SoK: Fraud in Telephony Network

***Abstract*—Telephone networks first appeared more than a hundred years ago, long before transistors were invented. They, therefore, form the oldest large scale network that has grown to touch over 7 billion people. Telephony is now merging many complex technologies and because numerous services enabled by these technologies can be monetized, telephony attracts a lot of fraud. In 2015, a telecom fraud association study estimated that the loss of revenue due to global telecom fraud was worth 38 billion US dollars per year. Because of the convergence of telephony with the Internet, fraud in telephony networks can also have a negative impact on security of online services. However, there is little academic work on this topic, in part because of the complexity of such networks and their closed nature. This paper aims to systematically explore fraud in telephony networks. Our taxonomy differentiates the root causes, the vulnerabilities, the exploitation techniques, the fraud types and finally the way fraud benefits fraudsters. We present an overview of each of these and use CAller NAMe (CNAM) revenue share fraud as a concrete example to illustrate how our taxonomy helps in better understanding this fraud and to mitigate it.**

1. Introduction

Telephony, which used to be a closed system, has undergone fundamental changes in the past several decades. The introduction of new communications technologies and convergence of telephony with the Internet has added to its complexity. Despite (or because) of having been deployed for virtually hundreds of years, security challenges for telephony are neither well understood nor well addressed.

In this paper, we focus on the fraud and cybercrime ecosystem surrounding voice telephony (over all three networks - the Public Switched Telephone Network or PSTN, cellular and IP networks). We aim to provide a systematization of knowledge relevant to understanding telephony fraud. Our taxonomy allows to classify the techniques and fraud schemes without ambiguity. We believe that a good understanding of telephony fraud will provide insights for future research, increase cooperation between researchers and industry and finally help in fighting such fraud.

Although, we focus on telephony fraud, our work has broader implications. For example, a recent work shows how telephony fraud can negatively impact secure creation of online accounts [1]. Also, online account takeovers by making a phone call to a call center agent have been reported in the past [2], [3]. Telephony is considered as a trusted medium, but it is not always. A better understanding of telephony vulnerabilities and fraud will therefore help us understand potential Internet attacks as well.

1.1. Fraud in Telecommunication Networks

Existing definitions of telecommunications fraud usually focus on obtaining free telecommunications services and gaining financial benefits [4], [5]. In this work, we narrow our perspective to voice telephony but we do not limit frauds to financial benefits (a definition will be given in Section 3). Perpetrators of voice fraud may be any actor of the telephony ecosystem, such as operators, third party service providers, customers, employees and any other external party with the means and motivation to commit fraud. On the other hand, victims of voice fraud can be the operators, customers and enterprises that use telecom networks.

A survey of telecom service providers in 2015 estimates the losses due to fraud to 38.1 billion US dollars. This constitutes 1.69% of the estimated global revenue [6]. In addition to the financial losses, fraud aiming at service disruption or reputation damage may have devastating effects, because the telecommunications network is a critical infrastructure with millions of users relying on it. On the other hand, consumers are also victims of such fraud, the United States Federal Trade Commission (FTC) receives an average of 400,000 complaints per month [7].

Perpetrating fraud in telecom networks is relatively easy. Most of the attacks can be performed remotely and they do not require major equipment or high level of technical expertise. Moreover, it is often very easy to obtain a financial benefit from telephony fraud [8]. Often, fraud is buried

in massive volume of traffic and large variety of services. Therefore, it is difficult to identify, detect and prevent.

Having a comprehensive understanding of telephony fraud is a challenging task. For this, one needs to have a good understanding of the telephony ecosystem, its history, underlying technologies, regulations and international agreements.

Telecom industry embodies different communities such as operators, regulators and users. Every actor in this ecosystem experiences or approaches fraud in a different way. Moreover, each community has its own terminology, context and resources regarding fraud, which is a major obstacle in understanding fraud. We next explain the related work from each community and their limitations.

1.2. Related Work

Operators and service providers usually share fraud related information among their partners and various industry associations (e.g., TMForum, i3Forum, GSMA, FIINA, CFCA).[1] Unfortunately, such groups are often restricted to vetted members and do not make their documents publicly available. The point we make in this paper is the opposite: *we will only be able to fight fraud efficiently if it is well understood and openly discussed*. A first attempt to create a fraud classification system that distinguishes *enabler techniques* and *fraud types* was proposed by the TM Forum [9], an approach that we extend in this work.

A lot of information about fraud schemes can be found in white papers by companies selling fraud detection systems [10], [11], but those often present an incomplete view because of the possible commercial interests.

In the academic literature, there is no previous systematic survey of telephony fraud. However, there are resources that handle part of the problem or try to reduce the problem into a single dimension such as actors (fraudster or victim) [12], underlying service and technology [13], [4], attack methodology or attack motivation [14]. However, the fraud ecosystem is too complex to be explained with a binary classification. [15] studies the telecom system security, covering many fraud related topics. It concludes that information on phone fraud is scattered and no single resource brings everything together. Another important work on telecommunications crime [16] presents historical information and some of the more recent fraud schemes. Existing surveys [14] address fraud detection, but do not try to systematize the fraud itself.

In [17], [18] authors analyze data from phone honeypots uncovering several fraud schemes affecting end users. [19] analyzes the voice spam ecosystem and evaluates existing solutions. There are also many books on telecom security related topics such as revenue assurance [20], fraud and quality of service management [13], UC (Unified Communications) [21] and VoIP network security. However, none of these resources provide a comprehensive view of the fraud ecosystem.

1. www.tmforum.org, i3forum.org, www.gsma.com, www.fiina.org, www.cfca.org

International bodies, such as ITU (an agency of the United Nations) and BEREC (an agency of the European Union), and regulatory bodies, such as the Federal Communications Commission (FCC) and the Federal Trade Commission (FTC), are also concerned about some aspects of the fraud (e.g., *number misuse* [22], *robocalling* [23]) but they also do not aim at providing a comprehensive view on the telephony fraud.

1.3. Goals

In this paper, we aim to clarify telephony fraud and provide a holistic understanding of telephony fraud by considering its causes, the techniques, the fraud schemes and the reasons why fraud may be profitable. We hope that a better understanding of fraud mechanisms will foster research on this topic. We also believe that it is required to understand telephony fraud well to address it efficiently.

A fraud scheme often has multiple names, e.g., describing a variant, the technical aspect or the user visible part of the iceberg. In other cases, one name is used to describe several different schemes. We therefore also aim to clarify the inconsistencies in existing fraud terminology.

Moreover, this study may be beneficial to increase fraud awareness among users and operators that are not members of any industry group. In fact, a survey conducted among the wholesale operators in 2013 [24] shows that around 73% of the operators are not members of any of the industry groups.

1.4. Paper Organization

In the next section (2) we provide the necessary background information on the telephony ecosystem, summarizing the key concepts and money flows. Then we present an overview of our methodology in Section 3. In the four next sections we describe fraud in our taxonomy: root causes (4), weaknesses (5), techniques (6), the main fraud schemes (7), and the way fraud can benefit fraudsters (8). We then present a case study in Section 9. Finally, we conclude the paper in Section 10.

2. Overview of the Telephony Ecosystem: Networks and Money Flows

In this section, we provide a high level overview of voice telephony related networks and components that are required to understand fraud in voice telephony.

2.1. Telephony Networks and Components

Public Switched Telephone Network (PSTN). The historic core of telephony networks is formed of copper telephone wires that use circuit-switching technology to transmit analog voice signals (also called Plain Old Telephone Service (POTS). Switches in operators' *Central Offices* (PSTN CO) control call establishment by creating a dedicated physical circuit from the caller's phone to the

callee's phone. Initially, the same circuit was used for the *in-band* signaling between the callee and the operator (e.g., dial tone and ringing) but also between operators (e.g., billing, call routing).

Integrated Services Digital Network (ISDN). ISDN allows digital transmission over the copper lines. Up to 30 lines can be multiplexed on a physical phone line (T1 or E1 *Primary Rate Interface* (PRI)) for transmitting data or voice. ISDN dedicates a separate channel for signaling (*out-of-band* signaling), which constitutes the user part of the Signaling System 7 (SS7) protocol [25]. Digital networks and out-of-band signaling solved some security problems (see Section 7.1) and introduced new features to telephony, e.g., voice mail, call forwarding and caller ID display.

Mobile Networks. Most of the mobile networks are still using GSM protocols and equipment (2G) but also support more recent protocols (3G and 4G/LTE). Each generation of mobile communication uses some form of encryption (over the wireless channel) and specific equipment to handle the communications and customer identification (e.g., Mobile Switching Center (MSC) and Home Location Register (HLR) in 2G). Mobile phones (except CDMA phones) use a SIM (Subscriber Identity Module) card with an International Mobile Subscriber Identity (IMSI) that uniquely identifies the user on the network. The SIM card contains a cryptographic key which is assigned by the operator and associated with the IMSI.

Voice over IP (VoIP). With the rise of the Internet, transmission of Voice over IP (VoIP) emerged as an alternative to traditional PSTN. Currently, telephone networks consist of various gateways between PSTN, cellular networks and VoIP telephony. Over-The-Top services (OTT) are services which work on top of data links and, in general, out of operators' control. Such voice services (e.g., Skype, Viber) are attracting more users and are seen as a threat by the operators [26].

Private Branch Exchange (PBX). Enterprise customers usually use a PBX to manage their internal and external communication needs. A traditional PBX provides *extensions*, i.e., an internal phone number to reach each user within the enterprise. A PBX also has a connection (called a *trunk*) with an operator to reach the PSTN or mobile networks. The trunk usually supports a certain number of simultaneous communications, which may be different from the total number of phone numbers used by the company. A traditional PBX uses phone cables for all internal lines which is expensive to deploy and manage. On the other hand, an IP-PBX can connect IP phones or soft phones over IP (see Figure 1). IP-PBXs can use PRI trunks, SIP trunks or SIM cards for external communications.

2.2. Telephony Actors

Apart from the end-users, the main actors of the telephone networks are the operators (carrier, telecom service provider) and third party service providers.

Operators. The deregulation of the telecommunications markets have resulted in wide variety of service providers and operators. Some of these operators invest in, or own, the network infrastructure and equipment, whereas others only resell the service they buy from other operators (e.g., Mobile Virtual Network Operators (MVNO)).

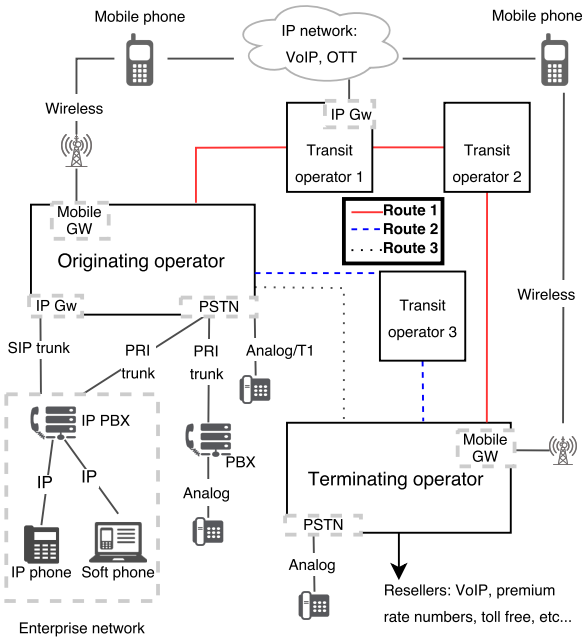

Figure 1: Overview of the telephony ecosystem.

Third Parties. Third party service providers and VoIP resellers [27] are important actors of the telephony ecosystem. Value added service (e.g., premium rate service) providers deliver content to end-users via phone calls, messaging or data network (e.g., gaming, chat lines or news). VoIP resellers buy communication services from carriers, and resell through VoIP gateways. They provide geographical numbers (numbers with country and area codes), mobile numbers, toll free numbers and premium rate numbers in every country. In recent years, cloud based communication services have appeared (e.g., Twilio [28]) and provide access to cheap bulk phone numbers (that are usually recycled), *cloud PBX*, SIP trunks or scripted *Interactive Voice Response* (IVR) systems.

2.3. Billing Systems and Call Routing

Understanding billing mechanisms is key to understand telephony fraud, as most of the fraud schemes aim at financial benefits. Operators keep Call Detail Records (CDR) for each call routed (originated, terminated or transited) over their networks. CDRs are created at the network switches and include various information, such as originating and destination phone numbers, inbound and outbound routes, date, call duration and call type. All CDRs generated at different switches are collected and processed in a central location and sent to the billing system to be charged. Operators deal with two types of billing: *retail billing* and *wholesale billing*.

Retail Billing. Most services (international or domestic landline, mobile, or data services) are billed to customers at the end of the billing period (*post-paid*). However,

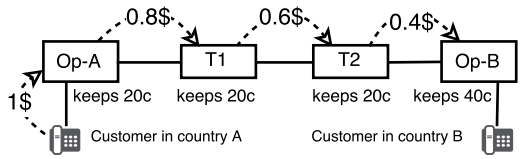

Figure 2: Overview of money flows in a call.

mobile services are also often available as *pre-paid*. The post-paid billing process involves the collection of usage reports, validating them, applying the tariff plan and sending the final bill to the customers. To be sure to be paid, operators verify the personal and financial information of their post-pay customers. In the pre-paid billing, customer information check is often less strict, because the customer will only be able to use the service he already paid for.

Wholesale Billing. The wholesale (interconnect) market is mainly for international and long distance calls, as operators need to make *interconnection agreements* and to rely on *transit operators* to be able to provide world-wide coverage. Such interconnect agreements describe the prices for interconnect communications, but also policies and dispute resolution. There are also stock-exchange like platforms where operators can buy and sell minutes directly and even anonymously [29].

An example of money flow, in an international call, is shown in Figure 2. The call is initiated from the originating operator (Op-A) and goes through two transit operators, to finally reach the customer through Op-B. For this call, Op-A will bill his end customer for a *collection charge* of $1. However, the operator will pay 80c for routing the call, and keep 20c, similarly the transit operators each keep a 20c and finally the terminating operator Op-B will keep the termination fee of 40c. In other words, each upstream (originator) network pays to its downstream (terminator) network the cost of terminating the call [30] until the call reaches its final destination. Operators may have multiple routing choices to route a call. They choose the best route depending on the prices and quality of alternative routes. The process of checking the quality and reliability of a transit operator before the partnership agreement is called *due diligence*. Unlike in IP networks, the routing of a call is very often opaque. Each operator only knows the next hop of the upstream and downstream routes as well as the originating[2] and the destination number.

3. Fraud Taxonomy: Overview and Systematization Methodology

One common fallacy in previous classifications is that the fraud descriptions are often bundling different problems together. For example, a fraud will be described by the technique it uses. However, techniques used by a given fraud often change, e.g., in reaction to the implementation of new countermeasures. The intricate combination of those concepts makes previous descriptions confusing or narrow.

2. The originating number may be absent or incorrect.

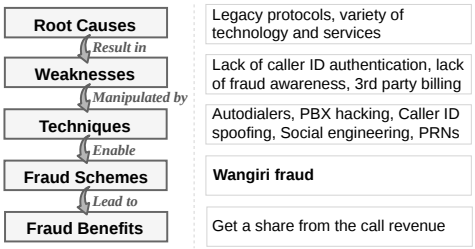

Figure 3: Overview of our fraud taxonomy with an example of Wangiri fraud.

We propose to analyze the problem in several layers to clarify the cause and effect relations surrounding telephony fraud and explore a part of the problem at each layer. For this purpose, we base our classification on the following definition of fraud:

> A **fraud scheme** is a way to obtain an illegitimate **benefit** using a **technique**. Such techniques are possible because of **weaknesses** in the system, which are themselves due to **root causes**.

Based on this general definition we further refine these concepts as follows:

- A **root cause** is an inherent characteristic of the telephony networks, standards and ecosystems which can result in weaknesses.
- A **weakness** is a vulnerability or a feature of the system, that can be manipulated in unintended ways.
- A **technique** is a mechanism, or service, which is used to abuse a weakness in a telephony system to commit a fraud. Such techniques may be illegitimate (e.g., compromising a PBX) or may have legitimate uses (e.g., conference calling) that are abused to commit a fraud.
- A **fraud scheme** is a method which is intentionally and knowingly used by a fraudster, relying on one or more techniques, to abuse a user, an entity, or a system with the goal of obtaining an illegitimate benefit.
- **Benefit**: The goal of a fraud scheme is to obtain a benefit, this can be a monetary benefit or not (e.g., competitive advantage, reputation, bypassing regulation).

3.1. Applying the Taxonomy on Wangiri Fraud

To present our taxonomy in a concrete way, we analyze Wangiri fraud, which is a well-known voice scam, within this context. Figure 3 summarizes this example.

Wangiri ('one ring and cut' in Japanese) fraud is also called *callback* scam, *ping call* or *one-ring* scam. In this scam, the fraudster leaves missing calls on a huge number of (usually randomly chosen) victims' phone numbers. The call only rings once, so that the victim does not have the opportunity to answer. As a result, the curious victim calls back the phone number, which usually turns out to be a premium rate number (PRN) owned by the fraudster. The **fraud benefit** in this scheme is financial: the premium rate service provider pays the fraudster a certain share of the call

revenue for each minute of call received by this premium rate number.

To generate the large number of calls, the fraudster can use **multiple techniques**, e.g., autodialers or compromised PBX systems and spoof the originating phone number (caller ID) as the premium rate number. The fraudster can easily set up this scheme using online premium rate service providers or resellers. Such online services even include ready to use IVR systems to keep victims on the phone for a longer duration.

These techniques abuse several **weaknesses** in the telephony ecosystem, which could be related to the underlying technologies (e.g., lack of caller ID authentication), third party services (e.g., abusive PRN resellers) or end users (e.g., users' lack of fraud and security awareness).

Finally, we can identify the **root causes** that result in these weaknesses, such as the presence of legacy protocols, convergence of multiple technologies and variety of service providers. Analyzing the problem at these different layers can help us see the overall picture and anticipate the outcome of possible actions to fight this fraud.

3.2. Methodology

Our goal is not to provide an exhaustive list of frauds, but to provide a comprehensive survey of the topic. For this, our first source of information was the literature, books, publications but also white papers from industry groups and fraud management companies. However, this is not enough as information on the topic is scattered and often incomplete.

To make sure we had a good understanding of the ecosystem, we interviewed several experts in the field and participated to industry forums. We also sent a questionnaire to a selected list of experts and well identified mailing lists to obtain feedback on the first version of our taxonomy. We only had 15 answers to this questionnaire (so we don't present statistics) but most were from experts in fraud management or those working in the field. Their feedback and some discussions with the respondents allowed us to refine our taxonomy, to better understand fraud, and to discover new fraud schemes.

Figure 4 shows a detailed view of the taxonomy. However, it is not feasible to draw all the relations between each component of the figure in one page. Therefore, we created a dynamic picture showing all the links between the components which is available, with a copy of the questionnaire, at: https://telephony-fraud.github.io/taxonomy/.

Finally, our goal with this classification is to help explain each component of telephony fraud without ambiguity. In the next sections, we describe the taxonomy: root causes and weaknesses, techniques, fraud schemes and benefits in more detail.

4. Root Causes of Telephony Fraud

Root causes are inherent to the telephony ecosystem and are unlikely to be solved in the near term.

The **legacy systems** that lie in the core of telephony network were not designed with security in mind. This was not an issue when telecom networks were a closed and controlled environment where all the entities were trusted (monopolistic operators). However, this can cause various weaknesses in today's environment. Unfortunately, upgrading these legacy systems on a global scale is not feasible in near future, due to high costs.

Telecommunication networks comprise of different, **interconnected technologies**, services and products, which are usually obscure and poorly understood [13]. This turns telephony networks into a large attack surface. All actors in the ecosystem have to adopt themselves to new technologies, while remaining vigilant against possible attacks.

As the telecom market became more liberalized, a **large number and variety of operators** have gotten involved in the market. As a result, it is not possible to make sure that all parties are carrying good intentions. It is also not possible to reduce the number of operators, as this would damage the competition and liberalization, and prevent the growth of new technologies and diversity of services.

5. Weaknesses of Telephony Networks

Weaknesses are consequences of the root causes, but they can be addressed or mitigated, if they are properly identified. We classify weaknesses in 4 categories related to **protocol and network**, **regulation**, **billing** and **human factors**.

5.1. Protocol and Network Weaknesses

Telecom networks are an interconnection of PSTN, cellular and IP networks, all of which have different weaknesses and vulnerabilities. In particular, the **lack of security mechanisms in SS7 signaling** leads to many problems, SS7 itself does not have any encryption or authentication mechanisms. Therefore, operators using SS7 (or anyone with access to signaling links) can tamper with SS7 messages or interact with SS7 systems [25]. The SIGTRAN protocol suite was introduced as a transport layer for SS7 messaging over IP, which can use TLS or IPSec [31]. However, there is no end-to-end security and each transit operator can modify the SS7 messages.

With deregulation and Internet convergence, it became **easy to access SS7 networks**, i.e., access is no more restricted to a small number of trusted operators. Nowadays, operators employ traffic screening mechanisms and filtering rules to discard unwanted incoming signaling messages [25]. Indeed, it became easier for external parties to have partial or complete access to signaling through femtocells, SIP/PRI trunks, operator partnerships (e.g., value added services) or by attacking telecom equipment [32]. Legal interception gateways, which operators often have to install to comply with laws, also have direct access to SS7, and have been sources of vulnerabilities [33], [34].

The SS7 protocol also does not support a mechanism to trace the route of a call. Each switch has its own routing

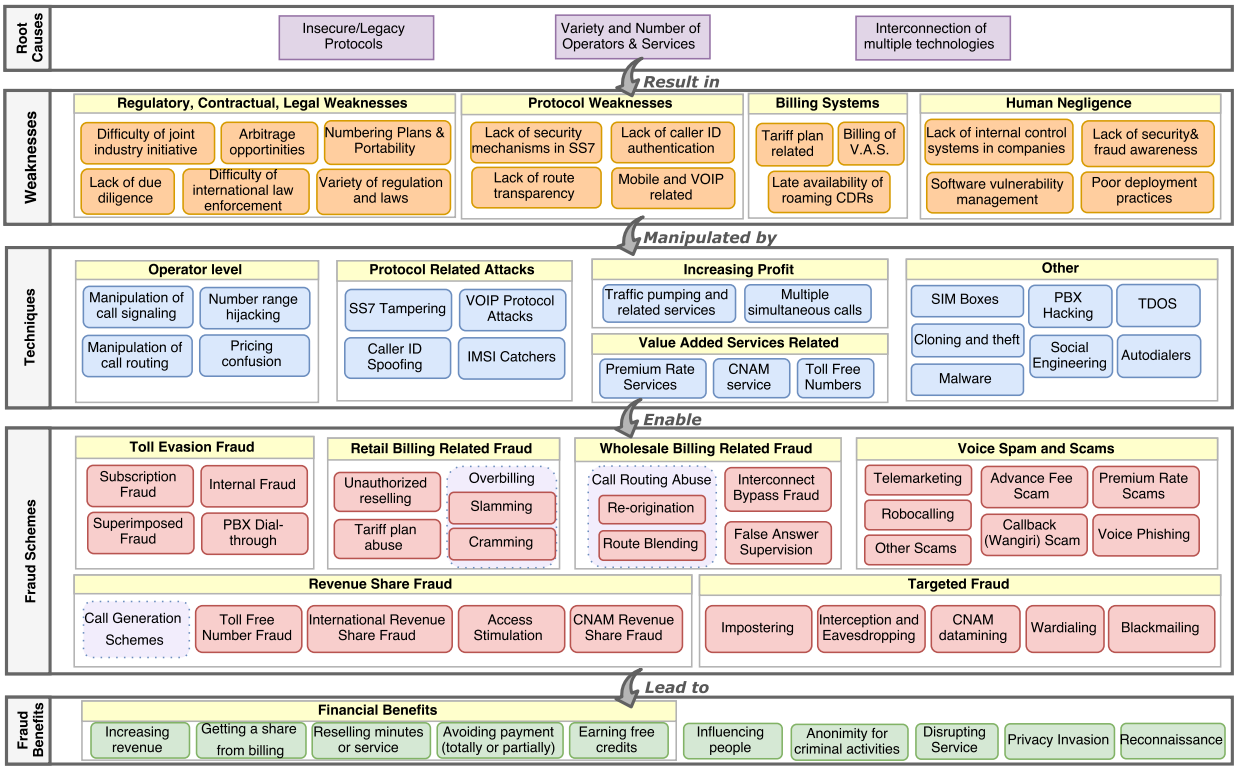

Figure 4: Comprehensive picture of voice fraud. A dynamic figure with links can be found at: https://telephony-fraud.github.io/taxonomy/

table and select the appropriate outbound link based on the destination phone number, pricing and commercial agreements. Thus, they only have a partial view of the call route which leads to a **lack of route transparency**. VoIP interconnections make it even harder to trace the calls. Similarly, during a phone call, caller ID (identification) information is transmitted between operators through the signaling system of the underlying telecommunication service. However, this information cannot be trusted as SS7 [25] or most of the IP based signaling protocols **lack caller ID authentication**.

Wireless and VoIP networks also often lack proper authentication or encryption, e.g., between a mobile device and a base station, leading to the possibility to use *IMSI Catchers* [35]. Most of the problems in mobile network protocols are addressed starting with third generation networks. However, legacy technologies are still widely deployed, opening the possibility of downgrade attacks [36]. In addition, cellular and VoIP networks inherit some vulnerabilities from PSTN, as calls still traverse PSTN networks [37]. LTE networks involve both VoIP and cellular network related issues, and can be vulnerable to billing, DoS and caller ID spoofing attacks [38].

5.2. Regulatory, Contractual and Legal Weaknesses

Arbitrage, as a concept in economics, is the manipulation of price discrepancies in different markets. In telecommunications, price discrepancies can occur between mobile/PSTN/VoIP originated calls or domestic/international calls. Fraudsters can circumvent the high cost route or terminate a high cost call in a low cost market to profit from the price difference. Countries with high international call termination rates (usually developing countries with heavy regulations [39]) are frequently manipulated by fraudsters.

Numbering plans allow to decode phone numbers and find the operator or type of service for a given number. The E.164 standard describes a globally routable phone numbering structure and assigns number ranges (country codes) to countries [40]. Each country has its own regulatory body to further assign and control its national number range, but number portability blurs the lines. There is no global numbering plan listing all valid number ranges that are in use, although some databases allow partial lookups[3]. Therefore, an operator may not know for sure, if a phone number in another country is currently in use [41]. VoIP protocols use the notion of contacts instead of phone numbers. However, if the call traverses a VoIP/PSTN gateway, a phone number should be associated with the contact [42]. Many OTT providers use phone numbers to identify and authenticate their users (e.g., Viber, WhatsApp).

Telephony ecosystem embodies a large **variety of regulations and laws**, and the notion of legality can significantly vary depending on the country and the communication medium. For example, some countries ban VoIP usage, e.g.,

3. www.bsmilano.it, www.numberingplans.com

to protect their revenue from international call termination [43]. Some countries try to bound OTT providers by the same regulations that operators are subjected to [44], [45]. In general, the need for regulation may not be perceived before the system is manipulated. Therefore, it can be difficult for regulators to anticipate regulation needs.

The **lack of cooperation** is another weakness of telephony ecosystem. Law enforcement authorities have **difficulties in international law enforcement**, which makes identification of fraudsters difficult, even when the fraud is detected [24]. Moreover, despite the presence of international organizations, there is a **lack of joint industry initiative** to fight fraud. Due to the privacy issues and competition, operators are usually not willing to share their pricing terms, routing options or fraud related findings [46]. In addition, not all the operators have the same incentives to fight fraud. Indeed, sometimes the losses due to fraud at one operator can benefit another, innocent, operator in addition to the fraudster. In other cases, fighting small scale fraud can be more expensive than the losses due to the fraud itself.

Having a large number of operators brings the inevitable need for partnerships between them. **Lack of due diligence** in these partnership agreements make call traffic vulnerable to fraud, if one party has fraudulent intentions. Especially the competitive transit operators may ignore route quality and make use of cheap routes to grow their business.

5.3. Billing Related Weaknesses

Complexity of billing mechanisms have increased with the introduction of new technologies and services. Any mistake in the billing process (e.g., inaccurate or late billing, errors in pre-paid credit tracking) can be manipulated by fraudsters [13], [20]. Most of the time, operators are reluctant to change the legacy billing systems, due to the high cost and backward compatibility problems. Errors in the complicated *tariff plans* can also be manipulated.

Billing of **value added services** is another weakness, because it adds a third party to the system. Because of their high fees, they can result in significant losses. Operators should be careful in identification of value added service numbers and registration of entities who use these numbers. Unfortunately, fraudsters often abuse complex networks of resellers and service providers and are therefore difficult to identify.

Mobile roaming services also complicate billing. **Roaming CDRs** are not immediately available to the home operator, so detecting and stopping fraud quickly is difficult. To address this issue, Near Real Time Roaming Data Exchange (NRTRDE) systems have been developed. Nevertheless, using NRTRDE, the transmission of CDRs from the visited network to the home network still takes about four hours [47], which is a long enough time window for the fraudsters to make profit.

5.4. Human Negligence

Humans interact a lot with telecom networks. This leads to various weaknesses due to their negligence or naivety. Lack of security and fraud awareness is frequently manipulated by fraudsters [13]. On the enterprise level, lack of internal control systems (such as access control), poor deployment practices (weak passwords, neglecting updates) and lack of vulnerability management in software and hardware systems are some other sources of weaknesses [21].

6. Techniques Used in Fraud Schemes

In this section, we describe the techniques which enable various fraud schemes. Some of these techniques may have legitimate uses as well. We group them by the kind of access they require (e.g., operator level) or their purpose (e.g., increasing profit).

6.1. Operator Level Techniques

Number range hijacking occurs when a fraudulent operator advertises very cheap rates for a destination number range and attracts traffic from other operators [48]. For example, in Figure 1, there are several possible routes to the terminating operator. Assume that routes 1 and 3 are the usual routes. In the event that the transit operator 3 suddenly advertise a very cheap rate (possibly for a very small range of numbers), the originating operator may select route 2 for delivering the calls. In this case, the calls to the victim number range will be hijacked and routed/terminated fraudulently [49], [50]. Lack of due diligence in operator partnership agreements facilitates this technique.

A parallel can be made between phone number range hijack and BGP hijacks [51]. In both cases, a part of the traffic is redirected by a malicious entity that advertises false (or misleading) information. For phone number ranges, this is the price for a destination, while in BGP, this is the prefix advertisements. However, as opposed to the IP networks, call routing is opaque (Section 5.1), which makes detection more difficult. Furthermore, there is no mechanism in telephony networks to directly authenticate the owner of a number range or check if an operator really has the connectivity to route the call to that number range. Like with BGP, deploying security mechanisms would face significant practical difficulties [52].

Manipulation of call routing is possible as the operators have full control over the calls that transit through their networks (either legitimately or because of a hijack). A fraudulent transit operator can divert a call or send it over illegitimate routes to perform different fraud schemes. In case of *call short-stopping*, the transit operator directly terminates the call (e.g., to an IVR) instead of sending the call to the legitimate destination. It can also selectively *short-stop* only some of the calls. Due to the lack of route transparency, the originating operator cannot know if the call was routed normally and has reached the correct destination.

Manipulation of call signaling messages is also easy for the operators. For example, the caller ID can be changed to fake the origin of the call (which may affect billing). Call setup signals can be tampered to answer the call before it is actually answered by the customer (*early answer*) or to not disconnect the call immediately (*late disconnect*) [53]. The call will be longer than it should, which will affect the revenue (False Answer Supervision, see Section 7.3).

Pricing confusion is the use of multiple and varying pricing plans to confuse customers about the real market price of a service. Such operators constantly provide new offerings and special introductory discounts, to be competitive [15], but quickly change the prices once customers are registered.

6.2. Techniques For Increasing Profit

Here we present techniques which can be used to make a fraud scheme more efficient, however, many of them have a legitimate use.

Traffic pumping, or artificial inflation of traffic, is the act of generating a high level of call traffic to some phone numbers deliberately. This can be achieved by creating and advertising 3rd party services such as conference calling [54], free radio broadcast over phone [55] or adult entertainment. By providing such services for free (or at a very low cost) many users are attracted, which, in turn, generates a high volume of calls. Value added services or arbitrage opportunities can make traffic pumping advantageous in certain fraud schemes (Sections 7.4 and 7.3).

Initiating **multiple simultaneous calls** allows the fraudster to increase the profit of a fraud scheme in a certain time window. Multiple outgoing calls, or conference calls, can be generated on compromised PBXs [10], VoIP accounts [56], or SIM cards. Up to 6 simultaneous calls can be generated from a single SIM card [57]. Finally, *call forwarding* can be used to forward all incoming calls to a certain fraudulent phone number.

6.3. Value Added Services

Premium Rate Numbers (PRN) are used to provide wide range of services such as gambling, live chat, adult services; through voice call or SMS. To cover the cost of services provided, the cost of calling a premium rate number is much higher than a regular call. In most countries, a fixed number range is allocated for PRNs which allows users to easily distinguish them, however, it is not true everywhere. Users sometimes tend to confuse the number ranges and call PRNs unwittingly. Such premium rate numbers may be abused, e.g., when the promised service is not delivered, the cost of the service is not clearly stated or artificial traffic is created to these numbers [48]. The abusive premium rate services usually manipulate the lack of due diligence between number resellers and numbering plans in which the premium rate number range is not clearly identifiable by users [58]. Many online sites offer premium rate number services, which gives a cash back on calls reaching this premium number.

CNAM (Caller Name) lookup service provides a 15-character long caller name string (associated with caller's phone number), to help users easily identify a caller [59]. In the USA, operators are responsible for making the CNAM lookup (dip) for the calls received by their customers. A CNAM service usually comes as part of the landline package and it is enabled by default. However, there is no centralized CNAM database in North America. Instead, multiple independent CNAM providers allow operators to lookup the CNAM information for a fee [60]. Fraudsters can use a CNAM service to register a false caller name for their phone number, or to abuse the payment mechanism (Section 9).

Toll free numbers are phone numbers which do not incur any charges to the caller. Instead, the call is charged to the toll free customer (call recipient), which are usually call center services. Toll free numbers use a prefix allocated by the regulator. For toll free numbers, charge collection is reversed: The toll free customer pays the toll free number provider (usually the terminating operator) for all incoming calls. Toll free providers keep a part of the profit and passes a share to the originating operator, as the caller does not pay for the call [61].

6.4. Protocol Related Attacks

SS7 tampering by external parties became possible with easy access to SS7 networks. This can lead to attacks such as locating the phone users, intercepting the calls or denial of service [62], [63].

VoIP protocol attacks can manipulate the implementation flaws, underlying network platform or the voice application layer [64]. Various attacks, such as SIP scanning, registration hijacking, redirection attacks, session tear down, SIP phone reboot and audio insertion are demonstrated in [21], [37]. Billing systems can be manipulated through VoIP attacks as well [65].

IMSI catchers (or *stingray*) [35], [36] are fake GSM base stations that are used to identify phones in proximity (catch their IMSI), intercept calls and communications, or even to send out spam and fraud messages [66]. IMSI catchers manipulate the lack of authentication from the network to the device in GSM. Such a fake base station can be built using operator grade equipment or open-source software and cheap hardware [67], [68], [69]. The phone is deceived to connect to the false base station and usually the mobile device is forced to not use encryption or downgrade to an insecure mode (e.g., 3G to 2G) [36]. More recent mobile protocols (like LTE) are using authentication but are not immune to such attacks; first, the authentication keys could be leaked (or seized); second, the IMSI catcher may abuse vulnerabilities in the protocol stacks [70]. Some discrepancies in the perceived network features can be used to detect IMSI catchers [71], [72], [73], [74].

Caller ID spoofing requires transmission of fake caller IDs in the signaling system. Even though there are certain