does your PBX have?
- What version of Mariadb (MySql) does your PBX have?
- How secure is your SSL connection?

PBX / IP-PBX (and other equipments) are IT assets, exposed to cyberattacks and vulnerabilities like any other networked infrastructure !

What methods are used for spam/scam calls today?

- **SIP Trunk Hacking:** attackers exploit unsecured SIP trunks (connections between PBX systems and VoIP providers) to send massive amounts of traffic, often for toll fraud, where victims are billed for premium services without realizing it.
- **Call Forwarding Abuse:** scammers manipulate call forwarding settings on vulnerable phones or PBX systems, rerouting legitimate calls to fraudulent lines, often premium-rate numbers, to charge high fees.
- **Automated Call Distribution (ACD) Exploits:** attackers can manipulate or overwhelm ACD systems (which route incoming calls in customer service environments) to reroute or drop legitimate traffic, potentially for extortion or to facilitate further fraud.



- What methods are used for spam/scam calls today?

Abuse of VoIP Signalling

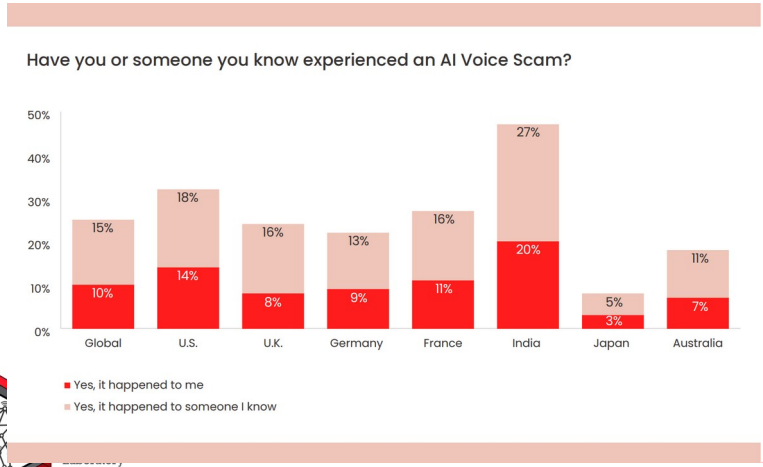
HSR HOCHSCHULE FÜR TECHNIK RAPPERSWIL
FHO Fachhochschule Ostschweiz

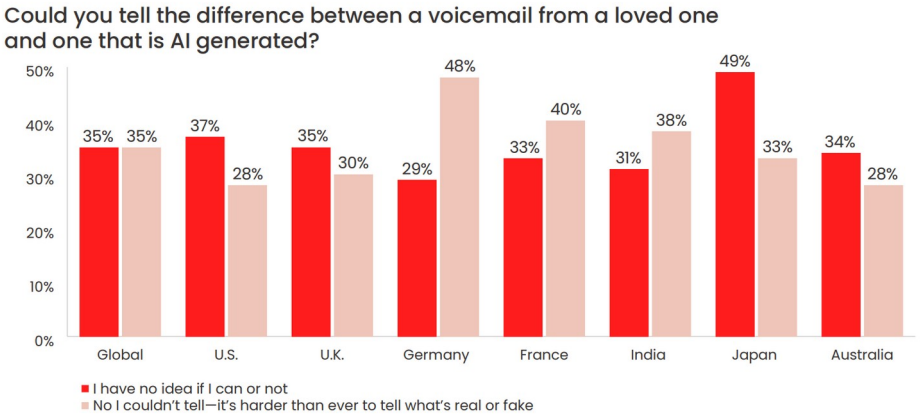
- Redirection or disruption of VoIP calls
  - If the SIP session management is not protected by special security measures an attacker can redirect VoIP calls to an arbitrary network destination (MITM attack) or can forcefully terminate them (DoS attack).
  - Dozens of VoIP signalling abuse scenarios have already been documented in the literature.
  - The call setup can be effectively secured by setting up a TLS session on a hop-to-hop basis (sips:bob@biloxi.com)
- Main problem: Lack of strong peer and gateway authentication
  - Man-in-the-Middle, Denial-of-Service or SPIT attacks can only be thwarted by a **strong** authentication of all communication parties (both clients and gateways). The introduction of a Public Key Infrastructure (PKI) will become **indispensable** at least at the domain level.

• What methods are used for spam/scam calls today?

And don't forget AI-driven attacks...

- 135% rise in novel social engineering attacks, primarily fueled by the adoption of generative AI tools, such as ChatGPT and Claude
- The generative capabilities of AI can be exploited to produce automated and personalized phishing calls and messages
- AI tools are being used to automate hacking attempts and generate polymorphic malware that evades detection





https://www.digitalinformationworld.com/2023/05/experts-raise-alarm-against-ai-voice.html

How can we reduce spam/scam calls?

Private Individuals:

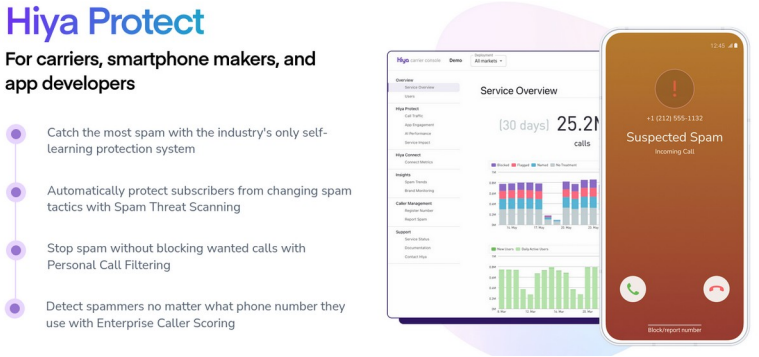
- Can block unknown or non-contacts without much impact.
- Risk missing personal or important calls from unknown numbers.
- Spam filters and blocklists can be more aggressive.
- ...

Business:

- Must balance call filtering carefully to avoid losing customers or important business calls.
- Blocking unknown numbers may result in missed leads or client calls.
- Need to rely on more sophisticated tools (e.g., CRM integration, call analytics) to differentiate between legitimate calls and spam/scam.
- ...

- How can we reduce spam/scam calls?

Well-known solutions



Examples of two commercial anti-spam/scam tools

How can we reduce spam/scam calls?

- **Whitelists:** Allow only calls from pre-approved contacts.
- **Blacklists:** Block calls from known spam numbers or patterns.
- **Reputation Filters:** Analyze caller reputation based on historical behavior and crowd-sourced data.
- **AI and Machine Learning Filters:** Identify and block scam patterns in real-time using advanced algorithms.
- **Challenge-Response Systems:** Require callers to verify their legitimacy before connecting.
- **Caller ID Authentication:** Verify caller identity using protocols like STIR/SHAKEN to prevent spoofing.

These solutions are often combined for better accuracy.

• How can we reduce spam/scam calls?

- **Time-based Blocking:** Restrict calls during specific hours to avoid peak spam times.
- **Geolocation Filtering:** Block calls based on suspicious or irrelevant geographic origins.
- **Pattern Recognition:** Identify abnormal calling patterns (e.g., repeated short calls) to detect spam.
- **Do Not Disturb Modes:** Automatically reject all calls except from essential contacts during set periods.
- **Behavioral Analytics:** Monitor call behavior to flag potential spam.
- **Interactive Voice Response (IVR) Screening:** Use pre-call voice menus to verify legitimate callers.
- ….

These solutions are often combined for better accuracy.

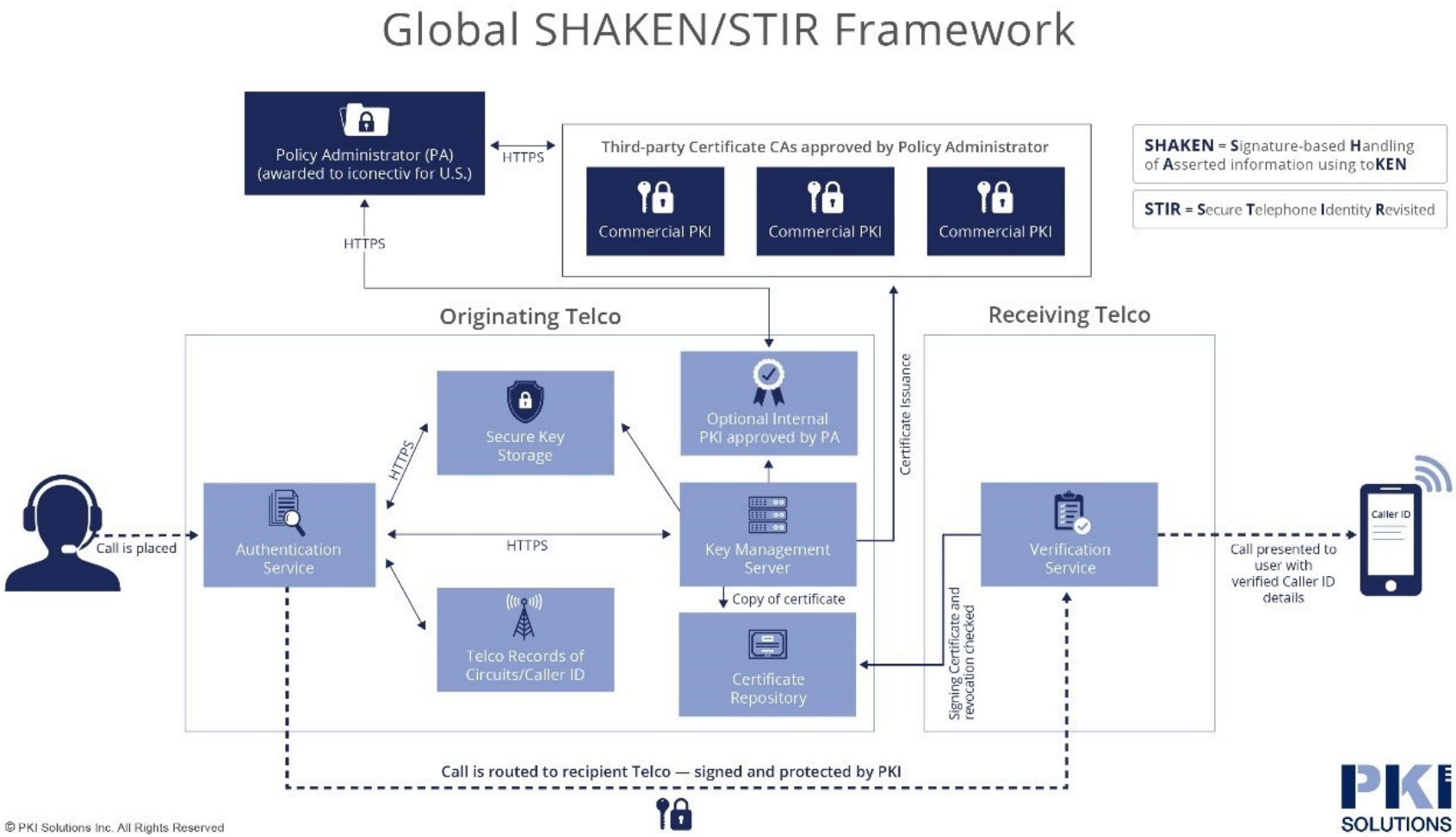
- How can we reduce spam/scam calls?

Academic proposals: potentially excellent, but the challenge is that they would need to be implemented by all network operators and/or end-to-end by users.

Study	Approach	Authentication	Validation	Anti-Spoofing	Shortcoming/Drawback
RFC 3325 [21]	Uses the P-Asserted-Identity header in the SIP to assert the identity of the caller	Medium	Low	Low	Inadequate for VoIP calls, easily circumvented and vulnerable to spoofing attacks
RFC 4474 [22]	Uses digital signatures to ensure the authenticity of the SIP INVITE message	High	Medium	Low	Complexity of the legacy infrastructure; not applicable in scenarios with SBCs; requires a public key infrastructure
STIR/SHAKEN [5]	Uses a signature-based token to verify the caller's number, aiming to reduce the impact of robocalling	High	High	Medium	Complexity of legacy infrastructure; centralized database required
RFC 8226 [8]	Uses X.509 certificates to authenticate the identity of the caller	High	High	Medium	Requires a trusted certificate authority
RFC 8224 [6]	Uses a header field in the SIP to carry a signature of the caller's identity	Medium	Medium	Low	Complexity of extracting caller-ID information; requirement for a centralized database
RFC 8225 [7]	A framework for verifying caller-ID using digital certificates; only applicable to VoIP calls that traverse the IP network and not to calls made via SS7	Medium	Medium	Medium	Lack of detailed implementation solution; inadequate for VoIP calls
BBCA [11]	Uses blockchain technology to create a decentralized ledger that stores caller-ID information and allows for real-time validation of caller-ID information to prevent caller-ID spoofing attacks	High	High	High	Implementation difficulty due to regulatory compliance and integration; every provider must be implement the protocol

TABLE I: Comparison of Various Approaches to Caller ID Authentication

- How can we reduce spam/scam calls?



• How are spam/scam calls regulated in different countries?

From a Legislative, Administrative, and Criminal Perspective

- Scam is prosecuted almost everywhere in the world
- Regulations on spam vary by country, however, over time, spam laws are becoming increasingly stringent.

Examples:

- European Union: companies that violate GDPR spam rules can face fines up to €20 million or 4% of their global annual turnover
- India: penalties can involve imprisonment and fines of up to $120,000 USD. For Spam Telecom Regulatory Authority imposing fines of ₹50,000 per violation.

  China: scams can lead to heavy penalties, including imprisonment for serious fraud cases, while spam violations under the country's cybersecurity laws can result in fines up to ¥1 million ($150,000 USD) for organizations that violate anti-spam provisions.
- ...

- How are spam/scam calls regulated in different countries?

From a Legislative and Technological Perspective

In the USA, the FCC has forced the adoption of STIR/SHAKEN to authenticate caller IDs. In practice, less than 50% of the calls are done under this framework.

Despite the regulatory push, major telecom companies like AT&T have difficulties to a full transition to SIP hence they still rely on outdated protocols and networks which not support the STIR/SHAKEN framework.

- How are spam/scam calls regulated in different countries?

From a Legislative and Technological Perspective

France promotes the adoption of technologies like STIR/SHAKEN, but progress is uneven, with partial implementation across operators' SIP core networks.

The fragmented approach leaves remote areas vulnerable, weakening the overall effectiveness of number authentication measures.

The French government acknowledges the challenges and emphasizes the need for a coordinated, comprehensive approach to integrate these solutions across all networks.

- How are spam/scam calls regulated in different countries?

From a Legislative and Technological Perspective

By 2024, the landscape of number authentication has evolved, with Canada and the UK joining the forefront along-side the USA and France.

Canada has made notable strides by aligning its policies with the USA to facilitate cross-border telecommunications security.

Singapore and Australia signed a Memorandum in 2022 of Understanding (MoU) to enhance cooperation in combating scams and spam communications, focusing on telephony.

- How are spam/scam calls regulated in different countries?

From a Legislative and Technological Perspective

Since 2019, **Brazil** has implemented measures like the "Do Not Disturb" list and "0303" prefix for telemarketing calls to reduce spam.

Tools such as the "Which Company Called Me" portal and STIR/SHAKEN protocol contributed to a **claimed** 60% drop in spam call complaints.

However, international calls, especially from countries without similar regulations, remain a challenge, particularly for businesses, as they are harder to detect when using non-Brazilian numbers.

- How are spam/scam calls regulated in different countries?

From a Legislative and Technological Perspective

And your country?

- What role do governments play in combating spam/scam calls?

- Government Role: essential in combating spam/scam calls, as companies resist implementing costly solutions.
- STIR/SHAKEN: while it is "a *de iure, de facto* solution", it must be complemented by other technologies like those in Brazil.
- AI Integration: intrusion detection will be crucial, and governments must guide its implementation through regulation.
- International Cooperation: global coordination is vital, as international spam and scam calls require unified regulations and cross-border enforcement efforts.

Conclusion

- Number authentication is key to improving telephony security.

- A multi-faceted approach involving **technology, regulation, and cooperation** is required – worldwide

Thank you for your attention!

If you have any other questions,
feel free to email me at
marcello@unimore.it