|  |
| --- |
|  |
| **Title\*:** | Overview of spoofed call developments |
|  |  |
| from **Source**\*: | Yaana Limited |
| Contact: | Anthony Rutkowski  |
|  |  |
| input for **Committee**\***:** | CYBER |
|  |  |
| Contribution **For\*:** | Decision |  |  |
|  | Discussion | **X** |  |
|  | Information |  |  |
|  |  |
| Submission date**\***: | 2016-09-08 |
|  |  |
| Meeting & Allocation: | **CYBER#8** -  |
| Relevant WI(s), or deliverable(s): |   |
|  |

**ABSTRACT:***This contribution provides a structured overview of requirements, reports, measures and venues addressing the growing challenges of spoofed telephone calls with a view to considering related TC CYBER activity.*

## Introduction

At the most generic level, spoofing is asserting a false identifier in the course of a communication. Spoofing can occur in many different telecommunication contexts by users, systems, and devices for different purposes – generally to undertake malicious acts. Spoofing can occur to fraudulently obtain service, to make massive numbers of unsolicited phone calls (also called robocalls) or messages, and perpetrate other forms of crime. In relatively rare instances, it can also occur lawfully to assist law enforcement in undertaking an investigation or protect security services.

The Telephone Service has been the subject to substantial treaty provisions since 1903.[[1]](#footnote-1) It also has been treated in a special category of international telecommunication service subject to additional obligations.[[2]](#footnote-2)

When defined gateways between the un-controlled tcp/ip internet and the well-controlled PSTN signalling systems began to emerge through application gateways circa 1993, the potential for spoofing at a massive scale emerged.[[3]](#footnote-3) With the passage of time, additional gateways emerged – especially for signalling and number resolution mechanisms to facilitate VoIP use. Coupled with the trend toward deregulation of legacy telecommunications infrastructure worldwide, and the fragmentation of those networks, the challenges of call spoofing have become ever worse.

Over the past decade, legislative, regulatory and technical bodies at global, regional, and national levels began treating the subject of spoofed calls. Call spoofing emerged as a major issue at the ITU in multiple venues beginning in 2012.[[4]](#footnote-4) Notwithstanding an entire ecosystem of spoofed call mitigation forums, standards, and law (described in the following clause below) treating the subject since the turn of the century, the spoofed call problem has grown exponentially worse. In 2014, OFCOM reported that in 2014, the spoofed call level in the UK had risen to 1-2 billion per year.[[5]](#footnote-5) Just how worse it has become was revealed several weeks ago by Pindrop Labs threat intelligence researchers at the 2016 Blackhat USA security conference.[[6]](#footnote-6) During the first half of 2016, Pindrop’s telephony spam honeypot recorded 100,000 calls. The associated levels of fraud and forms of crime are staggering – the largely U.S. oriented Communications Fraud Control Association estimating the 2015 losses at US$38.1 billion.[[7]](#footnote-7) The adverse effects on cyber security, consumer protection, critical infrastructure protection, lawful interception and almost every compliance obligation are enormous.[[8]](#footnote-8)

The situation has resulted in several significant regulatory actions. On 14 June 2016, the many of the members of the intergovernmental London Action Plan signed a MoU for international cooperation.[[9]](#footnote-9) On 19 August, the Federal Communications Commission in the U.S. convened a so-called Robocall Strike Force to develop solutions.[[10]](#footnote-10) At the recent ITU-T SG17 meeting, a new work item was also adopted.[[11]](#footnote-11) At the same time, some scepticism exists following years after the GSMA, 3GPP, CEPT ECC, ITU-T, ETSI, and other bodies have undertaken individual workshops and initiatives over nearly a decade with limited effect.[[12]](#footnote-12)

## Global Spoofed Call Mitigation Ecosystem

The rapidly growing adverse effects and challenges of mitigating spoofed calls have given rise to an extensive ecosystem of diverse industry technical and intergovernmental forums.



Figure 1. Spoofed call mitigation global ecosystem

This ecosystem depiction may not be complete, but it was prepared following significant searching and analysis of online materials, workshop proceedings, industry standards work items and guidelines, as well as the examining the cross references to other bodies and their work. It is fairly common to see institutional insularity – where bodies function largely within their own communities or national borders. Increasingly, however, global industry bodies like 3GPP, ECC, ITU-T and M3AAWG have become more proactive to identify a broad array of forums and avoiding duplication of existing work. The emergence of ISACs (Information Sharing and Analysis Centres) as part of this ecosystem is noteworthy as a means to measure with some precision the nature and source of the threats, to identify potential mitigations for deployment. It is also becoming apparent that spoofed calling is simply another species of cyber threat that is facing service providers and end users.

Arguably, the most significant activity is that of 3GPP because of the industry participants of which it is comprised, the scale and frequency of its meetings, and its force and effect in adopting required specifications for the global infrastructure. The 3GPP SA3 (security) initial study in TR33.831 ended in 2014 without an effective solution.[[13]](#footnote-13) A subsequent ongoing study in SA3 points to several technical solutions that may be more promising – relying on a combination of telephone identity certificates and authenticated traffic exchange developed by a combination of IETF, the SIP Forum, and ATIS.[[14]](#footnote-14) The identity mechanisms have also been recently introduced into 3GPP SA1 (services).[[15]](#footnote-15) The combination of “STIR and SHAKEN” platforms is being pursued by a significant industry segment.[[16]](#footnote-16)

However, significant operational and implementation challenges exist around the STIR and SHAKEN platforms that go to fundamental legal and regulatory issues such as who creates the certificates (CAs) used in these processes – and the criteria for verification and bindings to trusted global service provider identifiers (SPIDs) and authoritative allocations of E.164 international public telecommunication numbers.[[17]](#footnote-17) These challenges are exacerbated by the different policies among countries on what constitutes a service provider, how they are registered, identified and regulated, and the permissible uses of E.164 numbers. The concept of a Global SPID (historically referred to as an [ITU Carrier Code](https://www.itu.int/oth/T0201)) to identify E.164 number assignees was advanced in the ITU-T almost a decade ago with no resolution.[[18]](#footnote-18) Several years later, the need was recognized and pursued in multiple industry bodies, including GSMA, the I3 Forum, and the IETF.[[19]](#footnote-19) It is now partially implemented in a GSMA specification.[[20]](#footnote-20) Recently, ETSI TC NTECH has advanced a new work item on the impact of alphanumeric user identifiers on interconnection scenarios – focussing on interoperability and mapping of Internet domain names to E.164 numbers in order to allow interconnection between networks.[[21]](#footnote-21)

## Conclusions on a TC CYBER role

The challenges of spoofed caller ID and the ensuing harm have already created a rather large and diverse ecosystem of forums. The subject matter is also hardly new for ETSI – having engaged in related work a decade ago. Additionally, the criminal behaviour and policy decisions call for mitigating solutions that lie beyond just clever network operations traffic identity management. A broad array of governmental agencies worldwide have engaged and will continue to be active in their own national, regional, and global forums seeking solutions. The conclusions and recommendations from the “UK experience” articulated by OFCOM two years ago seem still applicable.[[22]](#footnote-22)

.

* CLI spoofing problem is growing
* Current mitigations are unlikely to be fully effective
* Longer term solutions will take time
* Implementation will be complex
* International cooperation and collaboration must be made more effective
* Implementation of longer term solutions needs to be considered in parallel to technical work

Technically, the rather remarkable threat intelligence forensics and analysis presented at the recent BlackHat USA 2016 conference by a startup spun out of several years of research at Georgia Tech, suggests that additional new mitigation techniques used in the cyber security field may be effective.[[23]](#footnote-23) Especially relevant is the finding that machine learning can “uniquely ‘fingerprint’ bad actors,” and “results show that 51% of the robocalls recorded can be attributed to only 38 distinct telephony infrastructures and that they can be quickly identified with high accuracy.”[[24]](#footnote-24)

All of these factors suggest a significant useful role for ETSI TC CYBER in the form of a Technical Report that: 1) facilitates the exchange of work and ideas across the many forums comprising the global ecosystem, and 2) examines how emerging cyber security techniques for threat information exchange and defence measures can be useful in meeting the challenges. TC CYBER can also work with other ETSI TCs (e.g., LI, ESI, NTECH), as well as serve as a source of information for London Action Plan members. No other body is likely to undertake such activity.

1. See [International Telegraph Service Regulations annexed to the International Telegraph Convention of St. Petersburg](http://www.itu.int/en/history/Pages/TelegraphAndTelephoneConferences.aspx?conf=24&dms=S0201000009) (London, 1903) [↑](#footnote-ref-1)
2. See, e.g., ITU, Telephone Regulations (Geneva, 1973); ITU, International Telecommunication Regulations (Melbourne, 1988); Final Acts of the World Conference on International Telecommunications (Dubai, 2012) [↑](#footnote-ref-2)
3. See, e.g., The Internet Multicasting Service, TPC.int, TPCint.org, See, also, RFC 1530, Principles of Operation for the TPC.INT Subdomain: General Principles and Policy, Oct 1993. [↑](#footnote-ref-3)
4. See, e.g., WTSA-12 Res. 65, *Calling Party Number Delivery, Calling Line Identification and Origin Identification*; WTSA-12 Res. 29, *Alternative Calling Procedure*; PP-06 Res. 21, *Alternative Calling Procedures on Telecommunication Networks*; and WTDC-10 Res. 22, *Alternative Calling Procedures on International Telecommunication Networks, Identification of Origin and Apportionment of Revenues, in Providing International Telecommunication Services*. [↑](#footnote-ref-4)
5. Saunders, Director, Network Infrastructure, OFCOM, [*The UK experience and approach to damage mitigation*](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/callerid/Documents/presentations/S1P2-Huw-Saunders.ppt), ITU Workshop on “Caller ID Spoofing,” 2 Jun 2014. [↑](#footnote-ref-5)
6. See, Aude Marzuoli, [Call Me: Gathering Threat Intelligence on Telephony Scams to Detect Fraud](https://www.blackhat.com/us-16/briefings/schedule/#call-me-gathering-threat-intelligence-on-telephony-scams-to-detect-fraud-4134), Blackhat USA 2016, 4 Aug 2016. [↑](#footnote-ref-6)
7. [Communications Fraud Control Association (CFCA) announces results of global telecom fraud survey, 28 Sep 2015](http://www.cfca.org/pdf/survey/2015_CFCA_Global_Fraud_Loss_Survey_Press_Release.pdf). [↑](#footnote-ref-7)
8. See ETSI TR103 369 (2016-08), CYBER; [Design requirements ecosystem](http://www.etsi.org/deliver/etsi_tr/103300_103399/103369/01.01.01_60/tr_103369v010101p.pdf). [↑](#footnote-ref-8)
9. See London Action Plan, [Commitment to international cooperation: London Action Plan members sign MoU](http://londonactionplan.org/news/commitment-to-international-cooperation-london-action-plan-members-sign-mou/), 14 Jun 2016. [↑](#footnote-ref-9)
10. Public Notice, [FCC To Host First Meeting Of Industry-Led Robocall Strike Force](http://transition.fcc.gov/Daily_Releases/Daily_Business/2016/db0812/DA-16-917A1.pdf), 12 Aug 2016. [↑](#footnote-ref-10)
11. See ITU-T X.ctss, *Supplement to ITU-T X.1231, Technical framework for countering telephone service scam*, SG17 Doc. TD2926 Rev.1 [↑](#footnote-ref-11)
12. See, e.g., Wired, [Apple and Google are teaming up0 to kill robocalls forever](https://www.wired.com/2016/08/fcc-robocall-strike-force/), 22 Aug 2016. See also, GaTech[, Telephone Scams and Spoofing](http://www.oit.gatech.edu/service/telecommunications/telephone-scams-and-spoofing), 2008; [ITU Workshop on “Caller ID Spoofing”,](file:///D%3A%5CUsers%5Ctrutkowski%5CDocuments%5Corgs%5CETSI%5CCYBER%5C05-CONTRIBUTIONS%5C2016%5C_spoofing%5CITU_workshop%5CITU%20Workshop%20on%20)  2 Jun 2014; 3GPP, [TR 33.831](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2318), Study on security on spoofed call detection and prevention; 3GPP, [TR 33.832](https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=2319), Study on IMS Enhanced Spoofed Call Prevention and Detection; CEPT ECC, [Increasing trust in calling line identification and originating identification Kristiansand](http://www.erodocdb.dk/Docs/doc98/official/pdf/ECCREP133.PDF), September 2009; ECC recommendation (11)02, [Calling line identification and originating identification](http://www.erodocdb.dk/Docs/doc98/official/pdf/REC1102.PDF), 5 May 2011; MIT Technology Review, [The Do-Not-Call List Has a Gaping Hole](https://www.technologyreview.com/s/602284/the-do-not-call-list-has-a-gaping-hole/), Sep 2016. [↑](#footnote-ref-12)
13. See 3GPP TR 33.831 V1.0.0 (2014-08), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study on Security on spoofed call detection and prevention (Stage 2); (Release 12) [designated FS\_SPOOF]. [↑](#footnote-ref-13)
14. See 3GPP TR 33.832 V0.3.0 (2015-08), 3rd Generation Partnership Project; Technical Specification Group Services and Systems Aspects; Study on IMS Enhanced Spoofed Call Prevention and Detection (Release 13) [designated ESCAPADES]; IETF, [Authenticated Identity Management in the Session Initiation Protocol (SIP)](https://www.ietf.org/id/draft-ietf-stir-rfc4474bis-12.txt), draft-ietf-stir-rfc4474bis-12, 9 Sep 2016; IETF, [Persona Assertion Token](https://www.ietf.org/id/draft-ietf-stir-passport-07.txt), draft-ietf-stir-passport-07, 9 Sep 2016; IETF, [Secure Telephone Identity Credentials: Certificates](https://www.ietf.org/id/draft-ietf-stir-certificates-08.txt), draft-ietf-stir-certificates-08, 9 Sep 2016; [ATIS, Developing Calling Party Spoofing Mitigation Techniques: ATIS’ Role](https://www.atis.org/01_resources/whitepapers/ATIS_Robocalling_Summary.pdf), August 2016; SIP Forum, SIPNOC2016, [Framework for Call Validation Display Anti Spoofing / Caller Validation / Robocall Mitigation](http://www.sipforum.org/component/option%2Ccom_docman/task%2Cdoc_download/gid%2C819/Itemid%2C261/). [↑](#footnote-ref-14)
15. See S1-16271, User Controlled Spoofed Call Treatment (SPECTRE), Aug 2016; S1-162272, Presentation of the results of spoofed call detection to the terminating user, Aug 2016; S1-162273, Addition of spoofed callerid as a criteria for call diversion and call blocking features, Aug 2016. [↑](#footnote-ref-15)
16. See COMCAST Labs, [STIR and SHAKEN Framework Overview](http://www.sipforum.org/component/option%2Ccom_docman/task%2Cdoc_view/gid%2C822/Itemid%2C261/), SIPNOC2016. [↑](#footnote-ref-16)
17. See Rec. ITU-T E.164, The international public telecommunication numbering plan (11/2010 as amended 2011/06); Rec. ITU-T E.164.1, Criteria and procedures for the reservation, assignment and reclamation of E.164 country codes and associated identification codes (ICs) (09/2008); Rec. ITU-T E.164.3, Principles, criteria and procedures for the assignment and reclamation of E.164 country codes and associated identification codes for groups of countries (09/2001); Rec. ITU-T E.195, ITU-T International numbering resource administration (09/2000); Rec. ITU-T E.156, Guidelines for ITU-T action on reported misuse of E.164 number resources (05/2006). See also, [Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)](http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN); ETSI TR 187 009 V2.1.1 (2008-07), [Telecommunications and Internet Converged Services and Protocols for Advanced Networking (TISPAN); Feasibility study of prevention of unsolicited communication in the NGN](http://www.etsi.org/deliver/etsi_tr/187000_187099/187009/02.01.01_60/tr_187009v020101p.pdf); ETSI TR 187 015 V3.1.1 (2011-05), [Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Prevention of Unsolicited Communication in the NGN](http://www.etsi.org/deliver/etsi_tr/187000_187099/187015/03.01.01_60/tr_187015v030101p.pdf). [↑](#footnote-ref-17)
18. See ITU, Verisign, [Implementation of Universal Global Trusted Service Provider Identity (Trusted SPID)](https://www.itu.int/dms_pub/itu-t/oth/15/05/T15050000020005PDFE.pdf), 2008; UK, [Service Provider Identifiers (SPIDs)](https://www.itu.int/md/dologin_md.asp?lang=en&id=T05-SG02-C-0090!!MSW-E), ITU-T COM2-90, April 2008. [↑](#footnote-ref-18)
19. See IETF, [SP URN](https://tools.ietf.org/html/draft-pfautz-service-provider-identifier-urn-02), draft-pfautz-service-provider-identifier-urn-02, February 17, 2012; Penn Pfautz, [Global Service Provider ID](https://www.ietf.org/proceedings/81/slides/dispatch-1.pptx)
draft-pfautz-service-provider-identifier-urn-01, IETF 81, July 2011; International Interconnection Forum for Services Over IP (i3 FORUM) [Global SPID Whitepaper](http://i3forum.org/sites/default/files/i3_Global_SPID_Specifications_Release_1_may_2011.pdf) (Release 1.0) May 2011. See also, [Number Portability Administration Center, How LNP Works](https://www.npac.com/number-portability/how-lnp-works). [↑](#footnote-ref-19)
20. GMSA PRD, [IR.67 DNS and ENUM Guidelines for Service Providers and GRX and IPX Providers](http://www.gsma.com/newsroom/wp-content/uploads/IR.67-v12.02.pdf) v12.02, 01 February 2016. [↑](#footnote-ref-20)
21. See ETSI TR 103 453 V0.0.2 (2016-09), Network Technologies (NTECH); Impact of alphanumeric user identifiers on interconnection scenarios. [↑](#footnote-ref-21)
22. Huw Saunders, [The UK experience and approach to damage mitigation, ITU Workshop on “Caller ID Spoofing”](http://www.itu.int/en/ITU-T/Workshops-and-Seminars/callerid/Documents/presentations/S1P2-Huw-Saunders.ppt) (Geneva, Switzerland, 2 June 2014). [↑](#footnote-ref-22)
23. Aude Marzuoli et al, [Call Me: Gathering Threat Intelligence on Telephony Scams to Detect Fraud](https://www.blackhat.com/docs/us-16/materials/us-16-Marzuoli-Call-Me-Gathering-Threat-Intelligence-On-Telephony-Scams-To-Detect-Fraud-wp.pdf), Blackhat USA 2016, 4 Aug 2016. See also, [Georgia Tech company profile](http://www.news.gatech.edu/features/company-profile-pindrop-security). [↑](#footnote-ref-23)
24. Ibid. [↑](#footnote-ref-24)